Ryhmän $PSL(2, K)$ yksinkertaisuus

Pro gradu -tutkielma
Antti Eronen
2187183
Matemaattisten tieteiden yksikkö
Oulun yliopisto
Kevät 2017

Sisältö

Johdanto **2**

1 Peruskäsitteitä ja tarpeellisia lauseita **3**
1.1 Ryhmät 3
1.2 Aliryhmät ja tekijäryhmät 5
1.3 Homomorfismit 6
1.4 Renkaat ja äärelliset kunnat 7
1.5 Konjugaatit 9
1.6 Matriisilaskentaa 2×2 -matriiseilla 10

2 Lineaariset ryhmät **12**

3 Ryhmän $PSL(2, K)$ yksinkertaisuudesta **17**
3.1 Ryhmä $PSL(2, 2)$ 17
3.2 Ryhmä $PSL(2, 3)$ 17
3.3 Ryhmä $PSL(2, 4)$ 20
3.4 Ryhmä $PSL(2, 5)$ 29
3.5 Ryhmä $PSL(2, K)$ 43

4 Ryhmän $PSL(m, K)$ yksinkertaisuudesta **52**

Lähdeluettelo **54**

Johdanto

Tutkielmassa on perehdytty lineaarisiin ryhmiin ja erityisesti astetta kaksi olevan projektiivisen erityisen lineaarisen ryhmän kunnan K suhteen, eli ryhmän $PSL(2, K)$, yksinkertaisuuteen. Luvussa 1 esitellään ryhmäteorian olennaisia peruskäsitteitä ja tarpeellisia peruslauseita, sekä valaistaan hieman matriisiteoriaa 2×2 -matriiseille. Luvussa 1 lauseille ei kuitenkaan esitetä todistuksia, sillä nämä käsitellään enemmänkin perustietona, joihin lukija voi halutessaan perehtyä lähdemateriaalin avulla tarkemmin.

Luvussa 2 määritellään tutkielmassa tarpeelliset kolme erilaista lineaaristä ryhmää. Näitä koskevat lemmat todistetaan käyttäen hyväksi luvussa 1 esitettyjä tietoja. Luvussa 2 määriteltävää astetta kaksi olevaa yleistä lineaarista ryhmää kunnan K suhteen, eli ryhmää $GL(2, K)$, ei käsitellä tarkasti. Se on kuitenkin hyödyllinen astetta kaksi olevan erityisen lineaarisen ryhmän kunnan K suhteen, eli ryhmän $SL(2, K)$, määrittelyyn. Pääpainona tutkielmassa on kuitenkin ryhmän $SL(2, K)$ tekijäryhmässä, eli ryhmässä $PSL(2, K)$.

Luvussa 3 päästään varsinaiseen tutkielman aiheeseen, eli tutkimaan ryhmän $PSL(2, K)$ yksinkertaisuutta. Aluksi osoitetaan, että mikäli kunnan K kertaluku on 2 tai 3, niin $PSL(2, K)$ ei ole yksinkertainen. Tämän jälkeen tehdään laajat konjugointiluokkatarkastelut, joiden avulla havaitaan, että ryhmä $PSL(2, K)$ on yksinkertainen, kun kunnan K kertaluku on 4 tai 5. Lopuksi tutkitaan yleistä tapausta ja havaitaan, että ryhmä $PSL(2, K)$ on yksinkertainen, jos ja vain jos kunnan K kertaluku on suurempi kuin kolme.

Lisäksi luvussa 4 valaistaan yleistä tapausta, eli ryhmän $PSL(m, K)$ yksinkertaisuutta. Luvussa 4 ei kuitenkaan todisteta enää varsinaisesti mitään, vaan tuloksia esitellään kerronnallisessa muodossa. Tämän luvun tavoite ei ole perehdyttää lukijaa yleisen tapauksen todistuksiin, vaan enemmänkin kertoa, mitä aiheeseen enemmän perehtyvä voi olettaa löytävänsä edestään.

1 Peruskäsitteitä ja tarpeellisia lauseita

Määritellään ensin muutamat tutkielman kannalta olennaiset käsitteet ja niille tarpeellisia peruslauseita. Todistuksia näille lauseille ei tässä tutkielmassa käsitellä, mutta ne löytyvät muutamaa poikkeusta lukuunottamatta lähteistä [2], [3], [4], [5] ja [7]. Näiden poikkeuksien kohdella mainitaan erikseen, mistä lähteestä todistukset löytyvät.

1.1 Ryhmät

Määritelmä 1.1. Olkoot $G \neq \emptyset$ ja $(*)$ joukon G operaatio. Nyt pari $(G, *)$ on *ryhmä*, mikäli seuraavat neljä ehtoa toteutuvat:

1. Operaatio $(*)$ on binäärinen eli

$$a * b \in G$$

   aina, kun $a, b \in G$;

2. Operaatio $(*)$ on assosiatiivinen eli

$$(a * b) * c = a * (b * c)$$

   aina, kun $a, b, c \in G$;

3. Joukossa G on sellainen alkio e, että

$$a * e = e * a = a$$

   kaikilla $a \in G$. Alkiota e kutsutaan *neutraalialkioksi* tai *ykkösalkioksi.* Ykkösalkiota merkataan tässä tutkielmassa usein myös luvulla $\mathbf{1}$;

4. Kaikilla $a \in G$ on olemassa sellainen alkio $a^{-1} \in G$, että

$$a * a^{-1} = a^{-1} * a = e.$$

   Alkiota a^{-1} kutsutaan *alkion a käänteisalkioksi.*

Jos lisäksi $(G, *)$ toteutaa ehdon

$$a * b = b * a$$

aina, kun $a, b \in G$ eli operaatio $(*)$ on kommutatiivinen, niin kyseessä on *Abelin ryhmä* eli kommutatiivinen ryhmä.

Ryhmän *kertaluku* on ryhmän alkioiden lukumäärä, merkitään $|G|$.

Lemma 1.2. *Ryhmän G ykkösalkio $\mathbf{1}$ ja alkion $a \in G$ käänteisalkio a^{-1} ovat yksikäsitteiset.*

Huomautus 1.3. Mikäli on selvää, mistä operaatiosta puhutaan, merkintä $a*b$ voidaan kirjata lyhyemmin muodossa ab.

Määritelmä 1.4. Kokonaisluvuista $\mathbb{Z}$ voidaan muodostaa *jäännösluokat* (mod m), kun käytetään hyväksi kongruenssia

$$x \equiv y (\text{mod } m) \ \Leftrightarrow m \mid x - y.$$

Kokonaisluvun $y \in \mathbb{Z}$ määräämässä jäännösluokassa (mod m), eli joukossa

$$[y] = \{x \in \mathbb{Z} \mid x \equiv y \ (m)\},$$

on kaikki sellaiset kokonaisluvut x, joilla on sama jakojäännös kuin luvulla y jaettaessa luvulla m.

Jakoalgoritmin nojalla jaettaessa luvulla m mahdollisia jakojäännöksiä ovat luvut $0, 1, 2, ..., m-1$. Siten kaikki jäännösluokat (mod m) ovat

$$\mathbb{Z}_m = \{[0], [1], [2], [3], ..., [m-1]\}.$$

Jäännösluokkaa $[a]$ sanotaan *alkuluokaksi* (mod m), mikäli $\text{syt}(a, m) = 1$. Alkuluokkien (mod m) joukkoa merkitään $\mathbb{Z}_m^*$

Huomautus 1.5. Mikäli m on alkuluku, niin $\mathbb{Z}_m^* = \{\mathbb{Z}_m \backslash [0]\} = \{[1], [2], [3], ..., [m-1]\}$.

Jäännösluokille (mod m) käytetään seuraavia yhteen- ja kertolaskuoperaatioita:

$$[a] + [b] = [a + b]$$

ja

$$[a][b] = [ab].$$

Jäännösluokkien avulla voidaan määrittää seuraavat paljon käytetyt ryhmät:

Lemma 1.6. *Joukkoja $\mathbb{Z}_m$ ja $\mathbb{Z}_m^*$ sekä näiden yhteen- ja kertolaskuoperaatioita hyödyntäen saadaan muodostettua seuraavat Abelin ryhmät:*

1. *Pari $(\mathbb{Z}_m, +)$ on Abelin ryhmä,*
2. *Pari $(\mathbb{Z}_m^*, \cdot)$ on Abelin ryhmä.*

1.2 Aliryhmät ja tekijäryhmät

Määritelmä 1.7. Olkoon $(G, *)$ ryhmä ja $H \subseteq G,\ H \neq \emptyset$. Jos $(H, *)$ on ryhmä, sitä sanotaan *ryhmän G aliryhmäksi;* merkitään $H \leq G$.

Lause 1.8. ***(Aliryhmäkriteeri)*** *Olkoon $(G, *)$ ryhmä ja $H \subseteq G,\ H \neq \emptyset$. Nyt $H \leq G$ jos ja vain jos seuraava ehto toteutuu:*

$$a, b \in H \Rightarrow a * b^{-1} \in H.$$

Määritelmä 1.9. Olkoon $H \leq G$ ja $a \in G$. Nyt joukkoa $aH = \{a * h \mid h \in H\}$ sanotaan *alkion a määräämäksi aliryhmän H vasemmaksi sivuluokaksi.* Vastaavasti $Ha = \{h * a \mid h \in H\}$ on *alkion a määräämä aliryhmän H oikea sivuluokka.* Vasempien sivuluokkien lukumäärä on aliryhmän H *indeksi ryhmässä G*, merkitään $[G : H]$.

Lause 1.10. ***(Lagrangen lause)*** *Jos G on äärellinen ryhmä ja $H \leq G$, niin*

$$|G| = [G : H] \cdot |H|.$$

Eli aliryhmän kertaluku jakaa ryhmän kertaluvun.

Olkoot $(G, *)$ ryhmä, $a \in G$ ja $n \in \mathbb{Z}_+$. Jatkossa käytetään seuraavia merkintöjä:

$$a^k = \underbrace{a * a * a * ... * a}_{k \text{ kpl}} \text{ ja } a^{-k} = \underbrace{a^{-1} * a^{-1} * a^{-1} * ... * a^{-1}}_{k \text{ kpl}}.$$

Lisäksi asetetaan $a^0 = e = \mathbf{1}$.

Nyt voidaan muodostaa yksittäisen alkion generoima syklinen ryhmä, joka on ryhmän G aliryhmä.

Määritelmä 1.11. Olkoon $(G, *)$ ryhmä, $a \in G$ ja $H = \{a^k \mid k \in \mathbb{Z}\}$. Nyt ryhmä $(H, *)$ on *alkion a generoima syklinen aliryhmä;* merkitään $\langle a \rangle$.

Lemma 1.12. *Olkoot G ryhmä, $a \in G$ ja n pienin sellainen positiivinen kokonaisluku, että $a^n = e$. Tällöin $|\langle a \rangle| = n$ ja*

$$\langle a \rangle = \{a^0 = e, a, a^2, a^3, ..., a^{n-1}\}.$$

Määritelmä 1.13. Olkoon $N \leq G$. Aliryhmää N sanotaan *normaaliksi,* mikäli $aN = Na$ tai $a^{-1}Na = N$ aina, kun $a \in G$; merkitään $N \trianglelefteq G$.

Huomautus 1.14. Ryhmällä G on aina triviaalit normaalit aliryhmät $\{e\}$ ja G.

Määritelmä 1.15. Mikäli ryhmällä G on vain triviaalit normaalit aliryhmät, niin G on *yksinkertainen ryhmä.*

Määritelmä 1.16. Ryhmän $(G, *)$ normaalin aliryhmän N sivuluokista voidaan muodostaa ryhmä $(\{aN \mid a \in G\}, *)$, jossa operaatio $(*)$ määritellään seuraavasti:

$$aN * bN = (a * b)N.$$

Ryhmää $(\{aN \mid a \in G\}, *)$ kutsutaan *ryhmän G tekijäryhmäksi aliryhmän N suhteen,* merkitään G/N.

Seuraavaksi esitettävän lauseen todistus löytyy lähteestä [1] sivulta 65.

Lause 1.17. *Olkoon G ryhmä. Tällöin*

$$N \trianglelefteq H \trianglelefteq G \Leftrightarrow H/N \trianglelefteq G/N.$$

Lause 1.17 pätee myös aliryhmille H, jolloin

$$N \trianglelefteq H \leq G \Leftrightarrow H/N \leq G/N.$$

Huomautus 1.18. Mikäli ryhmä G on äärellinen, niin

$$|G/N| = \frac{|G|}{|N|}.$$

Huomautus 1.19. Jos $H \leq G$ ja $[G : H] = \frac{|G|}{|H|} = 2$, niin $H \trianglelefteq G$.

1.3 Homomorfismit

Määritelmä 1.20. Olkoot $(G, \cdot)$ ja $(F, *)$ ryhmiä. Nyt kuvaus $f : G \to F$ on *ryhmähomomorfismi,* mikäli $f(a \cdot b) = f(a) * f(b)$ aina, kun $a, b \in G$. Jos lisäksi kuvaus f on bijektio, sitä kutsutan *isomorfismiksi.* Jos on olemassa tällainen isomorfismi, niin ryhmät G ja F ovat tällöin *isomorfiset*, merkitään $G \cong F$.

Määritelmä 1.21. *Homomorfismin f kuva* on joukko

$$f(G) = Im(f) = \{f(x) \mid x \in G\}$$

ja *ydin* on joukko

$$Ker(f) = \{x \in G \mid f(x) = e_F\},$$

missä e_F on ryhmän F ykkösalkio.

Lemma 1.22. *Olkoon kuvaus $f : G \to F$ homomorfismi. Tällöin*

$$Ker(f) \trianglelefteq G$$

ja

$$Im(f) \leq F.$$

Lause 1.23. ***(Homomorfismien peruslause)*** *Olkoon kuvaus $f : G \to F$ ryhmähomomorfismi. Tällöin*

$$G/Ker(f) \cong Im(f).$$

1.4 Renkaat ja äärelliset kunnat

Määritellään ensimmäisenä rengas, jotta pystytään määrittämään tämän pohjalta tutkimuksen kannalta olennainen erityistapaus, kunta.

Määritelmä 1.24. Kolmikko $(R, +, \cdot)$ on *rengas,* mikäli seuraavat kolme ehtoa toteutuvat:

1. Pari $(R, +)$ on Abelin ryhmä. Ryhmän ykkösalkiota merkataan luvulla $\mathbf{0}$ ja kutsutaan renkaan yhteydessä *nolla-alkioksi*;

2. Operaatio $(\cdot)$ on binäärinen ja assosiatiivinen sekä on olemassa $\mathbf{1} \in R$ siten, että
$$\mathbf{1} \cdot a = a \cdot \mathbf{1} = a$$
kaikilla $a \in R$. Alkiota $\mathbf{1}$ kutsutaan renkaan R *ykkösalkioksi;*

3. Seuraavat distributiivisuus- eli osittelulait ovat voimassa:
$$a(b + c) = ab + ac$$
ja
$$(a + b)c = ac + bc$$
aina, kun $a, b, c \in R$.

Rengas on *kommutatiivinen*, mikäli $ab = ba$ aina, kun $a, b \in R$.

Määritelmä 1.25. Rengas $(K, +, \cdot)$ on *kunta,* mikäli se on kommutatiivinen rengas ja $(K\backslash\{\mathbf{0}\}, \cdot)$ on ryhmä. Kunnassa $(K, +, \cdot)$ ryhmä $(K, +)$ on *additiivinen ryhmä* ja $(K\backslash\{\mathbf{0}\}, \cdot)$ on *multiplikatiivinen ryhmä.*

Olkoot $(K, +, \cdot)$ kunta, $a, b \in K$ ja $n \in \mathbb{Z}_+$. Kuntia käsiteltäessä käytetään seuraavia merkintöjä:

- $-a$ on alkion a käänteisalkio additiivisessa ryhmässä, kutsutaan myös *vasta-alkioksi* ja $b + (-a) = b - a$
- a^{-1} on alkion a käänteisalkio multiplikatiivisessa ryhmässä, kutsutaan *käänteisalkioksi*
- $na = \underbrace{a + a + a + ... + a}_{n \ kpl}$
- $-na = \underbrace{-a - a - a - ... - a}_{n \ kpl}$
- $a^n = \underbrace{a \cdot a \cdot a \cdot ... \cdot a}_{n \ kpl}$
- $a^{-n} = \underbrace{a^{-1} \cdot a^{-1} \cdot a^{-1} \cdot ... \cdot a^{-1}}_{n \ kpl}$.

Määritelmä 1.26. Kunnan ykkösalkion $\mathbf{1}$ additiivista kertalukua kutsutaan kunnan K *karakteristikaksi,* merkitään *char* K. Eli $charK$ on pienin positiivinen kokonaisluku n, jolla $n\mathbf{1} = \mathbf{0}$.

Lemma 1.27. *Kunnan karakteristika on aina alkuluku. Lisäksi, jos kunnan karakteristika on p ja $a \in K$, niin $pa = \mathbf{0}$.*

Erityisesti tutkielmassa tarvitaan äärellisiä kuntia, eli kuntia, joiden kertaluku on äärellinen.

Lemma 1.28. *Jokaisen äärellisen kunnan K kertaluku $|K| = p^n$, missä p on alkuluku ja $n \geq 1$. Tällöin $charK = p$. Lisäksi samaa kertalukua olevat kunnat ovat keskenään isomorfisia.*

Huomautus 1.29. Olkoot $(K, +, \cdot)$ kunta ja $a, b \in K$. Nyt tulo $ab = \mathbf{0}$ jos ja vain jos $a = \mathbf{0}$ tai $b = \mathbf{0}$, sillä $(K \backslash \{\mathbf{0}\}, \cdot)$ on ryhmä.

Seuraavaksi esitettävän lauseen todistus löytyy lähteestä [1] sivulta 126.

Lemma 1.30. *Äärellisen kunnan K multiplikatiivinen ryhmä $(K \backslash \{\mathbf{0}\}, \cdot)$ on syklinen.*

Huomautus 1.31. Lemmojen 1.30 ja 1.12 nojalla äärellisessä kunnassa K, jonka kertaluku $|K| = q$, on olemassa alkio $k \in K \backslash \{\mathbf{0}\}$, jolle

$$k^n = \mathbf{1}, \text{ jos } n = q - 1$$

ja

$$k^n \neq \mathbf{1}, \text{ jos } n < q - 1.$$

Lause 1.32. *Jäännösluokkarengas* $(\mathbb{Z}_m, +, \cdot)$ *on kunta jos ja vain jos* m *on alkuluku.*

1.5 Konjugaatit

Ryhmän yksinkertaisuutta tutkittaessa konjugointiluokat ovat oleellisessa osassa, sillä konjugointiluokkien unionien avulla pystytään muodostamaan kaikki mahdolliset normaalit aliryhmät.

Määritelmä 1.33. Olkoon G ryhmä ja $x, y \in G$. Jos on olemassa sellainen alkio $g \in G$, että $g^{-1}xg = y$, niin alkiot x ja y *konjugoivat ryhmässä* G. Alkion x konjugaatista käytetään myös merkintää $g^{-1}xg = x^g$.

Olkoon $\emptyset \neq M \subset G$. Vastaavasti voidaan määrittää *joukon* M *konjugaatti ryhmässä* G,

$$M^g = \{m^g \mid m \in M\}.$$

Määritelmä 1.34. Määritellään ryhmässä G ekvivalenssirelaatio $(\sim)$ seuraavasti:

$$x \sim y \Leftrightarrow \exists\ g \in G\ :\ x^g = y.$$

Tällöin ryhmä G jakautuu pistevieraisiin ekvivalenssiluokkiin eli *konjugointiluokkiin* $K_1, K_2, K_3, ..., K_r$. Tällöin

$$G = \bigcup_{i=1}^{r} K_i$$

ja

$$K_i \bigcap K_j = \emptyset, \text{ kun } i \neq j.$$

Lemma 1.35. *Olkoon* G *ryhmä ja* $N \leq G$. *Nyt* $N \trianglelefteq G$, *jos ja vain jos* N *saadaan konjugointiluokkien unionina.*

Määritellään konjugaattien avulla vielä kolme joukkoa.

Määritelmä 1.36. Olkoon $\emptyset \neq M \subset G$ ja G ryhmä.

1. Joukko
$$N_G(M) = \{g \in G \mid M^g = M\}$$
on joukon M *normalisoija* ryhmässä G;

2. Joukko
$$C_G(M) = \{g \in G \mid gm = mg \ \forall m \in M\}$$
on joukon M *sentralisoija* ryhmässä G;

3. Joukko
$$Z(G) = C_G(G) = \{g \in G \mid gx = xg \ \forall x \in G\}$$
on ryhmän G *keskus.*

Lemma 1.37. *Ryhmän G keskus $Z(G)$ on ryhmän G normaali aliryhmä, $Z(G) \trianglelefteq G$.*

Lause 1.38. *Olkoon G ryhmä ja $x \in G$. Tällöin alkion x generoiman konjugointiluokan kertaluku eli alkion x konjugaattien lukumäärä ryhmässä G on*

$$\frac{|G|}{|C_G(\{x\})|}.$$

Huomautus 1.39. Saman konjugointiluokan alkioilla on sama kertaluku. Sillä jos $|a| = n$, niin

$$(g^{-1}ag)^n = \underbrace{g^{-1}agg^{-1}ag...g^{-1}ag}_{n \ kpl} = g^{-1}a^n g = \mathbf{1}.$$

1.6 Matriisilaskentaa 2×2 -matriiseilla

Tutkielmassa käsiteltävät lineaariset matriisit muodostuvat 2×2 -matriiseista, joissa jokainen matriisin alkio kuuluu kuntaan K, joten kerrataan vielä näille muutamat oleelliset määritelmät ja laskusäännöt. Jatkossa kaikki käsiteltävät matriisit ovat 2×2 -matriiseja, vaikka annettavat laskusäännöt voitaisiinkin yleistää $m \times m$ -matriiseille. Matriiseissa pystyvektoreita kutsutaan sarakkeiksi ja vaakavektoreita riveiksi.

Määritelmä 1.40. Matriisi $I = \begin{pmatrix} \mathbf{1} & \mathbf{0} \\ \mathbf{0} & \mathbf{1} \end{pmatrix}$ on *identiteettimatriisi.*

Määritelmä 1.41. Olkoon $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Nyt matriisin A *determinantti* on

$$\det A = ad - bc.$$

Huomautus 1.42. Nyt matriisin determinantin määritelmän nojalla $\det A = \mathbf{0}$, jos ja vain jos

1. Ensimmäinen sarake on $\begin{pmatrix} \mathbf{0} \\ \mathbf{0} \end{pmatrix}$
2. Ensimmäinen sarake on $\begin{pmatrix} a \\ b \end{pmatrix}$ ja toinen sarake on $\begin{pmatrix} xa \\ xb \end{pmatrix}$, missä $x \in K$.

Matriisi A voidaan kertoa alkiolla $x \in K$, jolloin jokainen matriisin alkio kerrotaan alkiolla x,

$$x \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} xa & xb \\ xc & xd \end{pmatrix}.$$

Matriisien kertolasku toimii seuraavan kaavan mukaisesti:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} x & y \\ z & w \end{pmatrix} = \begin{pmatrix} ax + bz & ay + bw \\ cx + dz & cy + dw \end{pmatrix}.$$

Lemma 1.43. *Matriisien tulo on assosiatiivinen eli*

$$A(BC) = (AB)C.$$

Määritelmä 1.44. Nyt matriisi A on *kääntyvä*, mikäli on olemassa sellainen matriisi B, että

$$AB = BA = I.$$

Tällöin merkitään $B = A^{-1}$. Matriisia B kutsutaan matriisin A *käänteismatriisiksi.*

Lemma 1.45. *Matriisi* $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ *on kääntyvä, mikäli* $\det A \neq \mathbf{0}$ *ja tällöin*

$$A^{-1} = \begin{pmatrix} d(\det A)^{-1} & -b(\det A)^{-1} \\ -c(\det A)^{-1} & a(\det A)^{-1} \end{pmatrix}.$$

Lemma 1.46. *Matriisien tulon determinantti on determinanttien tulo eli*

$$\det AB = \det A \cdot \det B = \det B \cdot \det A = \det BA.$$

Lisäksi

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

2 Lineaariset ryhmät

Määritellään seuraavaksi kolme erilaista lineaarista ryhmää. Lineaariset ryhmät voitaisiin muodostaa millä tahansa $m \times m$ -matriiseilla, mutta tässä tutkielmassa käsitellään 2×2 -matriisien avulla muodostettuja lineaarisia ryhmiä käyttäen operaationa matriisien tuloa. Jatkossa K on äärellinen kunta ja merkitään kunnan K nolla-alkiota $\mathbf{0} = 0$ sekä ykkösalkiota $\mathbf{1} = 1$.

Määritelmä 2.1. Olkoon

$$GL(2, K) = \{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in K,\ ad - bc \neq 0 \}.$$

Nyt siis $GL(2, K)$ on joukko, joka sisältää kaikki 2×2 -matriisit, jossa alkiot kuuluvat kuntaan K ja matriisin determinatti ei ole 0. Tätä kutsutaan nimellä *yleinen lineaarinen astetta kaksi oleva ryhmä kunnan K suhteen.*

Osoitetaan vielä, että $GL(2, K)$ on ryhmä matriisien tulon suhteen.

Lemma 2.2. *$GL(2, K)$ on ryhmä matriisien tulon suhteen.*

Todistus. Osoitetaan, että määritelmän 1.1 mukaiset ehdot toteutuvat.

1. Olkoot $A, B \in GL(2, K)$. Nyt selvästi matriisin tulon määritelmän nojalla AB on edelleen 2×2 -matriisi, jonka alkiot kuuluvat kuntaan K. Lisäksi lemman 1.46 nojalla

   $$\det AB = \det A \cdot \det B \neq 0.$$

   Eli matriisien tulo on binäärinen operaatio joukossa $GL(2, K)$.

2. Lemman 1.43 nojalla tiedetään, että matriisien tulo on assosiatiivinen.

3. Selvästi $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in GL(2, K)$ ja

   $$AI = IA = A.$$

   Eli I on ryhmän $GL(2, K)$ ykkösalkio.

4. Olkoon $A \in GL(2, K)$. Tällöin lemman 1.45 mukaisella käänteismatriisilla A^{-1} pätee

   $$AA^{-1} = A^{-1}A = I.$$

   Lisäksi $A^{-1} \in GL(2, K)$.

Nyt määritelmän 1.1 mukaiset neljä ehtoa toteutuvat, joten $GL(2, K)$ on ryhmä matriisien tulon suhteen.

□

Lemma 2.3. *Olkoon* $|K| = q = p^k$, *missä* p *on alkuluku. Nyt ryhmän* $GL(2, K)$ *kertaluku on* $(q^2 - 1)(q^2 - q)$.

Todistus. Nyt huomautuksen 1.42 nojalla ensimmäinen sarake ei saa olla $\begin{pmatrix} 0 \\ 0 \end{pmatrix}$ eli vaihtoehtoja on kunnan K kertaluvun nojalla ensimmäiselle sarakkeelle $q^2 - 1$ kappaletta. Toinen sarake ei saa olla ensimmäinen sarake kerrottuna alkiolla $x \in K$ eli vaihtoehtoja toiselle sarakkeelle on $q^2 - q$ kappaletta.

Siten molemmat sarakkeet huomioiden saadaan ryhmän $GL(2, K)$ sisältämien erilaisten matriisien lukumääräksi

$$(q^2 - 1)(q^2 - q),$$

joka ryhmän $GL(2, K)$ kertaluku. □

Määritellään seuraavaksi toinen lineaarinen ryhmä, joka on yleisen lineaarisen ryhmän erikoistapaus.

Määritelmä 2.4. Joukko

$$SL(2, K) = \{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in K,\ ad - bc = 1 \}$$

on *erityinen lineaarinen ryhmä astetta 2 kunnan* K *suhteen.*

Tämä voidaan osoittaa ryhmäksi matriisien kertolaskun suhteen kuten $GL(2, K)$, mutta se saadaan myös osoitettua homomorfismien nojalla.

Lemma 2.5. *Olkoon* $|K| = q$. *Tällöin* $SL(2, K) \trianglelefteq GL(2, K)$ *ja* $|SL(2, K)| = (q - 1)q(q + 1)$.

Todistus. Nyt kuvaus $F : GL(2, K) \to K\backslash\{0\},\ F(A) = \det A$ on selvästi surjektiivinen homomorfismi, sillä lemman 1.46 nojalla

$$F(AB) = \det AB = \det A \cdot \det B = F(A) \cdot F(B)$$

ja jos $k \in K\backslash\{0\}$, niin $F(\begin{pmatrix} k & 0 \\ 0 & 1 \end{pmatrix}) = k$, missä $\begin{pmatrix} k & 0 \\ 0 & 1 \end{pmatrix} \in GL(2, K)$. Lisäksi nähdään suoraan määritelmästä 1.21, että

$$Ker(F) = SL(2, K).$$

Tällöin tiedetään lemman 1.22 nojalla, että $SL(2,K) \trianglelefteq GL(2,K)$. Näin ollen $SL(2,K)$ on ryhmä.

Kun huomioidaan, että kuvaus F on surjektio, saadaan homomorfismien peruslauseen, lauseen 1.23, nojalla muodostettua kertaluokalle seuraava yhtälö:

$$\frac{|GL(2,K)|}{|SL(2,K)|} = |K\backslash\{0\}|$$

eli

$$|SL(2,K)| = \frac{|GL(2,K)|}{|K\backslash\{0\}|}$$

eli

$$|SL(2,K)| = \frac{|GL(2,K)|}{q-1},$$

josta saadaan lemman 2.3 nojalla

$$|SL(2,K)| = \frac{(q^2-1)(q^2-q)}{q-1}$$

eli

$$|SL(2,K)| = (q-1)q(q+1).$$

□

Merkitään jatkossa $SL(2,\mathbb{Z}_p) = SL(2,p)$, missä p on alkuluku, ja $SL(2,K) = SL(2,p^n)$, missä $|K| = p^n$.

Lemma 2.6. *Ryhmän $SL(2,K)$ määritelmän 1.36 mukainen keskus on*

$$Z(SL(2,K)) = \{\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \mid a^2 = 1\}.$$

Todistus. Nyt nähdään selvästi, että $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} = aI \in Z(SL(2,K))$, kun $a^2 = 1$, sillä jos $B \in SL(2,K)$, niin

$$aI \cdot B = B \cdot aI.$$

Osoitetaan vielä, että kaikki alkiot keskuksessa ovat tätä muotoa.

Olkoon $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in Z(SL(2,K))$. Nyt $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in SL(2,K)$ ja siten

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

eli

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

Näin ollen

$$c = 0 \text{ ja } a = d.$$

Lisäksi $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \in SL(2,K)$ ja

$$\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & a \end{pmatrix}$$

eli

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

Näin ollen

$$b = 0$$

eli

$$A = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}.$$

Lisäksi $\det A = 1$ eli $a^2 = 1$. □

Huomautus 2.7. Jos *char* $K \neq 2$, niin yhtälöllä $a^2 = 1$ on ratkaisut 1 ja -1, joten $Z(SL(2,K)) = \{I, -I\}$, mutta jos *char* $K = 2$, niin yhtälöllä $a^2 = 1$ on vain yksi ratkaisu $a = 1$, jolloin $Z(SL(2,K)) = \{I\}$.

Nyt lemman 1.37 nojalla $Z(SL(2,K)) \trianglelefteq SL(2,K)$, jolloin voidaan muodostaa tekijäryhmä, joka on kolmas määriteltävistä lineaarisista ryhmistä.

Määritelmä 2.8. Joukko

$$PSL(2,K) = SL(2,K)/Z(SL(2,K))$$

on *projektiivinen erityinen lineaarinen ryhmä astetta 2 kunnan K suhteen.*

Huomautus 2.9. Jos *char* $K \neq 2$, niin huomautuksien 1.19 ja 2.7 nojalla saadaan

$$|PSL(2,K)| = \frac{1}{2}|SL(2,K)| = \frac{1}{2}(q-1)q(q+1)$$

ja jos *char* $K = 2$

$$|PSL(2,K)| = |SL(2,K)| = (q-1)q(q+1).$$

3 Ryhmän $PSL(2, K)$ yksinkertaisuudesta

Seuraavaksi siirrytään tutkielman varsinaiseen ydiasiaan ja täällä esitettävät lauseet käsitellään tarkasti todistuksineen. Aloitetaan ensin tutkimalla yksittäisiä tapauksia $PSL(2, K)$ ryhmistä, jonka jälkeen siirytään yleisen tapauksen käsittelyyn.

3.1 Ryhmä $PSL(2, 2)$

Tutkitaan ensimmäisenä yksinkertaisin tapaus eli $PSL(2, 2)$.

Lause 3.1. *Ryhmä $PSL(2, 2)$ ei ole yksinkertainen.*

Todistus. Nyt *char* $\mathbb{Z}_2 = 2$, jolloin huomautuksen 2.7 nojalla $PSL(2, 2) = SL(2, 2)$. Riittää siis osoittaa, että $SL(2, 2)$ ei ole yksinkertainen, eli löydetään jokin ei triviaali normaali aliryhmä N. Lisäksi tiedetään, että

$$|SL(2, 2)| = (q - 1)q(q + 1) = (2 - 1)2(2 + 1) = 6.$$

Esitetään ryhmä $SL(2, 2)$ kokonaisuudessaan,

$$SL(2,2) = \{\overset{I}{\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}}, \overset{A}{\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}}, \overset{B}{\begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix}}, \overset{C}{\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}}, \overset{D}{\begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix}}, \overset{D^2}{\begin{pmatrix}0 & 1\\ 1 & 1\end{pmatrix}}\}.$$

Nyt alkion D generoima syklinen aliryhmä on määritelmän 1.11 nojalla

$$\langle D\rangle = \{I, D, D^2\},$$

ja $|\langle D\rangle| = 3$, jolloin

$$\frac{|SL(2, 2)|}{|\langle D\rangle|} = 2.$$

Siten huomautuksen 1.19 nojalla tiedetään, että $\langle D\rangle \trianglelefteq SL(2, 2)$, joka on selvästi ei triviaali normaali alisyhmä. Näin ollen $SL(2, 2) = PSL(2, 2)$ ei ole yksinkertainen.

□

3.2 Ryhmä $PSL(2, 3)$

Tutkitaan seuraavaksi ryhmän $PSL(2, 3)$ yksinkertaisuutta konjugointiluokkien tarkastelun avulla.

Lause 3.2. *Ryhmä $PSL(2,3)$ ei ole yksinkertainen.*

Todistus. Nyt $PSL(2,3) = SL(2,3)/Z(SL(2,3))$ ja huomautuksen 2.7 nojalla $Z(SL(2,3)) = \{I, -I\}$. Nyt lauseen 1.17 nojalla riittää, että löydetään ryhmästä $SL(2,3)$ aito normaali aliryhmä N, joka sisältää muutakin, kuin ryhmän $Z(SL(2,3)) = \{I, -I\}$. Lisäksi tiedetään lemman 2.5 nojalla, että

$$|SL(2,3)| = (3+1)3(3-1) = 24.$$

Nyt muodostetaan kolme tarpeellista osajoukkoa:

$$\begin{aligned}
&K_1 = \{I\},\\
&K_2 = \{-I\},\\
&K_3 = \{A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},\ A^{-1} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},\ B = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix},\\
&\quad B^{-1} = \begin{pmatrix} -1 & -1 \\ -1 & 1 \end{pmatrix},\ C = \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix},\ C^{-1} = \begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix}\}.
\end{aligned}$$

Selvästi joukot K_1 ja K_2 ovat konjugointiluokkia. Vielä on tarkasteltava onko joukko K_3 konjugointiluokka. Nyt $A^2 = B^2 = C^2 = -I$ ja $A^4 = B^4 = C^4 = I$ eli alkioiden A, B ja C kertaluku on sama, joten huomautuksen 1.39 nojalla ne voivat olla samassa konjugointiluokassa. Vastaavasti $(A^{-1})^2 = (B^{-1})^2 = (C^{-1})^2 = -I$ ja $(A^{-1})^4 = (B^{-1})^4 = (C^{-1})^4 = I$ eli alkioiden A^{-1}, B^{-1} ja C^{-1} kertaluku on myös neljä.

Lisäksi joukko $SL(2,3)$ sisältää alkiot

$$D = \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix},\ D^5 = \begin{pmatrix} -1 & -1 \\ 0 & -1 \end{pmatrix},\ E = \begin{pmatrix} -1 & 0 \\ 1 & -1 \end{pmatrix},\ E^5 = \begin{pmatrix} -1 & 0 \\ -1 & -1 \end{pmatrix},$$
$$F = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix},\ F^5 = \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix},\ G = \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix} \text{ ja } G^5 = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix},$$

joiden kertaluku on 6, sillä

$$\begin{aligned}
D^2 &= \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix}^2 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},\\
D^3 &= \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix} = -I,\\
D^4 &= -I\begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix},\\
D^5 &= \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} -1 & -1 \\ 0 & -1 \end{pmatrix} = D^{-1},\\
D^6 &= \begin{pmatrix} -1 & -1 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix} = I
\end{aligned}$$

ja vastaavasti voidaan osoittaa muiden kertalukua kuusi olevien alkioiden kertaluku. Näiden lisäksi joukko $SL(2,3)$ sisältää vielä alkiot

$$D^2 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, D^4 = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}, E^2 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, E^4 = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix},$$
$$F^2 = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}, F^4 = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}, G^2 = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix} \text{ ja } G^4 = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix},$$

joiden kertaluku on 3, sillä

$$(D^2)^2 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^2 = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix},$$
$$(D^2)^3 = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = I$$

ja vastaavasti voidaan osoittaa muiden kertalukua kolme olevien alkioiden kertaluku. Näin ollen huomautuksen 1.39 nojalla vain alkiot A, A^{-1}, B, B^{-1}, C ja C^{-1} voivat olla keskenään samassa konjugointiluokassa.

Lasketaan vielä lauseen 1.38 nojalla alkion $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ generoiman konjugointiluokan kertaluku:

$$\frac{|SL(2,3)|}{|C_{SL(2,3)}(A)|}.$$

Nyt täytyy siis selvittää alkion A sentralisoijan kertaluku ryhmässä $SL(2,3)$.

Määritelmän 1.36 nojalla

$$C_{SL(2,3)}(A) = \{S \in SL(2,3) \mid SA = AS\},$$

joten täytyy selvittää millä matriiseilla S toteutuu yhtälö:

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

eli

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

Näin ollen

$$a = d \text{ ja } b = -c$$

eli

$$S = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}.$$

Nyt yhtälölle $\det S = a^2 + b^2 = 1$ on neljä ratkaisua kunnassa $\mathbb{Z}_3$, jos $a = 0$, niin $b = 1$ tai -1 ja jos $b = 0$, niin $a = 1$ tai -1.

Tämän nojalla $|C_{SL(2,3)}(A)| = 4$, joten

$$\frac{|SL(2,3)|}{|C_{SL(2,3)}(A)|} = \frac{24}{4} = 6.$$

Eli edellä esitetty osajoukko K_3, joka sisälsi kuusi alkiota, on todellakin konjugointiluokka.

Olkoon konjugointiluokkien K_1, K_2 ja K_3 unioni N. Osoitetaan siis vielä, että $N \leq SL(2,3)$, jolloin tiedetään lemman 1.35 nojalla, että $N \trianglelefteq SL(2,3)$. Selvästi $IS = SI \in N$ ja $-IS = S(-I) \in N$ aina, kun $S \in N$. Lisäksi $AB = C$, $AC = B^{-1}$, $AB^{-1} = C^{-1}$, $AC^{-1} = B$, $BC = A$, $BA^{-1} = C$, $BC^{-1} = A^{-1}$, $CA^{-1} = B^{-1}$, $CB^{-1} = A$, $A^{-1}B^{-1} = C$, $A^{-1}C^{-1} = B^{-1}$ ja $B^{-1}C^{-1} = A$, joita operoimalla oikealta tai vasemmalta joukon K_3 alkioilla nähdään, että $ST \in N$ aina, kun $S,\ T \in N$.

Siten N on aliryhmäkriteerin, lauseen 1.8, nojalla ryhmän $SL(2,3)$ aliryhmä. Lisäksi se on konjugointiluokkien unionina normaali aliryhmä lemman 1.35 nojalla. Näin ollen aliryhmä N sisältää muutakin, kuin aliryhmän $Z(SL(2,3)) = \{I, -I\}$. Siten lauseen 1.17 nojalla tiedetään, että ryhmä $SL(2,3)$ ei ole yksinkertainen.

□

3.3 Ryhmä $PSL(2,4)$

Seuraavaksi käsitellään ryhmää $PSL(2,4)$ ja tämän yksinkertaisuuden käsittely alkaa samalla menetelmällä kuin lause 3.2 eli jakamalla aluksi ryhmä konjugointiluokkiin. Mutta koska ryhmä $PSL(2,4)$ osoitetaan yksinkertaiseksi, tullaan lopussa edellisestä poiketen osoittamaan, ettei konjugointiluokkien unionina saada muodostettua sopivaa aliryhmää ja tämän avulla ryhmä voidaan todeta yksinkertaiseksi. Ryhmässä $PSL(2,4)$ on 60 alkiota, joten näitä ei luetella, vaan konjugointiluokat muodostetaan niitä edustavan alkion avulla.

Esitetään aluksi neljän alkion kunta ja alkioiden väliset operaatiot, sillä nämä eivät ole aivan yhtä itsestäänselvät, kuin alkuluvun jäännösluokista muodostettavalla kunnalla.

Huomautus 3.3. Olkoon $(K, +, \cdot) = (\{0, 1, \alpha, \beta\}, +, \cdot)$ kunta. Nyt alkioiden väliset operaatiot voidaan taulukoida seuraavasti:

$+$	0	1	α	β
0	0	1	α	β
1	1	0	β	α
α	α	β	0	1
β	β	α	1	0

$\cdot$	0	1	α	β
0	0	0	0	0
1	0	1	α	β
α	0	α	β	1
β	0	β	1	α

Taulukko 1: Nelialkioisen kunnan yhteen- ja kertolaskuoperaatiot

Lisäksi huomataan, että $\alpha^3 = \beta^3 = 1$, sillä $|K\backslash\{0\}| = 3$, ja kaikkien alkioiden vasta-alkioita ovat alkiot itse, eli $-k = k$ aina, kun $k \in K$, sillä $char\ K = 2$.

Nyt voidaan siirtyä varsinaisen yksinkertaisuuden tarkastelun pariin ja kuntana toimii edellä esitetty neljän alkion kunta. Alla esitettävässä todistuksessa tätä kuntaa merkitään kirjaimella K lukemisen helpottamiseksi.

Lause 3.4. *Ryhmä $PSL(2, 4)$ on yksinkertainen.*

Todistus. Nyt $charK = 2$, sillä $|K| = 2^2$, jolloin huomautuksen 2.7 nojalla $PSL(2, 4) = SL(2, 4)$. Riittää siis osoittaa, että $SL(2, 4)$ on yksinkertainen, eli ryhmän $SL(2, 4)$ ainoat normaalit aliryhmät ovat $\{I\}$ ja $SL(2, 4)$. Lisäksi tiedetään lemman 2.5 nojalla, että

$$|SL(2, 4)| = (q - 1)q(q + 1) = 3 \cdot 4 \cdot 5 = 60.$$

Merkataan todistuksessa jatkossa ryhmää $SL(2, 4)$ kirjaimella G. Lähdetään nyt muodostamaan ryhmän G konjugointiluokkia. Selvästi $K_1 = \{I\}$ on oma yhden alkion konjugointiluokkansa.

Tarkastellaan seuraavaksi matriisin $S = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, joka selvästi kuuluu ryhmään G, generoimaa konjugointiluokkaa K_2. Nyt lauseen 1.38 nojalla tiedetään, että konjugointiluokan K_2 kertaluku on

$$|K_2| = \frac{|G|}{|C_G(\{S\})|}.$$

Täytyy siis selvittää $|C_G(\{S\})|$, joten tutkitaan joukkoa $C_G(\{S\})$. Tämä on määritelmän 1.36 nojalla

$$C_G(\{S\}) = \{g \in G \mid gS = Sg\}.$$

Olkoon nyt $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$. Nyt täytyy sevittää millä matriiseilla A toteutuu yhtälö:

$$\begin{aligned} & AS = SA \\ \Leftrightarrow \; & \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \\ \Leftrightarrow \; & \begin{pmatrix} b & a \\ d & c \end{pmatrix} = \begin{pmatrix} c & d \\ a & b \end{pmatrix}. \end{aligned}$$

Näin ollen

$$a = d \text{ ja } b = c$$

eli

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

Nyt determinantin avulla saadaan yhtälö

$$\det A = a^2 - b^2 = a^2 + b^2 = 1,$$

joka toteutuu kunnassa K, kun $a = 1$ ja $b = 0$, $a = 0$ ja $b = 1$, $a = \alpha$ ja $b = \beta$ tai $a = \beta$ ja $b = \alpha$. Eli matriisille A on neljä eri vaihtoehtoa, jolloin alkion S generoiman konjugointiluokan kertaluku on

$$|K_2| = \frac{|G|}{|C_G(\{S\})|} = \frac{60}{4} = 15.$$

Olkoon nyt $\omega \in K \backslash \{0, 1\}$ jolloin selvästi $\omega^3 = 1$, ja lisäksi $\omega^2 = \omega + 1 = \omega^{-1}$. Tarkastellaan seuraavaksi matriisin $T = \begin{pmatrix} \omega & 0 \\ 0 & \omega^2 \end{pmatrix}$, joka myös selvästi kuuluu ryhmään G, generoimaa konjugointiluokkaa K_3. Käyttämällä taas lausetta 1.38 tiedetään, että konjugointiluokan K_3 kertaluku on

$$|K_3| = \frac{|G|}{|C_G(\{T\})|}.$$

Tutkitaan siis, kuten edellä, mitkä matriisit $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$ toteuttavat yhtälön:

$$\begin{aligned} & AT = TA \\ \Leftrightarrow \; & \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \omega & 0 \\ 0 & \omega^2 \end{pmatrix} = \begin{pmatrix} \omega & 0 \\ 0 & \omega^2 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \\ \Leftrightarrow \; & \begin{pmatrix} a\omega & b\omega^2 \\ c\omega & d\omega^2 \end{pmatrix} = \begin{pmatrix} a\omega & b\omega \\ c\omega^2 & d\omega^2 \end{pmatrix}. \end{aligned}$$

Näin ollen

$$b\omega^2 = b\omega \text{ ja } c\omega = c\omega^2$$

eli

$$b\omega = b \text{ ja } c\omega = c,$$

josta alkion ω valinnan nojalla saadaan

$$b = 0 \text{ ja } c = 0$$

eli

$$A = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}.$$

Nyt determinantin avulla saadaan yhtälö

$$\det A = ad = 1,$$

joka toteutuu kunnassa K, kun $a = 1$ ja $d = 1$, $a = \alpha$ ja $d = \beta$ tai $a = \beta$ ja $d = \alpha$. Eli matriisille A on kolme eri vaihtoehtoa, jolloin alkion T generoiman konjugointiluokan kertaluku on

$$|K_3| = \frac{|G|}{|C_G(\{T\})|} = \frac{60}{3} = 20.$$

Määritellään vielä matriisi $R = \begin{pmatrix} 1 & \omega \\ \omega & \omega \end{pmatrix}$, joka myös selvästi kuuluu joukkoon G, sillä $\det R = \omega - \omega^2 = \omega + \omega^2 = \omega + \omega + 1 = 1$ suoraan alkion ω

määritelmän nojalla. Nyt matriisin R generoiman konjugointiluokan K_4 kertaluku on

$$|K_4| = \frac{|G|}{|C_G(\{R\})|}.$$

Selvitetään, kuten edellä, mitkä matriisit $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$ toteuttavat yhtälön:

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

Näin ollen

$$\begin{aligned} a + b\omega &= a + c\omega, \\ \Leftrightarrow b &= c. \end{aligned}$$

Tällöin toteutuu myös ehto

$$c\omega + d\omega = b\omega + d\omega.$$

Lisäksi on oltava voimassa ehto

$$a\omega + b\omega = b + d\omega.$$

Määritellään nyt alkioille a ja d rajoitteet eri alkion b arvoilla käyttäen yhtälöä $a\omega + b\omega = b + d\omega$ ja determinanttia $\det A = ad + b^2 = 1$.

1. Olkoon ensin $b = \omega$. Sijoittamalla tämä yhtälöön $a\omega + b\omega = b + d\omega$, saadaan

$$\begin{aligned} & a\omega + \omega^2 = \omega + d\omega \\ \Leftrightarrow\ & a\omega + d\omega = \omega + \omega^2 \\ \Leftrightarrow\ & a\omega + d\omega = \omega + \omega + 1 \\ \Leftrightarrow\ & \omega(a + d) = 1 \\ \Leftrightarrow\ & a + d = \omega^{-1} \\ \Leftrightarrow\ & d = \omega^{-1} + a, \end{aligned}$$

jolloin determinantin nojalla saadaan

$$\begin{aligned} & ad + \omega^2 = 1 \\ \Leftrightarrow\ & a(\omega^{-1} + a) = 1 + \omega^2 \\ \Leftrightarrow\ & a(\omega + 1 + a) = \omega \\ \Leftrightarrow\ & a\omega + a + a^2 = \omega. \end{aligned}$$

Tälle yhtälölle on ratkaisut $a = \omega$ ja $a = 1$, sillä

$$\begin{aligned} \omega\omega + \omega + \omega^2 &= \omega, \\ 1\omega + 1 + 1^2 &= \omega, \\ 0\omega + 0 + 0^2 &= 0 \neq \omega, \\ \omega^{-1}\omega + \omega^{-1} + (\omega^{-1})^2 &= 1 + \omega^{-1} + \omega \\ &= 1 + \omega + 1 + \omega \\ &= 0 \neq \omega. \end{aligned}$$

Näin ollen saadaan kaksi mahdollista matriisia A, kun $b = \omega$.

2. Tarkastellaan sitten tilanne $b = 0$. Yhtälön $a\omega + b\omega = b + d\omega$ nojalla saadaan

$$\begin{aligned} & a\omega = d\omega \\ \Leftrightarrow\ & a = d, \end{aligned}$$

jolloin determinantin nojalla saadaan $a^2 + b^2 = a^2 = 1$ eli $a = 1$. Siten matriisille A on yksi vaihtoehto, kun $b = 0$.

3. Tarkastellaan vielä tilanne $b = 1$. Yhtälön $a\omega + b\omega = b + d\omega$ nojalla saadaan

$$\begin{aligned} & a\omega + \omega = d\omega + 1 \\ \Leftrightarrow\ & a\omega + \omega + d\omega = 1 \\ \Leftrightarrow\ & \omega(a + d + 1) = 1 \\ \Leftrightarrow\ & a + d + 1 = \omega^{-1} \\ \Leftrightarrow\ & a + d = \omega^{-1} + 1 \\ \Leftrightarrow\ & a + d = \omega. \end{aligned}$$

Determinantin nojalla saadaan $ad + 1 = 1$ eli $ad = 0$. Nyt ehdot $a + d = \omega$ ja $ad = 0$ toteutuvat, kun $a = 0$ ja $d = \omega$ tai $d = 0$ ja $a = \omega$. Siten matriisille A on kaksi vaihtoehtoa, kun $b = 1$.

Edellä osoitettujen nojalla matriisille A on viisi eri vaihtoehtoa, joten alkion R generoiman konjugointiluokan kertaluku on

$$|K_4| = \frac{|G|}{|C_G(\{R\})|} = \frac{60}{5} = 12.$$

Lopuksi tarkastellaan vielä matriisin $W = \begin{pmatrix} \omega & 1 \\ 1 & 0 \end{pmatrix} \in G$ generoimaa konjugointiluokkaa K_5, jonka kertaluku on

$$|K_5| = \frac{|G|}{|C_G(\{W\})|}.$$

Kuten edellisten konjugointiluokkienkin kanssa, selvitetään taas, millä matriiseilla A toteutuu yhtälö:

$$\begin{aligned} & AW = WA \\ \Leftrightarrow\ & \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \omega & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} \omega & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \\ \Leftrightarrow\ & \begin{pmatrix} a\omega + b & a \\ c\omega + d & c \end{pmatrix} = \begin{pmatrix} a\omega + c & b\omega + d \\ a & b \end{pmatrix}. \end{aligned}$$

Näin ollen

$$b = c \text{ ja } a = b\omega + d.$$

Määritellään alkioille a ja d rajoitteet eri alkion b arvoilla käyttäen yhtälöä $a = b\omega + d$ ja determinanttia $\det A = ad + b^2 = 1$. Tämä on lähes vastaava, kuin konjugointiluokan K_4 kertaluvun määrittäminen, joten välivaiheita ei esitetä niin tarkasti.

1. Olkoon ensin $b = \omega$. Sijoittamalla tämä yhtälöön $a = b\omega + d$, saadaan

$$\begin{aligned} & a = \omega^2 + d \\ \Leftrightarrow\ & d = \omega^{-1} + a, \end{aligned}$$

jolloin determinantin nojalla saadaan

$$\begin{aligned} & ad + \omega^2 = 1 \\ \Leftrightarrow\ & a(\omega^{-1} + a) = 1 + \omega^2 \\ \Leftrightarrow\ & a\omega + a + a^2 = \omega. \end{aligned}$$

Kuten konjugointiluokan K_4 yhteydessä, tälle yhtälölle on ratkaisut $a = \omega$ ja $a = 1$. Näin ollen saadaan kaksi mahdollista matriisia A, kun $b = \omega$.

2. Tarkastellaan sitten tilanne $b = 0$. Yhtälön $a = b\omega + d$ nojalla saadaan $a = d$, jolloin determinantin nojalla saadaan $a^2 + b^2 = a^2 = 1$ eli $a = d = 1$. Näin ollen matriisille A on yksi vaihtoehto, kun $b = 0$.

3. Tarkastellaan vielä tilanne $b = 1$. Yhtälön $a = b\omega + d$ nojalla saadaan $a + d = \omega$ ja determinantin nojalla saadaan $ad + 1 = 1$ eli $ad = 0$. Kuten konjugointiluokan K_4 yhteydessä, nämä toteutuvat, kun $a = 0$ ja $d = \omega$ tai $d = 0$ ja $a = \omega$. Siten matriisille A on kaksi vaihtoehtoa, kun $b = 1$.

Siten saadaan matriisille A viisi eri vaihtoehtoa, joten alkion W generoiman konjugointiluokan kertaluku on

$$|K_5| = \frac{|G|}{|C_G(\{W\})|} = \frac{60}{5} = 12.$$

Osoitetaan vielä, että $K_4 \neq K_5$. Tähän riittää, että alkiot R ja W eivät konjugoi keskenään. Tutkitaan siis millä matriiseilla $A \in G$ toteutuu yhtälö

$$\begin{aligned} & A^{-1}RA = W \\ \Leftrightarrow\ & RA = AW \\ \Leftrightarrow\ & \begin{pmatrix} 1 & \omega \\ \omega & \omega \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \omega & 1 \\ 1 & 0 \end{pmatrix} \\ \Leftrightarrow\ & \begin{pmatrix} a + c\omega & b + d\omega \\ a\omega + c\omega & b\omega + d\omega \end{pmatrix} = \begin{pmatrix} a\omega + b & a \\ c\omega + d & c \end{pmatrix}. \end{aligned}$$

Tästä saadaan muodostettua yhtälöryhmä

$$\begin{cases} a + c\omega = a\omega + b \\ b + d\omega = a \\ a\omega + c\omega = c\omega + d \\ b\omega + d\omega = c, \end{cases}$$

josta kolmannesta yhtälöstä saadaan $a\omega = d$. Kun toinen yhtälö sijoitetaan ensimmäiseen yhtälöön, saadaan

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

Nyt sijoittamalla tämä yhtälöön $a\omega = d$, saadaan yhtälö

$$d\omega + c\omega = d,$$

johon sijoittamalla yhtälöryhmän neljäs yhtälö, saadaan

$$\begin{aligned} & d = d\omega + \omega(b\omega + d\omega) \\ \Leftrightarrow\ & d = d\omega + d\omega^2 + b\omega^2 \\ \Leftrightarrow\ & d = d(\omega + \omega^2) + b\omega^2 \\ \Leftrightarrow\ & d = d(\omega + \omega + 1) + b\omega^2 \\ \Leftrightarrow\ & d = d + b\omega^2 \\ \Leftrightarrow\ & b\omega^2 = 0 \\ \Leftrightarrow\ & b = 0. \end{aligned}$$

Sijoittamalla tämä yhtälöryhmän neljänteen yhtälöön, saadaan $c = d\omega$. Sijoittamalla tämä ja $b = 0$ toiseen yhtälöön, saadaan $c = a$. Sijoittamalla vielä nämä yhtälöryhmän ensimmäiseen yhtälöön, saadaan

$$\begin{aligned} & a + a\omega = a\omega \\ \Leftrightarrow\ & a = 0. \end{aligned}$$

Näin ollen $A = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, mutta nyt $\det A = 0$ eli $A \notin G$, joten $K_4 \neq K_5$.

Nyt on muodostettu konjugointiluokat, joiden kertaluvut ovat

$$\begin{aligned} |K_1| &= 1, \\ |K_2| &= 15, \\ |K_3| &= 20, \\ |K_4| &= 12, \\ |K_5| &= 12. \end{aligned}$$

Näiden alkioiden summa on $60 = |SL(2,4)|$, joten tässä täytyy olla kaikkien konjugointiluokkien, sillä konjugointiluokat ovat määritelmän 1.34 nojalla pistevieraita. Nyt konjugointiluokista ei pystytä muodostamaan sellaista unionia, että se sisältäisi konjugointiluokan $K_1 = \{I\}$ ja unionin kertaluku jakaisi luvun 60, mutta ei ole kaikkien konjugointiluokkien unioni tai pelkkä K_1. Siis konjugointiluokkien unionina ei voida muodostaa muita aliryhmiä, kuin $\{I\}$ ja $SL(2,4)$, joten lemman 1.35 nojalla ryhmällä $SL(2,4) = PSL(2,4)$ on pelkät triviaalit normaalti aliryhmät. Näin ollen ryhmä $PSL(2,4)$ on yksinkertainen. □

3.4 Ryhmä $PSL(2,5)$

Ryhmän $PSL(2,5)$ yksinkertaisuuden osoitus on hyvin saman kaltainen, kuin ryhmän $PSL(2,4)$, mutta ryhmän suuremmasta koosta johtuen hiukan laajempi. Todistus vaatisi usean samankaltaisen konjugointiluokan kertaluvun osoittamisen, sekä usean osoituksen siitä, että tietyt alkiot eivät konjugoi keskenään. Näitä ei kuitenkaan kaikkia kirjoiteta auki, vaan todistuksessa muutamat kohdat todetaan keskenään saman kaltaisiksi. Kunnan $\mathbb{Z}_5$ alkioita käsiteltäessä on hyvä muistaa, että $-1 = 4$.

Lause 3.5. *Ryhmä $PSL(2,5)$ on yksinkertainen.*

Todistus. Nyt $char\mathbb{Z}_5 \neq 2$, jolloin määritelmän 2.8 nojalla $PSL(2,5) = SL(2,5)/Z(SL(2,5))$. Nyt lauseen 1.17 nojalla ryhmän $PSL(2,5)$ yksinkertaisuuden osoittamiseen riittää, että ryhmän $SL(2,5)$ ainoat normaalit aliryhmät ovat $\{I\}$, $\{I,-I\}$ ja $SL(2,4)$. Lisäksi tiedetään lemman 2.5 nojalla, että

$$|SL(2,5)| = (q-1)q(q+1) = 4 \cdot 5 \cdot 6 = 120.$$

Merkataan todistuksessa jatkossa ryhmää $SL(2,5)$ kirjaimella G lukemisen helpottamiseksi.

Lähdetään nyt muodostamaan ryhmän G konjugointiluokkia. Selvästi $K_1 = \{I\}$ ja $K_2 = \{-I\}$ ovat yhden alkion konjugointiluokkia. Tutkitaan seuraavaksi alkion $T = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in G$ generoimaa konjugointiluokkaa K_3. Kuten lauseen 3.4 todistuksessa, tutkitaan konjugointiluokan kertalukua lauseen 1.38 nojalla, jolloin

$$|K_3| = \frac{|G|}{|C_G(\{T\})|}.$$

Täytyy selvittää $|C_G(\{T\})|$, joten tutkitaan joukkoa $C_G(\{T\})$. Tämä on määritelmän 1.36 nojalla

$$C_G(\{T\}) = \{g \in G \mid gT = Tg\}.$$

Olkoon nyt $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$. Nyt täytyy sevittää millä matriiseilla A toteutuu yhtälö:

$$\begin{aligned} & AT = TA \\ \Leftrightarrow \quad & \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \\ \Leftrightarrow \quad & \begin{pmatrix} b & -a \\ d & -c \end{pmatrix} = \begin{pmatrix} -c & -d \\ a & b \end{pmatrix}. \end{aligned}$$

Näin ollen

$$a = d \text{ ja } c = -b$$

eli

$$A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}.$$

Nyt determinantin avulla saadaan yhtälö

$$\det A = a^2 + b^2 = 1.$$

Taulukoidaan yhtälön $a^2 + b^2 = 1$ ratkaisut kunnassa $\mathbb{Z}_5$.

a	b	$a^2 + b^2$
0	1	1
0	-1	1
1	0	1
-1	0	1

Taulukko 2: Yhtälön $a^2 + b^2 = 1$ ratkaisuparit (a, b) kunnassa $\mathbb{Z}_5$.

Selvästi nähdään, että nämä ovat ainoat ratkaisuparit kunnassa $\mathbb{Z}_5$, sillä kunnassa $\mathbb{Z}_5$ ainoita neliöitä ovat 0, 1 ja $-1(= 2^2 = 3^2)$. Eli matriisille A on neljä eri vaihtoehtoa. Näin ollen alkion T generoiman konjugointiluokan kertaluku on

$$|K_3| = \frac{|G|}{|C_G(\{T\})|} = \frac{120}{4} = 30.$$

Tutkitaan seuraavaksi matriisin $S = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} \in G$ generoimaa konjugointiluokkaa K_4. Nyt konjugointiluokan K_4 kertaluku saadaan taas yhtälöstä

$$|K_4| = \frac{|G|}{|C_G(\{S\})|},$$

jota varten täytyy selvittää $|C_G(\{S\})|$. Kuten edellä, määritelmän 1.36 nojalla

$$C_G(\{S\}) = \{g \in G \mid gS = Sg\}.$$

Olkoon nyt $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$. Kuten edellä, täytyy selvittää millä matriiseilla A toteutuu yhtälö:

$$\begin{aligned} & AS = SA \\ \Leftrightarrow \; & \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \\ \Leftrightarrow \; & \begin{pmatrix} -b & a-b \\ -d & c-d \end{pmatrix} = \begin{pmatrix} c & d \\ -a-c & -b-d \end{pmatrix}. \end{aligned}$$

Näin ollen

$$c = -b \text{ ja } d = a - b$$

eli

$$A = \begin{pmatrix} a & b \\ -b & a-b \end{pmatrix}.$$

Nyt determinantin nojalla saadaan yhtälö

$$\det A = a^2 - ab + b^2 = 1.$$

Selkeyden vuoksi taulukoidaan lausekkeen $a^2 - ab + b^2$ arvot alkiopareilla (a, b) kunnassa $\mathbb{Z}_5$.

a	b	a^2-ab+b^2	a	b	a^2-ab+b^2	a	b	a^2-ab+b^2
0	1	1	0	0	0	−1	1	3
0	−1	1	0	2	−1	−1	2	2
1	0	1	0	3	−1	−1	3	3
1	1	1	1	−1	3	2	2	−1
−1	−1	1	1	2	3	2	3	2
−1	0	1	1	3	2	3	3	−1

Taulukko 3: Lausekkeen $a^2 - ab + b^2$ arvot alkiopareilla (a, b) kunnassa $\mathbb{Z}_5$.

Taulukosta 3 nähdään, että ensimmäiset kuusi esitettyä paria (a, b) ovat yhtälön $a^2 - ab + b^2 = 1$ ratkaisupareja. Alkioparit (a, b), joita ei esiinny taulukossa 3, jätetään taulukoimatta, sillä yhtälön $a^2 - ab + b^2 = 1$ muodosta johtuen, (α, β) on yhtälön ratkaisupari, jos ja vain jos (β, α) on yhtälön ratkaisupari. Siten ensimmäiset kuusi ovat ainoat ratkaisuparit. Eli matriisille A

on kuusi eri vaihtoehtoa. Näin ollen alkion S generoiman konjugointiluokan kertaluku on

$$|K_4| = \frac{|G|}{|C_G(\{S\})|} = \frac{120}{6} = 20.$$

Nyt selvästi alkion $-S$ sentralisoija $C_G(\{-S\})$ on identtinen alkion S sentralisoijan kanssa, sillä

$$\begin{aligned} & A(-S) = -SA \\ \Leftrightarrow \; & \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \\ \Leftrightarrow \; & \begin{pmatrix} b & -a+b \\ d & -c+d \end{pmatrix} = \begin{pmatrix} -c & -d \\ a+c & b+d \end{pmatrix} \\ \Leftrightarrow \; & \begin{pmatrix} -b & a-b \\ -d & c-d \end{pmatrix} = \begin{pmatrix} c & d \\ -a-c & -b-d \end{pmatrix}. \end{aligned}$$

Näin ollen

$$c = -b \text{ ja } d = a - b$$

eli

$$A = \begin{pmatrix} a & b \\ -b & a-b \end{pmatrix}.$$

Näin ollen myös alkion $-S$ generoiman konjugointiluokan K_5 kertaluku $|K_5| = 20$. Osoitetaan vielä, että $K_5 \neq K_4$, joka on yhtäpitävää sen kanssa, että alkiot S ja $-S$ eivät konjugoi ryhmässä G. Tutkitaan siis millä alkiolla $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$ toteutuu

$$\begin{aligned} & A^{-1}SA = -S \\ \Leftrightarrow \; & SA = A(-S) \\ \Leftrightarrow \; & \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} \\ \Leftrightarrow \; & \begin{pmatrix} c & d \\ -a-c & -b-d \end{pmatrix} = \begin{pmatrix} b & -a+b \\ d & -c+d \end{pmatrix}. \end{aligned}$$

Tästä saadaan yhtälöryhmä

$$\begin{cases} b = c \\ d = -a + b \\ d = -a - c \\ -b - d = -c + d, \end{cases}$$

josta yhdistämällä keskimmäiset yhtälöt ja sijoittamalla ylin yhtälö alimpaan yhtälöön saadaan

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

Tästä edelleen sieventämällä kahta alinta yhtälöä saadaan

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

Näin ollen

$$\begin{cases} b = c = 0 \\ d = 0. \end{cases}$$

Nyt $A = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$, mutta tällöin $\det A = 0$ eli $A \notin G$. Näin ollen alkiot S ja $-S$ eivät konjugoi ryhmässä G, jolloin $K_5 \neq K_4$.

Tutkitaan seuraavaksi matriisin $R = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in G$ generoimaa konjugointiluokkaa K_6. Konjugointiluokan K_6 kertaluku saadaan, kuten edellä, yhtälöstä

$$|K_6| = \frac{|G|}{|C_G(\{R\})|},$$

jota varten täytyy selvittää $|C_G(\{R\})|$, missä

$$C_G(\{R\}) = \{g \in G \mid gR = Rg\}.$$

Olkoon nyt $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$. Selvitetään taas, millä matriiseilla A toteutuu yhtälö:

$$\begin{aligned} & AR = RA \\ \Leftrightarrow \; & \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \\ \Leftrightarrow \; & \begin{pmatrix} a & a+b \\ c & c+d \end{pmatrix} = \begin{pmatrix} a+c & b+d \\ c & d \end{pmatrix}. \end{aligned}$$

Näin ollen

$$\begin{aligned} a &= a + c \\ \Leftrightarrow c &= 0 \end{aligned}$$

ja

$$\begin{aligned} a + b &= b + d \\ \Leftrightarrow a &= d \end{aligned}$$

eli

$$A = \begin{pmatrix} a & b \\ 0 & a \end{pmatrix}.$$

Nyt determinantin nojalla saadaan yhtälö

$$\det A = a^2 = 1,$$

joka toteutuu kunnassa $\mathbb{Z}_5$, kun a on 1 tai -1. Lisäksi alkio b voidaan valita viidellä eri tavalla kunnassa $\mathbb{Z}_5$, jolloin matriisille A on $2 \cdot 5 = 10$ eri vaihtoehtoa. Näin ollen alkion R generoiman konjugointiluokan kertaluku on

$$|K_6| = \frac{|G|}{|C_G(\{R\})|} = \frac{120}{10} = 12.$$

Nyt, kuten alkioille S ja $-S$, voidaan osoittaa, että alkiot R ja $-R$ eivät konjugoi ja niiden generoimat konjugointiluokat ovat yhtä suuret. Selvästi alkion $-R$ sentralisoija $C_G(\{-R\})$ on identtinen alkion R sentralisoijan kanssa, sillä

$$
\begin{aligned}
& A(-R) = -RA \\
\Leftrightarrow\ & \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} -1 & -1 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} -1 & -1 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \\
\Leftrightarrow\ & \begin{pmatrix} -a & -a-b \\ -c & -c-d \end{pmatrix} = \begin{pmatrix} -a-c & -b-d \\ -c & -d \end{pmatrix}.
\end{aligned}
$$

Näin ollen

$$
\begin{aligned}
-a &= -a - c \\
\Leftrightarrow c &= 0
\end{aligned}
$$

ja

$$
\begin{aligned}
-a - b &= -b - d \\
\Leftrightarrow a &= d
\end{aligned}
$$

eli

$$
A = \begin{pmatrix} a & b \\ 0 & a \end{pmatrix}.
$$

Näin ollen myös alkion $-R$ generoiman konjugointiluokan K_7 kertaluku $|K_7| = 12$. Osoitetaan vielä, että $K_6 \neq K_7$, joka on yhtäpitävää sen kanssa, että alkiot R ja $-R$ eivät konjugoi ryhmässä G. Tutkitaan siis millä alkiolla $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$ toteutuu

$$
\begin{aligned}
& A^{-1}RA = -R \\
\Leftrightarrow\ & RA = A(-R) \\
\Leftrightarrow\ & \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} -1 & -1 \\ 0 & -1 \end{pmatrix} \\
\Leftrightarrow\ & \begin{pmatrix} a+c & b+d \\ c & d \end{pmatrix} = \begin{pmatrix} -a & -a-b \\ -c & -c-d \end{pmatrix}.
\end{aligned}
$$

Tästä saadaan yhtälöryhmä

$$
\begin{cases}
a + c = -a \\
b + d = -a - b \\
c = -c \\
d = -c - d,
\end{cases}
$$

jolloin kolmannesta yhtälöstä saadaan kunnassa $\mathbb{Z}_5$ ratkaisu $c = 0$ ja sijoittamalla tämä ensimmäiseen ja neljänteen yhtälöön, saadaan

$$\begin{cases} a = -a \\ b + d = -a - b \\ c = 0 \\ d = -d. \end{cases}$$

Nyt ylimmästä yhtälöstä saadaan $a = 0$ ja alimmasta yhtälöstä $d = 0$ ja sijoittamalla nämä toiseen yhtälöön, saadaan

$$\begin{cases} a = 0 \\ b = -b \\ c = 0 \\ d = 0. \end{cases}$$

Näin ollen

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

Siten $A = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, mutta tällöin $\det A = 0$ eli $A \notin G$. Näin ollen alkiot R ja $-R$ eivät konjugoi ryhmässä G, jolloin $K_6 \neq K_7$.

Tutkitaan vielä matriisin $R^2 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ generoimaa konjugointiluokkaa K_8. Konjugointiluokan K_8 kertaluku

$$|K_8| = \frac{|G|}{|C_G(\{R^2\})|},$$

jota varten täytyy taas selvittää $|C_G(\{R^2\})|$, missä

$$C_G(\{R^2\}) = \{g \in G \mid gR^2 = R^2 g\}.$$

Olkoon nyt $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$. Selvitetään taas, millä matriiseilla A toteutuu

yhtälö:

$$\begin{aligned} & AR^2 = R^2A \\ \Leftrightarrow \; & \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \\ \Leftrightarrow \; & \begin{pmatrix} a & 2a+b \\ c & 2c+d \end{pmatrix} = \begin{pmatrix} a+2c & b+2d \\ c & d \end{pmatrix}. \end{aligned}$$

Näin ollen

$$\begin{aligned} a &= a + 2c \\ \Leftrightarrow c &= 0 \end{aligned}$$

ja

$$\begin{aligned} 2a + b &= b + 2d \\ \Leftrightarrow a &= d \end{aligned}$$

eli

$$A = \begin{pmatrix} a & b \\ 0 & a \end{pmatrix}.$$

Nyt matriisille A saadaan identtiset ehdot, kuin alkion R konjugointiluokkaa tarkasteltaessa, jolloin matriisille A on taas 10 eri vaihtoehtoa. Näin ollen alkion R^2 generoiman konjugointiluokan kertaluku on

$$|K_8| = \frac{|G|}{|C_G(\{R^2\})|} = \frac{120}{10} = 12.$$

Osoitetaan vielä, että $K_8 \neq K_6$, joka on yhtäpitävää sen kanssa, että alkiot R ja R^2 eivät konjugoi ryhmässä G. Tutkitaan siis millä alkiolla $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$ toteutuu

$$\begin{aligned} & A^{-1}RA = R^2 \\ \Leftrightarrow \; & RA = AR^2 \\ \Leftrightarrow \; & \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \\ \Leftrightarrow \; & \begin{pmatrix} a+c & b+d \\ c & d \end{pmatrix} = \begin{pmatrix} a & 2a+b \\ c & 2c+d \end{pmatrix}. \end{aligned}$$

Näin ollen

$$\begin{aligned} & a = a + c \\ \Leftrightarrow\ & c = 0 \end{aligned}$$

ja

$$\begin{aligned} & 2a + b = b + d \\ \Leftrightarrow\ & 2a = d. \end{aligned}$$

Nyt $A = \begin{pmatrix} a & b \\ 0 & 2a \end{pmatrix}$, jolloin determinantti $\det A = 2a^2 = 1$, joka on kunnassa $\mathbb{Z}_5$ yhtäpitävää yhtälön $a^2 = 3$ kanssa. Kuitenkin aiemmin jo todettiin, että ainoat neliöt kunnassa $\mathbb{Z}_5$ ovat 0, 1 ja -1, joten yhtälöllä $a^2 = 3$ ei ole ratkaisua kunnassa $\mathbb{Z}_5$. Näin ollen alkiot R ja R^2 eivät konjugoi ryhmässä G, jolloin $K_8 \neq K_6$.

Vastaavasti voidaan osoittaa, että $-R$ ja R^2 eivät konjugoi ryhmässä G. Osoitetaan siis, että $K_8 \neq K_7$, joka on yhtäpitävää sen kanssa, että alkiot $-R$ ja R^2 eivät konjugoi ryhmässä G. Tutkitaan siis millä alkiolla $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$ toteutuu

$$\begin{aligned} & A^{-1}(-R)A = R^2 \\ \Leftrightarrow\ & -RA = AR^2 \\ \Leftrightarrow\ & \begin{pmatrix} -1 & -1 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \\ \Leftrightarrow\ & \begin{pmatrix} -a-c & -b-d \\ -c & -d \end{pmatrix} = \begin{pmatrix} a & 2a+b \\ c & 2c+d \end{pmatrix}. \end{aligned}$$

Tästä saadaan yhtälöryhmä

$$\begin{cases} -a - c = a \\ -b - d = 2a + b \\ -c = c \\ -d = 2c + d, \end{cases}$$

jolloin kolmannesta yhtälöstä saadaan kunnassa $\mathbb{Z}_5$ ratkaisu $c = 0$ ja sijoittamalla tämä ensimmäiseen ja neljänteen yhtälöön, saadaan

$$\begin{cases} a = -a \\ -b - d = 2a + b \\ c = 0 \\ d = -d. \end{cases}$$

Nyt ylimmästä yhtälöstä saadaan $a = 0$ ja alimmasta yhtälöstä $d = 0$ ja sijoittamalla nämä toiseen yhtälöön, saadaan

$$\begin{cases} a = 0 \\ b = -b \\ c = 0 \\ d = 0. \end{cases}$$

Näin ollen

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

Siten $A = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, mutta tällöin $\det A = 0$ eli $A \notin G$. Näin ollen alkiot $-R$ ja R^2 eivät konjugoi ryhmässä G, jolloin $K_8 \neq K_7$.

Lisäksi, kuten alkioille S ja $-S$ sekä R ja $-R$, voidaan osoittaa, että alkion $-R^2$ generoiman konjugointiluokan K_9 kertaluku on sama, kuin alkion R^2 generoiman konjugoiniluokan kertaluku. Tarkastellaan siis vielä matriisin $-R^2 = \begin{pmatrix} -1 & -2 \\ 0 & -1 \end{pmatrix}$ generoimaa konjugointiluokkaa K_9. Konjugointiluokan K_9 kertaluku

$$|K_9| = \frac{|G|}{|C_G(\{-R^2\})|},$$

jota varten täytyy taas selvittää $|C_G(\{-R^2\})|$, missä

$$C_G(\{-R^2\}) = \{g \in G \mid g(-R^2) = -R^2 g\}.$$

Olkoon nyt $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$. Selvitetään taas, millä matriiseilla A toteutuu yhtälö:

$$\begin{aligned} & A(-R^2) = -R^2 A \\ \Leftrightarrow \; & \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} -1 & -2 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} -1 & -2 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \\ \Leftrightarrow \; & \begin{pmatrix} -a & -2a-b \\ -c & -2c-d \end{pmatrix} = \begin{pmatrix} -a-2c & -b-2d \\ -c & -d \end{pmatrix}. \end{aligned}$$

Näin ollen

$$\begin{aligned} -a &= -a - 2c \\ \Leftrightarrow c &= 0 \end{aligned}$$

ja

$$\begin{aligned} -2a - b &= -b - 2d \\ \Leftrightarrow a &= d \end{aligned}$$

eli

$$A = \begin{pmatrix} a & b \\ 0 & a \end{pmatrix}.$$

Nyt matriisille A saadaan taas identtiset ehdot, kuin alkion R konjugointiluokkaa tarkasteltaessa, jolloin matriisille A on taas 10 eri vaihtoehtoa. Näin ollen alkion $-R^2$ generoiman konjugointiluokan kertaluku on

$$|K_9| = \frac{|G|}{|C_G(\{-R^2\})|} = \frac{120}{10} = 12.$$

Kuten edellä, täytyy vielä osoittaa, että alkio $-R^2$ ei konjugoi alkioiden R, $-R$ tai R^2 kanssa ryhmässä G. Osoitetaan aluksi, että $-R^2$ ei konjugoi alkion R kanssa ryhmässä G, joka on yhtäpitävää sen kanssa, että $K_9 \neq K_6$. Tutkitaan siis millä alkiolla $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$ toteutuu

$$\begin{aligned} & A^{-1}RA = -R^2 \\ \Leftrightarrow \; & RA = A(-R^2) \\ \Leftrightarrow \; & \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} -1 & -2 \\ 0 & -1 \end{pmatrix} \\ \Leftrightarrow \; & \begin{pmatrix} a+c & b+d \\ c & d \end{pmatrix} = \begin{pmatrix} -a & -2a-b \\ -c & -2c-d \end{pmatrix}. \end{aligned}$$

Tästä saadaan yhtälöryhmä

$$\begin{cases} a + c = -a \\ b + d = -2a - b \\ c = -c \\ d = -2c - d, \end{cases}$$

joka on yhtäpitävä seuraavan yhtälöryhmän kanssa.

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

Tämä on identtinen alkioiden $-R$ ja R^2 konjugointia tutkittaessa muodostuneen yhtälöryhmän kanssa. Näin ollen alkiot R ja $-R^2$ eivät konjugoi ryhmässä G, jolloin $K_9 \neq K_6$.

Tutkitaan sitten alkioiden $-R^2$ ja $-R$ konjugointia ryhmässä G. Tutkitaan siis millä alkiolla $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$ toteutuu

$$\begin{aligned} & A^{-1}(-R)A = -R^2 \\ \Leftrightarrow \quad & -RA = A(-R^2) \\ \Leftrightarrow \quad & \begin{pmatrix} -1 & -1 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} -1 & -2 \\ 0 & -1 \end{pmatrix} \\ \Leftrightarrow \quad & \begin{pmatrix} -a - c & -b - d \\ -c & -d \end{pmatrix} = \begin{pmatrix} -a & -2a - b \\ -c & -2c - d \end{pmatrix}, \end{aligned}$$

jota kertomalla puolittain alkiolla -1 saadaan

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

Tämä on identtinen alkioiden R ja R^2 konjugointia tutkittaessa muodostuneen yhtälöryhmän kanssa. Näin ollen alkiot $-R$ ja $-R^2$ eivät konjugoi ryhmässä G, jolloin $K_9 \neq K_7$.

Osoitetaan lopuksi, että alkiot $-R^2$ ja R^2 eivät konjugoi ryhmässä G eli $K_9 \neq K_8$. Nyt

$$
\begin{aligned}
& A^{-1}R^2A = -R^2 \\
\Leftrightarrow\ & R^2A = A(-R^2) \\
\Leftrightarrow\ & \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} -1 & -2 \\ 0 & -1 \end{pmatrix} \\
\Leftrightarrow\ & \begin{pmatrix} a+2c & b+2d \\ c & d \end{pmatrix} = \begin{pmatrix} -a & -2a-b \\ -c & -2c-d \end{pmatrix}.
\end{aligned}
$$

Tästä saadaan muodostettua yhtälöryhmä

$$
\begin{cases}
a + 2c = -a \\
b + 2d = -2a - b \\
c = -c \\
d = -2c - d,
\end{cases}
$$

jolloin kolmannesta yhtälöstä saadaan taas $c = 0$ ja sijoittamalla tämä ensimmäiseen ja neljänteen yhtälöön, saadaan

$$
\begin{cases}
a = -a \\
b + 2d = -2a - b \\
c = 0 \\
d = -d.
\end{cases}
$$

Nyt ylimmästä yhtälöstä saadaan $a = 0$ ja alimmasta yhtälöstä $d = 0$ ja sijoittamalla nämä toiseen yhtälöön, saadaan

$$
\begin{cases}
a = 0 \\
b = -b \\
c = 0 \\
d = 0.
\end{cases}
$$

Näin ollen

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

Siten $A = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, mutta tällöin $\det A = 0$ eli $A \notin G$. Näin ollen alkiot $-R^2$ ja R^2 eivät konjugoi ryhmässä G, jolloin $K_9 \neq K_8$.

Nyt on muodostettu pistevieraat konjugointiluokat, jotka ovat kertalukuineen:

$$
\begin{aligned}
&K_1 = \{I\},\ |K_1| = 1;\\
&K_2 = \{-I\},\ |K_2| = 1;\\
&K_3 = \{\text{alkion } T \text{ generoima konjugointiluokka}\},\ |K_3| = 30;\\
&K_4 = \{\text{alkion } S \text{ generoima konjugointiluokka}\},\ |K_4| = 20;\\
&K_5 = \{\text{alkion } -S \text{ generoima konjugointiluokka}\},\ |K_5| = 20;\\
&K_6 = \{\text{alkion } R \text{ generoima konjugointiluokka}\},\ |K_6| = 12;\\
&K_7 = \{\text{alkion } -R \text{ generoima konjugointiluokka}\},\ |K_7| = 12;\\
&K_8 = \{\text{alkion } R^2 \text{ generoima konjugointiluokka}\},\ |K_8| = 12;\\
&K_9 = \{\text{alkion } -R^2 \text{ generoima konjugointiluokka}\},\ |K_9| = 12.
\end{aligned}
$$

Tässä täytyy olla kaikkien konjugointiluokkien, sillä näitä alkioita on kaikkiaan $120 = |G|$.

Olkoon nyt $N \trianglelefteq G$, joka sisältää muutakin kuin konjugointiluokat K_1 ja K_2. Nyt lemman 1.35 nojalla N on konjugointiluokkien unionina muodostettu aliryhmä ja lisäksi Lagrangen lauseen, lause 1.10, nojalla $|N|$ jakaa luvun $120 = |G|$. Näin ollen N ei voi jaollisuuden nojalla sisältää konjugointiluokkien K_1 ja K_2 lisäksi luokkaa K_3, K_4 tai K_5 ilman, että $N = G$.

Olkoon nyt N joukko, joka sisältää konjugointiluokat K_1 ja K_2 sekä jonkun konjugointiluokista K_6, K_7, K_8 tai K_9. Tällöin aliryhmänä joukko N sisältää kaikki konjugointiluokat K_6, K_7, K_8 ja K_9. Siten aliryhmä N sisältää vähintään $2 + 4 \cdot 12 = 50$ alkiota ja koska tämä ei jaa lukua 120, täytyy lisätä vielä jokin konjugointiluokista K_3, K_4 tai K_5, jolloin $N = G$.

Näin ollen ryhmän $G = SL(2,5)$ ainoat normaalit aliryhmät ovat $\{I\}$, $\{I, -I\}$ ja $SL(2,4)$, jolloin lauseen 1.17 nojalla ryhmä $PSL(2,5)$ on yksinkertainen.

□

3.5 Ryhmä $PSL(2,K)$

Lopuksi tutkitaan vielä yleisesti ryhmän $PSL(2,K)$ yksinkertaisuutta. Ennen ryhmän $PSL(2,K)$ yksinkertaisuuden varsinaista tutkimista tarvitaan

kuitenkin vielä yksi uusi määritelmä ja kolme hyödyllistä lemmaa. Ensimmäisenä tutkitaan yhtälön $x^2 - y^2 = a$ ratkeamista kunnassa K.

Lemma 3.6. *Olkoon K äärellinen kunta ja $a \in K$. Tällöin yhtälöllä $x^2 - y^2 = a$ on ratkaisupari (x, y) kunnassa K.*

Todistus. Tarkastellaan erikseen tapaukset *char* $K \neq 2$ ja *char* $K = 2$.

1. Olkoon *char* $K \neq 2$. Nyt seuraava yhtäpitävyys on voimassa:

$$\begin{aligned} & x^2 - y^2 = a \\ \Leftrightarrow\ & (x - y)(x + y) = a. \end{aligned}$$

Tälle voidaan muodostaa yksi mahdollinen ratkaisuvaihtoehto

$$\begin{cases} x - y = 1 \\ x + y = a, \end{cases}$$

jotka laskemalla puolittain yhteen, saadaan

$$x + x = a + 1.$$

Nyt, koska *char* $K \neq 2$, niin $x+x \neq 0$, jos $x \neq 0$. Näin ollen on olemassa alkio $k \in K\backslash\{0\}$, jolle pätee $kx = x + x$. Tällöin myös $k^{-1} \in K\backslash\{0\}$, jolloin saadaan

$$\begin{aligned} & kx = a + 1 \\ \Leftrightarrow\ & x = k^{-1}(a + 1). \end{aligned}$$

Kun tämä sijoitetaan yhtälöparin ylempään yhtälöön, saadaan

$$y = k^{-1}(a + 1) - 1,$$

josta muokkaamalla alkiota 1 saadaan

$$y = k^{-1}(a + 1) - k^{-1}k,$$

eli

$$y = k^{-1}(a + 1 - k).$$

Näin ollen saadaan yhtälölle $x^2 - y^2 = a$ ratkaisupari

$$\begin{cases} x = k^{-1}(a + 1) \in K \\ y = k^{-1}(a + 1 - k) \in K. \end{cases}$$

2. Olkoon *char* $K = 2$. Tällöin $|K| = 2^n$ ja $|K\backslash\{0\}| = 2^n - 1$. Tarkastellaan yhtälöä $x^2 - y^2 = a$.

   Jos $a = 0$ saadaan ratkaisuvaihtoehto $x = y = 0$.

   Tutkitaan seuraavaksi tilanne $a \in K\backslash\{0\}$, jolloin $1 = a^{2^n-1}$. Kertomalla tämä puolittain alkiolla a, saadaan

$$a = a^{2^n} = a^{2\cdot 2^{n-1}} = (a^{2^{n-1}})^2.$$

   Nyt voidaan valita $x = a^{2^{n-1}} \in K$ ja $y = 0 \in K$, joka on yhtälön $x^2 - y^2 = a$ ratkaisu.

Näin ollen yhtälöllä $x^2 - y^2 = a$ on aina ratkaisupari (x, y) kunnassa K. □

Määritellään vielä transvektiot, joiden avulla yksinkertaisuuden osoittaminen helpottuu huomattavasti.

Määritelmä 3.7. Alkioita $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \in SL(2, K)$ ja $\begin{pmatrix} 1 & 0 \\ y & 1 \end{pmatrix} \in SL(2, K)$ kutsutaan *transvektioiksi*.

Huomautus 3.8. Nyt

$$\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & -x \\ 0 & 1 \end{pmatrix} \text{ ja } \begin{pmatrix} 1 & 0 \\ y & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 0 \\ -y & 1 \end{pmatrix},$$

joten transvektioiden käänteisalkiot ovat transvektioita.

Lemma 3.9. *Transvektiot generoivat ryhmän* $SL(2, K)$.

Todistus. Todistuksessa käytetään merkintää $c^{-1}k = \frac{k}{c}$, missä $k \in K$ ja $c \in K\backslash\{0\}$. Olkoon $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2, K)$. Tällöin determinantin nojalla $ad - bc = 1$. Tarkastellaan todistus kahdessa osassa $c \neq 0$ ja $c = 0$.

1. Olkoon nyt $c \neq 0$. Tällöin $T_1 = \begin{pmatrix} 1 & \frac{1-a}{c} \\ 0 & 1 \end{pmatrix}$ on transvektio ja saadaan

$$\begin{aligned} \begin{pmatrix} 1 & \frac{1-a}{c} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} &= \begin{pmatrix} 1 & b + d\frac{1-a}{c} \\ c & d \end{pmatrix} \\ &= \begin{pmatrix} 1 & \frac{bc-ad+d}{c} \\ c & d \end{pmatrix}, \end{aligned}$$

josta saadaan determinantin $ad - bc = 1$ nojalla

$$= \begin{pmatrix} 1 & \frac{d-1}{c} \\ c & d \end{pmatrix}.$$

Tämän kertomalla edelleen transvektiolla $T_2 = \begin{pmatrix} 1 & 0 \\ -c & 1 \end{pmatrix}$, saadaan

$$\begin{pmatrix} 1 & 0 \\ -c & 1 \end{pmatrix} \begin{pmatrix} 1 & \frac{d-1}{c} \\ c & d \end{pmatrix} = \underbrace{\begin{pmatrix} 1 & \frac{d-1}{c} \\ 0 & 1 \end{pmatrix}}_{T_3},$$

missä $T_3 = \begin{pmatrix} 1 & \frac{d-1}{c} \\ 0 & 1 \end{pmatrix}$ on transvektio. Näin ollen

$$T_2 T_1 A = T_3$$

eli

$$A = T_1^{-1} T_2^{-1} T_3,$$

missä alkiot T_1^{-1}, T_2^{-1} ja T_3 ovat transvektioita. Näin ollen matriisi A voidaan esittää transvektioiden tulona.

2. Olkoon $c = 0$ eli $A = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ ja $\det A = ad = 1$, jolloin $a \neq 0$ ja $d \neq 0$. Nyt $T = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ on transvektio ja

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} = \underbrace{\begin{pmatrix} a & b \\ a & b+d \end{pmatrix}}_{C},$$

missä C voidaan 1. kohdan nojalla esittää transvektioiden tulona. Näin ollen $A = T^{-1}C$ eli A voidaan esittää transvektioiden tulona.

□

Lemma 3.10. *Jos $N \trianglelefteq SL(2, K)$ ja N sisältää ainakin yhden transvektion muotoa $U = \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix}$, missä $u \neq 0$, niin $N = SL(2, K)$.*

Todistus. Olkoon $U = \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix} \in N$ ja $B = \begin{pmatrix} x^{-1} & 0 \\ 0 & x \end{pmatrix} \in SL(2, K)$ eli $x \neq 0$. Koska N on normaali aliryhmä, niin $B^{-1}UB \in N$ eli

$$\begin{pmatrix} x^{-1} & 0 \\ 0 & x \end{pmatrix}^{-1} \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x^{-1} & 0 \\ 0 & x \end{pmatrix} = \begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix} \begin{pmatrix} x^{-1} & ux \\ 0 & x \end{pmatrix}$$
$$= \begin{pmatrix} 1 & ux^2 \\ 0 & 1 \end{pmatrix} \in N.$$

Vastaavasti voidaan myös osoittaa, että jos $y \in K$ ja $y \neq 0$, niin

$$\begin{pmatrix} 1 & uy^2 \\ 0 & 1 \end{pmatrix} \in N,$$

jolloin aliryhmäkriteerin, lauseen 1.8 nojalla

$$\begin{pmatrix} 1 & ux^2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & uy^2 \\ 0 & 1 \end{pmatrix}^{-1} \in N,$$

eli

$$\begin{pmatrix} 1 & ux^2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -uy^2 \\ 0 & 1 \end{pmatrix} \in N,$$

eli

$$\begin{pmatrix} 1 & ux^2 - uy^2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & u(x^2 - y^2) \\ 0 & 1 \end{pmatrix} \in N.$$

Nyt lemman 3.6 nojalla $x^2 - y^2$ käy läpi kaikki kunnan K alkiot, jolloin myös $u(x^2 - y^2)$ käy läpi kaikki kunnan K alkiot. Tämän nojalla normaali aliryhmä N sisältää kaikki transvektiot $\begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix}$, missä $c \neq 0$.

Lisäksi, koska N on normaali ja $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in SL(2, K)$, saadaan

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^{-1} \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in N$$

eli

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} c & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -c & 1 \end{pmatrix} \in N.$$

Näin ollen N sisältää kaikki transvektiot $\begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix}$, missä $c \neq 0$. Selvästi N myös sisältää transvektion $\begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix}$, missä $c = 0$, eli alkion I. Näin ollen N sisältää kaikki ryhmän $SL(2, K)$ transvektiot, jolloin lemman 3.9 nojalla $N = SL(2, K)$.

□

Nyt kaikki tarpeellinen ryhmän $PSL(2, K)$ yksinkertaisuutta varten on käsitelty. Siirrytään siis seuraavaksi tarkastelemaan yleisesti ryhmän $PSL(2, K)$ yksinkertaisuutta. Todistuksessa on hyvä muistaa, että jos $char\ K = 2$, niin $\{I, -I\} = \{I\}$. Todistuksessa tapausta $char\ K = 2$ ei käsitellä erikseen. Todistus mukailee hyvin tarkasti Markku Niemenmaan ryhmäteorian luennoilla 2014 esittämää todistusta, joka löytyy lähteestä [5].

Lause 3.11. *Ryhmä $PSL(2, K)$ on yksinkertainen, jos ja vain jos $|K| \geq 4$.*

Todistus. Lauseissa 3.1 ja 3.2 on osoitettu, että $PSL(2, K)$ ei ole yksinkertainen, jos $|K| < 4$. Riittää siis osoittaa, että $PSL(2, K)$ on yksinkertainen, kun $|K| \geq 4$. Lisäksi lauseen 3.4 nojalla $PSL(2, K)$ on yksinkerteinen, kun $|K| = 4$ ja lauseen 3.5 nojalla $PSL(2, K)$ on yksinkerteinen, kun $|K| = 5$. Nyt voidaan siis olettaa, että $|K| > 5$.

Olkoon $|K| > 5$. Määritelmän 2.8 nojalla

$$PSL(2, K) = SL(2, K) / \underbrace{Z(SL(2, K))}_{\{I, -I\}}.$$

Lauseen 1.17 nojalla ryhmän $PSL(2, K)$ yksinkertaiseksi osoittamiseen riittää osoittaa, että jos $\{I, -I\} \trianglelefteq N \trianglelefteq SL(2, K)$ ja $\{I, -I\} \neq N$, niin $N = SL(2, K)$.

Olkoon nyt siis $\{I, -I\} \trianglelefteq N \trianglelefteq SL(2, K)$ ja $\{I, -I\} \neq N$, jolloin normaali aliryhmä N sisältää sellaisen alkion A, että $A \in SL(2, K) \backslash \{I, -I\}$. Merkitään $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Nyt lemman 3.10 nojalla riittää, että N sisältää ainakin yhden transvektion muotoa $U = \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix}$, missä $u \neq 0$. Jaetaan tarkastelu kahteen osaan $c = 0$ ja $c \neq 0$.

1. Olkoon $c = 0$. Tällöin alkio $A \in N$ on determinantin nojalla muotoa $A = \begin{pmatrix} \alpha^{-1} & x \\ 0 & \alpha \end{pmatrix}$, missä $\alpha \neq 0$.

Jos $\alpha = \pm 1$, niin $A = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$ tai $A = \begin{pmatrix} -1 & x \\ 0 & -1 \end{pmatrix}$, jolloin A tai $-A$ ovat transvektioita, missä $x \neq 0$, sillä $A \in SL(2,K)\backslash\{I,-I\}$. Lisäksi $-A \in N$, sillä $A \in N$, $-I \in N$ ja $-IA = -A$, jolloin $-A \in N$, koska N on normaali aliryhmä.

Oletetaan jatkossa, että $\alpha \in K\backslash\{1,-1\}$, jolloin $\alpha^2 \neq 1$ sillä yhtälö

$$\alpha^2 = 1$$

on yhtäpitävä yhtälön

$$\alpha^2 - 1 = 0$$

kanssa, joka voidaan edelleen muokata muotoon

$$(\alpha + 1)(\alpha - 1) = 0.$$

Vasta-alkion yksikäsitteisyyden nojalla yhtälön ainoat ratkaisut kunnassa K ovat

$$\alpha = 1$$

ja

$$\alpha = -1.$$

Tällöin, koska N on normaali aliryhmä ja $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in SL(2,K)$, niin

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

Eli

$$\begin{aligned}
&\begin{pmatrix} \alpha^{-1} & x \\ 0 & \alpha \end{pmatrix}^{-1} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{-1} \begin{pmatrix} \alpha^{-1} & x \\ 0 & \alpha \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \\
&= \begin{pmatrix} \alpha & -x \\ 0 & \alpha^{-1} \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \alpha^{-1} & x \\ 0 & \alpha \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \\
&= \begin{pmatrix} \alpha & -\alpha - x \\ 0 & \alpha^{-1} \end{pmatrix} \begin{pmatrix} \alpha^{-1} & \alpha^{-1} + x \\ 0 & \alpha \end{pmatrix} \\
&= \begin{pmatrix} 1 & 1 + \alpha x - \alpha^2 - \alpha x \\ 0 & 1 \end{pmatrix} \\
&= \underbrace{\begin{pmatrix} 1 & 1 - \alpha^2 \\ 0 & 1 \end{pmatrix}}_{T} \in N.
\end{aligned}$$

Nyt $1-\alpha^2 \neq 0$, sillä $\alpha^2 \neq 1$, joten $T = \begin{pmatrix} 1 & 1-\alpha^2 \\ 0 & 1 \end{pmatrix}$ on lemman 3.10 vaatima transvektio U.

2. Olkoon nyt $c \neq 0$. Olkoon lisäksi $\beta \in K\backslash\{0\}$. Tällöin on olemassa sellainen alkio $\gamma \in K$, että $B = \begin{pmatrix} a\beta & \gamma \\ c\beta & -a\beta \end{pmatrix} \in SL(2,K)$, sillä determinantin nojalla nähdään, että

$$\begin{aligned} \det B = -a^2\beta^2 - \gamma c\beta &= 1 \\ \Leftrightarrow -\gamma c\beta &= 1 + a^2\beta^2 \\ \Leftrightarrow -\gamma c &= (\beta^{-1} + a^2\beta) \\ \Leftrightarrow \gamma &= -(\beta^{-1} + a^2\beta)c^{-1} \in K. \end{aligned}$$

Lisäksi on tärkeä tehdä huomio, että $B^{-1} = \begin{pmatrix} -a\beta & -\gamma \\ -c\beta & a\beta \end{pmatrix} = -B$, sillä

$$\begin{pmatrix} a\beta & \gamma \\ c\beta & -a\beta \end{pmatrix} \begin{pmatrix} -a\beta & -\gamma \\ -c\beta & a\beta \end{pmatrix} = \begin{pmatrix} -a^2\beta^2 - \gamma c\beta & -\gamma a\beta + \gamma a\beta \\ -c\beta a\beta + c\beta a\beta & -a^2\beta^2 - \gamma c\beta \end{pmatrix},$$

josta saadaan determinantin $\det B = -a^2\beta^2 - \gamma c\beta = 1$ nojalla

$$\begin{pmatrix} -a^2\beta^2 - \gamma c\beta & 0 \\ 0 & -a^2\beta^2 - \gamma c\beta \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Nyt normaali aliryhmä N sisältää alkion

$$\begin{aligned} \underbrace{-I}_{\in N}\underbrace{B^{-1}AB}_{\in N}\underbrace{A}_{\in N} &= -I(-B)ABA \\ &= BABA \\ &= (BA)^2 \\ &= \left[\begin{pmatrix} a\beta & \gamma \\ c\beta & -a\beta \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right]^2 \\ &= \begin{pmatrix} a^2\beta + c\gamma & ab\beta + d\gamma \\ ac\beta - ac\beta & bc\beta - ad\beta \end{pmatrix}^2 \\ &= \begin{pmatrix} a^2\beta + c\gamma & ab\beta + d\gamma \\ 0 & -\beta(ad-bc) \end{pmatrix}^2. \end{aligned}$$

Koska $\det A = ad - bc = 1$ ja $\gamma = -(\beta^{-1} + a^2\beta)c^{-1}$, niin

$$\begin{pmatrix} a^2\beta + c\gamma & ab\beta + d\gamma \\ 0 & -\beta(ad-bc) \end{pmatrix}^2 = \begin{pmatrix} -\beta^{-1} & ab\beta + d\gamma \\ 0 & -\beta \end{pmatrix}^2$$
$$= \begin{pmatrix} \beta^{-2} & -\beta^{-1}(ab\beta + d\gamma) - \beta(ab\beta + d\gamma) \\ 0 & \beta^2 \end{pmatrix}.$$

Kun vielä merkitään $x = -\beta^{-1}(ab\beta + d\gamma) - \beta(ab\beta + d\gamma)$, saadaan

$$\begin{pmatrix} \beta^{-2} & x \\ 0 & \beta^2 \end{pmatrix} = E \in N.$$

Nyt, kuten 1. kohdassa, normaali aliryhmä N sisältää alkion

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

Eli

$$\begin{pmatrix} \beta^{-2} & x \\ 0 & \beta^2 \end{pmatrix}^{-1} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{-1} \begin{pmatrix} \beta^{-2} & x \\ 0 & \beta^2 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$
$$= \begin{pmatrix} \beta^2 & -x \\ 0 & \beta^{-2} \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \beta^{-2} & x \\ 0 & \beta^2 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$
$$= \begin{pmatrix} \beta^2 & -\beta^2 - x \\ 0 & \beta^{-2} \end{pmatrix} \begin{pmatrix} \beta^{-2} & \beta^{-2} + x \\ 0 & \beta^2 \end{pmatrix}$$
$$= \begin{pmatrix} 1 & 1 + \beta^2 x - \beta^4 - \beta^2 x \\ 0 & 1 \end{pmatrix}$$
$$= \underbrace{\begin{pmatrix} 1 & 1 - \beta^4 \\ 0 & 1 \end{pmatrix}}_{T} \in N.$$

Koska oletettiin, että $|K| > 5$, niin huomautuksen 1.31 nojalla on olemassa sellainen $\beta \in K \backslash \{0\}$, että $\beta^4 \neq 1$, jolloin $T = \begin{pmatrix} 1 & 1 - \beta^4 \\ 0 & 1 \end{pmatrix}$ on lemman 3.10 vaatima transvektio U.

Nyt molemmissa tapauksissa $c = 0$ ja $c \neq 0$ löydettiin lemman 3.10 vaatima transvektio U, joten $N = SL(2, K)$. Nyt, huomioiden myös lauseet 3.1, 3.2, 3.4 ja 3.5, on osoitettu, että $PSL(2, K) = SL(2, K)/Z(SL(2, K))$ on yksinkertainen, jos ja vain jos $|K| \geq 4$.

□

4 Ryhmän $PSL(m, K)$ yksinkertaisuudesta

Luvussa 2 todettiin, että lineaariset ryhmät voitaisiin muodostaa $m \times m$ -matriiseille. Tässä luvussa tullaan käsittelemään kyseisiä lineaarisia ryhmiä. Näitä ei kuitenkaan määritellä, eikä matriisien operaatioitakaan tulla yleistämään $m \times m$ -matriiseille, vaan tulokset käsitellään hyvin pintapuoleisesti. Todistuksien tarkat muotoilut vaatisivat laajan määrän lineaarialgebran peruskäsitteiden avaamista. Lisäksi aiheeseen liittyvät tarpeelliset määritelmät, lemmat ja lauseet eivät ole nopeasti esitettävissä, joten näiden tarkka käsittely ei ole tämän laajuisen tutkielman kannalta mielekästä. Luvun 4 tarkoituksena ei olekaan tehdä enää puhdasta matemaattista todistamista, vaan enemmänkin valaista lukijalle, mitä aiheeseen enemmän perehtyvälle on edessä. Luvussa esiteltävien tuloksien todistukset löytyvät lähteestä [6] sivuilta $227 - 233$.

Tässä luvussa käytetään merkintöjä $GL(m, K)$, $SL(m, K)$ ja $PSL(m, K)$, missä kukin lineaarinen ryhmä on vastaava, kuin määritelmissä 2.1, 2.4 ja 2.8, mutta 2×2 -matriisien sijasta nämä lineaariset ryhmät on määritelty $m \times m$ -matriisien avuilla. Eli merkinnät $GL(m, K)$, $SL(m, K)$ ja $PSL(m, K)$ viittaavat astetta m oleviin lineaarisiin ryhmiin kunnan K suhteen.

Lisäksi tullaan puhumaan $m \times m$ -matriisien transvektioista. Näitä määriteltäessä täytyy käsitellä matriiseja alkioiden a_{ij} avulla. Näin käsiteltäessä $m \times m$ -matriisi muodostuu alkioista a_{ij}, missä alkio a_{ij} on $m \times m$ -matriisissa rivillä i ja sarakkeessa j. Lisäksi on tärkeä huomata, että jos $i = j$, niin alkio a_{ij} on diagonaalialkio. Nyt $m \times m$ -matriisi on transvektio, mikäli $a_{ij} = 1$ aina, kun $i = j$, yhdellä alkiolla, missä $i \neq j$, $a_{ij} \neq 0$ ja kaikki muut matriisiin alkiot $a_{ij} = 0$. Näin ollen $m \times m$ -matriisien transvektio on $m \times m$ -matriisi, joka poikkeaa yhdellä alkiolla identiteettimatriisista. Poiketen tutkielmassa esitettävästä transvektion määritelmästä 3.7, lähteessä [6] esitettävässä transvektion määritelmässä ei hyväksytä identiteettimatriisia transvektioksi. Tämä ei varsinaisesti vaikuta todistukseen muuten kuin siten, ettei todistuksissa erikseen tarvitse kertoa transvektion olevan identiteettimatriisista poikkeava.

Ryhmässä $GL(m, K)$, voidaan osoittaa, että kaikki transvektiot konjugoivat keskenään. Tämä tulos on voimassa myös 2×2 -matriiseille, mutta se ei ole ryhmän $PSL(2, K)$ yksinkertaisuuden kannalta merkittävä tulos, sillä tästä eteenpäin johdettava tulos ei ole enää voimassa 2×2 -matriiseille. Voidaan siis lisäksi osoittaa, että jos $m \geq 3$, niin kaikki transvektiot konjugoivat keskenään ryhmässä $SL(m, K)$. Tähän on helppo esittää vastaesimerkki, joka näyttää, että tulos ei ole voimassa ryhmälle $SL(2, K)$.

Esimerkki 4.1. Nyt alkiot $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in SL(2,3)$ ja $\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \in SL(2,3)$ ovat selvästi transvektioita. Osoitetaan, että nämä alkiot eivät konjugoi keskenään ryhmässä $SL(2,3)$. Olkoon $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2,3)$, jolloin $\det A = 1$ ja lemman 1.45 nojalla $A^{-1} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \in SL(2,3)$. Tutkitaan millä matriiseilla A toteutuu yhtälö

$$\begin{aligned} A^{-1} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} A &= \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \\ \Leftrightarrow \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} &= \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \\ \Leftrightarrow \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \begin{pmatrix} a+c & b+d \\ c & d \end{pmatrix} &= \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \\ \Leftrightarrow \begin{pmatrix} da+dc-bc & db+d^2-db \\ -ca-c^2+ca & -cb-cd+ad \end{pmatrix} &= \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}. \end{aligned}$$

Tällöin ensimmäisen rivin toisesta sarakkeesta saadaan yhtälö

$$db + d^2 - db = -1$$

eli

$$d^2 = -1.$$

Tämä on ristiriita kunnassa $\mathbb{Z}_3$, sillä $0^2 = 0$, $1^2 = 1$ ja $(-1)^2 = 1$. Näin ollen transvektiot $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ ja $\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$ eivät konjugoi ryhmässä $SL(2,3)$.

Lisäksi ryhmälle $SL(m,K)$ voidaan tehdä vastaava todistus, kuin lemma 3.9, eli transvektiot generoivat ryhmän $SL(m,K)$. Tämän ja edellä esitellyn tuloksen, jos $m \geq 3$, niin kaikki transvektiot konjugoivat keskenään ryhmässä $SL(m,K)$, avulla voidaan käsitellä ryhmän $PSL(m,K)$ yksinkertaisuutta. Näitä hyödyntäen, saadaan todistettua, että ryhmä $PSL(m,K)$ on yksinkertainen, jos $m \geq 3$.

Lähdeluettelo

[1] John F. Humphreys: *A Course in Group Theory*; Oxford University Press, 1996.

[2] Kari Myllylä: *Lukuteoria ja ryhmät: luentomateriaalit*; Oulun yliopisto, 2011.

[3] Kari Myllylä: *Renkaat, kunnat ja polynomit: luentomateriaalit*; Oulun yliopisto, 2011.

[4] Markku Niemenmaa: *Permutaatiot, kunnat ja Galois'n teoria: luentomateriaalit*; Oulun yliopisto, 2012.

[5] Markku Niemenmaa: *Ryhmäteoria: luentomateriaalit*; Oulun yliopisto, 2014.

[6] Joseph J. Rotman: *An Introduction to the Theory of Groups*; Springer-Verlag New York, Inc., 1999.

[7] Tero Vedenjuoksu: *Matriisiteoria: luentomateriaalit*; Oulun yliopisto, 2015.