JYVÄSKYLÄN YLIOPISTO
MATEMATIIKAN JA TILASTO-
TIETEEN LAITOS

Pro gradu-tutkielma

Toisen asteen imaginääristen lukukuntien perusalueet hyperbolisessa avaruudessa

Jaakko Kustaa Toivonen

17. kesäkuuta 2024

Tekijä
Jaakko Kustaa Toivonen

Otsikko
Toisen asteen imaginääristen lukukuntien perusalueet hyperbolisessa puoliavaruudessa

Tutkinto-ohjelma
Matematiikan maisteriohjelma

Päivämäärä
17. kesäkuuta 2024

Sivumäärä
61

Tiivistelmä

Tässä tutkielmassa käsitellään toisen asteen imaginääristen lukukuntien luokkaluvun yhteyttä kunnan kokonaislukurenkaan virittämän hyperbolisen avaruuden isometrioiden ryhmän $\mathbf{PSL}_2(\mathcal{O}_K)$ eli Bianchin ryhmän muodostamaan perusalueeseen. Tutkielma perustuu pääosin Jürgen Elstrodtin, Fritz Grunewaldin ja Jens Mennicken kirjaan Groups Acting on Hyperbolic Spaces; Harmonic Analysis and Number Theory kappaleeseen 7. [9] Tutkielma esittelee kappaleen sisällon todistaen sen tulokset lähdeteosta perusteellisemmin. Lisäksi tutkielmassa esitetään vaadittavat algebralliset ja geometriset esitiedot.

Keskeisenä työkaluna tässä tutkielmassa käytetään ideaalien teoriaa. Tutkielmassa esitellään keskeisten määritelmien lisäksi merkittäviä algebrallisia tuloksia kuten Kiinalainen jäännöslause ja Minkowskin lause. Algebrallisia tuloksia ei välttämättä esitellä yleisimmässä mahdollisessa muodossa todistusten selkeyden vuoksi.

Tutkielmassa esitellään lisäksi kolmiulotteisen hyperbolisen avaruuden määritelmä ja joitain sen geometrisiä ominaisuuksia. Keskeisenä määritelmänä on 2×2-matriisien erityinen lineaarinen ryhmä, jonka todetaan toimivan isometrioilla hyperbolisessa avaruudessa. Erityisen lineaarisen ryhmän aliryhmällä, jonka kertoimet ovat toisen asteen imaginäärisen lukukunnan kokonaislukuja, todistetaan olevan algebrallisesti merkittäviä ominaisuuksia.

Tutkielman kaksi viimeistä kappaletta osoittavat yhteyden luokkaluvun ja Bianchin ryhmän hyperbolisen perusalueen välillä. Lukukunnan perusalueen konstruktio esitellään ensin ja tämän jälkeen joukon todistetaan olevan perusalue. Perusalueen konstruktiosta päätellään joitain joukon geometrisiä ominaisuuksia. Lopuksi esitellään ja visualisoidaan kuntien $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{-3})$ ja $\mathbb{Q}_{\sqrt{-5}}$ perusalueet sekä huomioidaan perusalueen ja kompleksitason leikkauspisteiden yhteys kunnan luokkalukuun.

Sisällys

Johdanto

Lukukunta K ja sen kokonaislukujen rengas $\mathcal{O}_K$ vastaavat joiltain ominaisuuksiltaan intuitiivisesti rationaalilukujen kuntaa $\mathbb{Q}$ ja kokonaislukujen rengasta $\mathbb{Z}$. Algebrallinen lukuteoria tutkii muun muassa lukukuntia ja niiden kokonaislukurenkaiden ominaisuuksia erityisesti, kun ne poikkeavat kunnan $\mathbb{Q}$ ja renkaan $\mathbb{Z}$ ominaisuuksista. Esimerkiksi renkaan alkioiden uniikki alkutekijöihin jako on algebrallisen lukuteorian kannalta merkittävä ominaisuus. Tekijöihinjaon uniikkiutta mittaa kunnan luokkaluku, joka määritellään kunnan ideaaliluokkien määränä. Ideaaliluokka on kunnan murtoideaalien ekvivelanssiluokka. Kaksi murtoideaalia kuuluu samaan ideaaliluokkaan, jos niiden ideaalitulot joidenkin pääideaalien kanssa tuottavat saman ideaalin. Tässä tutkielmassa esitetään erityinen yhteys toisen asteen imaginääristen lukukuntien luokkalukujen ja Bianchin ryhmän $\mathbf{PSL}_2(\mathcal{O}_K)$, joka on kunnan kokonaislukujen renkaan määrittämä kolmiulotteisen hyperbolisen avaruuden isometrioiden diskreetti ryhmä, perusalueen välillä. Lukukunnan ja perusalueen yhteys havaitaan kunnan Bianchin ryhmän algebrallisten kärkien joukosta, jotka voidaan geometrisesti tunnistaa perusalueen sulkeuman ja kompleksitason leikkauspisteistä.

Tutkielman tarkoituksena on esittää tulokset selkeällä tavalla ilman aiempaa syventävämmän algebrallisen lukuteorian tai geometrian tuntemusta. Lukijalta kuitenkin odotetaan muutaman perustavan konseptin tuntemus kuten renkaan, kunnan ja isometrian määritelmät.

Tutkielmassa todistetaan joitain merkittäviä algebrallisen lukuteorian tuloksia. Ensimmäisissä kappaleissa todistetaan useita perustavia ideaaliteorian tuloksia. Lähteet [1], [2], [7] ja [14] antavat tätä tutkielmaa kattavamman perehdyksen lukukuntiin, algebralliseen lukuteoriaan ja ideaaliteoriaan.

Tutkielmassa todistettava Kiinalainen jäännöslause (Lause 3.1) on satoja vuosia tunnettu tulos, jolla on useita esitystapoja. ([13], luku 5.3) Tässä tutkielmassa todistetaan lause kommutatiivisen renkaan ideaaleille. Kiinalainen jäännöslause kertoo, että äärelliselle joukolle renkaan ideaaleja on olemassa homomorfismi renkaalta renkaan tekijäavaruuksien ideaalien suhteen muodostamaan tuloavaruuteen. Lisäksi kyseisen homomorfismin ydin on ideaalien leikkaus. Lausetta käytetään muodostamaan hyödyllinen bijektio renkaan tekijäavaruudelta ideaalien tulon suhteen $R/(I_1 I_2 \dots I_n)$ tuloavaruuteen renkaan tekijäavaruuksia ideaalien suhteen $R/I_1 \times R/I_2 \times \cdots \times R/I_n$.

Tutkielmassa todistetaan myös Minkowskin lause (Lause 3.6). Lause todistetaan vain toisen asteen imaginäärisissä lukukunnissa, mutta lauseesta on olemassa yleisempi muotoilu. [15] Minkowskin lause kertoo, että origon suhteen symmetrinen konveksi joukko, jonka pinta-ala on kokonaislukurenkaan hilan perussuunnikkaaseen verrattuna nelinkertainen, sisältää kokonaisluku-

renkaan pisteen. Lause on geometrisesti merkittävä ja sitä käytetään tässä tutkielmassa todistamaan Minkowskin epäyhtälö (Lause 3.7). Minkowskin epäyhtälö kertoo, että on olemassa positiivinen reaaliluku M siten, että jokaisessa ideaaliluokassa on kokonaislukurenkaan ideaali, jonka normi on alle M. Minkowskin epäyhtälön seurauksena todetaan, että ideaaliluokkien ryhmä on äärellinen.

Tutkielman kannalta tärkeä tulos on määritellä bijektio kunnan algebrallisilta kärjiltä, jotka määritellään kappaleessa 6.1, ideaaliluokkien ryhmään. Lause mahdollistaa luokkaluvun tutkimisen geometrisesti. Lisäksi tutkielmassa määritellään perusalue Bianchin ryhmälle hyperbolisessa avaruudessa. Alue muodostuu äärettömyyspisteen stabilisoijan perusalueen ja euklidisten puolipallojen rajaaman alueen leikkauksena. Perusalueen rajaavien puolipallojen keskipisteet ovat kompleksitasossa olevia kunnan murtolukuja, joiden osoittaja ja nimittäjä virittävät kunnan kokonaislukujen renkaan.

Keskeisin tulos tutkielman kannalta on osoittaa, että toisen asteen imaginäärisessä lukukunnassa luokkaluku on 1, jos ja vain jos kunnan Bianchin ryhmän kolmiulotteisen hyperbolisen perusalueen sulkeuman ja kompleksitason leikkaus on tyhjä. Tulos antaa geometrisen tavan tutkia kunnan luokkalukua.

Ensimmäiset kolme kappaletta sisältävät tarvittavan algebrallisen taustan tutkielman tuloksiin. Tarkoituksena on esitellä riittävä tuntemus algebrallisiin objekteihin kuten algebrallisiin kokonaislukuihin, lukukuntiin ja ideaaleihin, että lukija pysyy tulosten todistusten mukana. Lukijalle esitellään hilojen ja ideaalien ominaisuuksia, joita hyödynnetään tutkielman eri todistuksissa. Kappaleessa kolme esitellään Kiinalainen jäännöslause ja Minkowskin lause. Näiden merkittävien algebrallisen lukuteorian lauseiden seuraukset ovat hyödyllisiä tutkielman myöhemmissä todistuksissa.

Tutkielman kappaleessa neljä esitellään hyperbolinen avaruus ja määritellään Bianchin ryhmä, joka on hyödyllinen isometrioiden ryhmä hyperbolisessa avaruudessa. Tämän jälkeen viidennessä kappaleessa esitellään yhteys kompleksitason kunnan pisteiden ja luokkaluvun välillä.

Kappaleet kuusi ja seitsemän kokonaisuudessaan esittelevät geometrisen tavan käsitellä toisen asteen imaginääristä lukukuntaa. Kappaleessa kuusi määritellään algebrallinen kärki ja määritelmä yhdistetään kappaleen neljä ja viisi tuloksiin. Kappaleessa seitsemän määritellään perusalue ja esitellään Bianchin ryhmän perusalueen konstruktio.

Viimeisessä kappaleessa esitellään joitain konkreettisia esimerkkejä tutkielman yleisistä tuloksista. Kappaleessa esitetyt kuvat antavati intuitiivisemman käsityksen perusalueen geometriasta ja sen yhteydestä luokkalukuun.

Tutkielman kappaleet 5-8 perustuvat pääosin Jürgen Elstrodtin, Fritz

Grunewaldin ja Jens Mennicken kirjaan Groups Acting on Hyperbolic Spaces; Harmonic Analysis and Number Theory [9].

1 Toisen asteen lukukunta

1.1 Lukukunta ja kokonaislukujen rengas

Tässä kappaleessa määritellään joitain algebrallisen lukuteorian tärkeitä määritelmiä. On hyödyllistä tutkia kokonaislukujen ja rationaalilukujen kaltaisia renkaita ja kuntia esimerkiksi kompleksitasossa. Ensimmäiset määritelmät mahdollistavat rationaalilukujen ja kokonaislukujen laajentamisen hyvin määriteltyyn kuntaan ja renkaaseen.

Määritelmä 1.1. Olkoon K kunta. Kunta L on kunnan K n asteinen *algebrallinen laajennus*, jos kaikki $l \in L$ ovat kunnan $K \subset L$ kertoimisten nollasta poikkeavien n asteisten polynomien juuria. Algebrallisen laajennoksen alkioita kutsutaan *algebrallisiksi luvuiksi*. Murtolukujen kunnan $\mathbb{Q}$ algebrallista laajennusta kutsutaan lukukunnaksi.

Määritelmä 1.2. Olkoon B rengas ja $A \subset B$ sen alirengas. Alkiota $b \in B$, jolle on olemassa $n \in \mathbb{N}$ siten, että $b^n + a_{n-1}b^{n-1} + \cdots + a_0 = 0$ jollain $a_{n-1}, \ldots, a_0 \in A$, kutsutaan *kokonaiseksi* kunnassa A.
Lukukunnan K alkio, joka on kokonainen kokonaislukujen renkaassa $\mathbb{Z}$, on *algebrallinen kokonaisluku*.

Lukukunnat ovat yksi algebrallisen lukuteorian tärkeimmistä objekteista. Ne mahdollistavat lukuteorian esimerkiksi tietyillä kompleksilukujen osajoukoilla. Jos lukukunta voidaan kuvata kuntahomomorfismilla reaalilukujen alikunnaksi kutsutaan sitä reaaliseksi. Muuten on olemassa kuntahomomorfismi kompleksilukujen oalikunnaksi ja lukukuntaa kutsutaan imaginääriseksi. ([1], luku 13.1) Tässä tutkielmassa merkittäviä ovat erityisesti toisen asteen imaginääriset lukukunnat. Esitetään eksplisiittisesti toisen asteen imaginäärisen lukukunnan alkiot.

Määritelmä 1.3. Kokonaisluku $d \in \mathbb{Z}$ on *neliötön*, jos $d \neq a^2b$ millään kokonaisluvuilla $a, b \in \mathbb{Z}$.
Rationaalilukujen kunnan $\mathbb{Q}$ toisen asteen imaginäärinen lukukunta $\mathbb{Q}(\sqrt{d})$ jollain neliöttömällä kokonaisluvulla $d < 0$ on kompleksilukujen osajoukko, joka muodostuu alkioista $a + b\sqrt{d}$, missä $a, b \in \mathbb{Q}$.

Toisen asteen imaginäärisen lukukunnan K alkioiden esitys yllä mainitussa muodossa muodostuu luonnollisesti tutkimalla toisen asteen polynomeja. On hyvä huomioida, että algebrallisten kokonaislukujen joukko muodostaa renkaan $\mathcal{O}_K$. ([14], s.10-11) Lukukunnan alkiot ovat toisen asteen ratkaisukaavan mukaan eksplisiittisesti muotoa $x = \frac{-b \pm \sqrt{D}}{2a}$ murtoluvuilla a b ja c

sekä diskriminantilla $D = b^2 - 4ac$, jolle $D < 0$. Täten toisen asteen imaginäärisen lukukunnan alkion voi kirjoittaa muodossa $a + b\sqrt{D}$. Huomioidaan, että diskriminantin ollessa q^2D murtoluvulla q, $x = a + b\sqrt{q^2D}$ saa murtoluvuilla a ja b samat ratkaisut kuin yhtälö $x = a + b\sqrt{D}$. Täten kirjoitetaan lukukunnan alkio muodossa $a + b\sqrt{d}$ jollain neliöttömällä kokonaisluvulla $D = d < 0$.

Tutkitaan seuraavaksi toisen asteen imaginäärisen lukukunnan kokonaislukuja. Lukukunnan kokonaislukujen renkaan $\mathcal{O}_K$ alkioiden muodostuksessa mainittakoon, että $\mathbb{Z} \subset \mathcal{O}_K$ pätee aina. Huomioidaan, että yhtälön

$$x = \frac{-b \pm \sqrt{b^2 - 4c}}{2}$$

tulee päteä kokonaisluvuilla b ja c. Yhtälön diskriminantti $D = b^2 - 4c$ on selkeästi kongruentti lukuun 0 tai 1 modulo 4, koska $4c$ on kongruentti luvun 0 kanssa ja b^2 on kongruentti lukuun 0 tai 1 modulo 4.

Jos $D \equiv 1 \bmod 4$ saadaan $b^2 - 4c = 4r - 1$ eli $c = 1/4 + b^2/4 - r$ jollain $D = 4r - 1$. Saadaan yhtälö

$$x^2 + bx + c = x^2 + bx + b^2/4 + 1/4 - r = (x + b/2)^2 + 1/4 - r = 0,$$

josta kertomalla puolittain neljällä saadaan $(2x + b)^2 + 1 - 4r = 0$. Huomioidaan, että yhtälölle on ratkaisuja vain kun kokonaisluku b on pariton. Lisäksi, koska D on pariton, kokonaisluku c, jolle pätee $c^2d = D$ kokonaisluvulla d, on myös pariton. Täten $x = \pm\frac{-b+\sqrt{D}}{2} = \pm\frac{-b-1}{2} \pm \frac{1+\sqrt{D}}{2}$.

Jos puolestaan $D \equiv 0 \bmod 4$, $b^2 - 4c = 4r$ eli $c = b^2/4 - r$ jollain kokonaisluvulla r. Jos $r \equiv 1 \bmod 4$ pätee $\mathbb{Q}(\sqrt{D}) = \mathbb{Q}(\sqrt{r})$. Koska kunnat ovat identtiset, niiden kokonaislukurenkaat ovat identtiset ja tapaus vastaa tilannetta, missä $D \equiv 1 \bmod 4$.

Muutoin saadaan yhtälö

$$x^2 + bx + c = x^2 + bx + b^2/4 - r = (x + b/2)^2 - r = 0,$$

josta kertomalla puolittain neljällä saadaan $(2x+b)^2-4r = 0$. Täten saadaan $x = \pm b\sqrt{r}$.

Kokonaislukujen renkaan alkioiden summat ovat myös renkaassa eli, koska kaikilla $a \in \mathbb{Z}$ on polynomi $x - a = 0$, renkaan $\mathcal{O}_K$ alkiot ovat seuraavaa muotoa.

Lemma 1.4. *Olkoon $\mathbb{Q}(\sqrt{d})$ toisen asteen imaginäärinen lukukunta jollain neliöttömällä kokonaisluvulla $d < 0$. Sen kokonaislukujen rengas muodostuu alkioista*

$$x + y\sqrt{d}, \text{ jos } d \not\equiv 1 \bmod 4,$$

tai

$$x + y\frac{1+\sqrt{d}}{2}, \text{ jos } d \equiv 1 \ mod\ 4,$$

missä $x, y \in \mathbb{Z}$. *([2], s.383-384)*

Nyt ollaan osoitettu, että toisen asteen imaginäärisen lukukunnan ja sen kokonaislukujen renkaan määritelmä on konsistentti. Huomioidaan vielä, että lukukunnan $\mathbb{Q}(\sqrt{d})$ diskriminantti on $D = d$, kun $D \equiv 1 \bmod 4$, ja muutoin $D = 4d$. Jos algebrallisten kokonaislukujen joukkoa tarkastellaan geometrisesti, on hyvä määritellä vastaava geometrinen objekti.

1.2 Hilat

Imaginäärisissä lukukunnissa on hyödyllistä käsitellä kompleksitason summaoperaatiolla suljettuja diskreettejä osajoukkoja. Geometrista tulkintaa varten määristelmät määritellään $\mathbb{R}^2$ tasossa, mutta määritelmiä käytetään imaginäärisiin lukukuntiin tulkiten kompleksiluvut $\mathbb{R}^2$ tason alkioina.

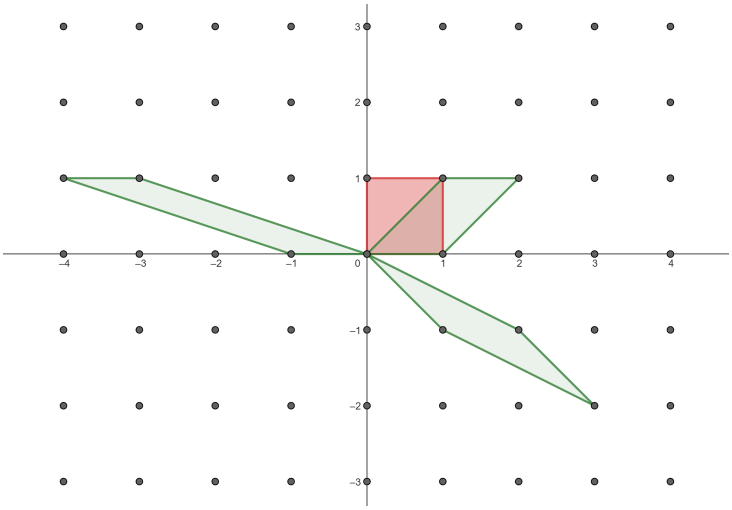
Määritelmä 1.5. Ääretön joukko $L \subset \mathbb{R}^2$ on *hila*, jos:

- $0 \in L$
- kaikille $l, t \in L$ pätee $l + t \in L$ ja $l - t \in L$
- on olemassa $a, b \in L$, jotka ovat lineaarisesti riippumattomat eli $a \neq rb$ millään $r \in \mathbb{R}$
- ja jos L on diskreetti, eli kaikille $a, b \in L$ pätee $a+b \in L$ ja on olemassa $\epsilon > 0$ siten, että $\|a - b\| \geq \epsilon$ kaikille $a \neq b$.

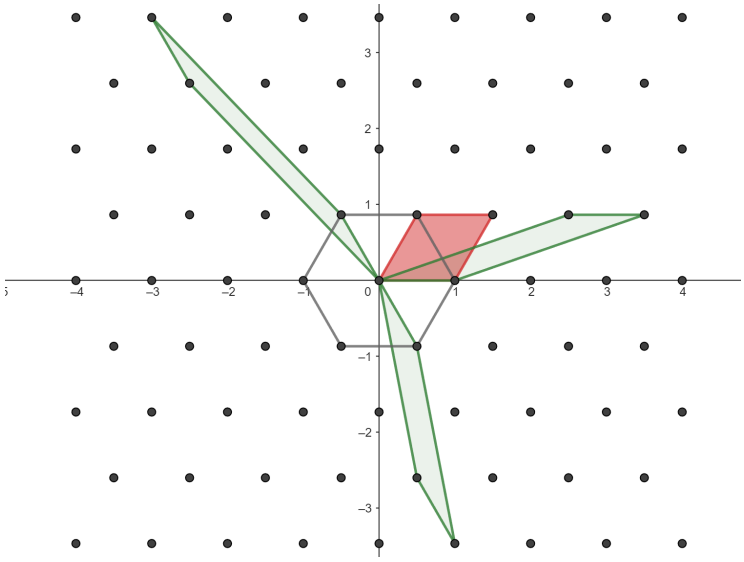
On kohtuullisen helppoa nähdä esimerkiksi Lemman 1.4 avulla, että algebrallisten kokonaislukujen joukko tulkittuna $\mathbb{R}^2$ tason alkioina on hila. Esitellään lukukuntien $\mathbb{Q}(i)$ kokonaislukurenkaan eli Gaussin kokonaislukujen ja $\mathbb{Q}(\sqrt{-3})$ kokonaislukurenkaan eli Eisensteinin kokonaislukujen hilat.

Gaussin kokonaisluvut ovat Lemman 1.4 mukaan muotoa $a+bi$ kokonaisluvuilla a ja b. Kuten kuvasta 1.2 näkee Gaussin kokonaislukujen hila muodostaa neliölaatoituksen kompleksitasoon. Gaussin kokonaisluvut sisältävät neljä luvun 1 juurta 1, i, -1 ja $-i$.

Eisensteinin kokonaisluvut ovat Lemman kok mukaan muotoa $a+b\frac{1+\sqrt{-3}}{2}$, missä $a, b \in \mathbb{Z}$. Ne muodostavat tasasivuisten kolmioiden laatoituksen. On hyvä huomioida, että Eisensteinin kokonaisluvuissa on yhteensä kuusi erillistä luvun 1 juurta 1, $\frac{1+\sqrt{-3}}{2}$, $\frac{1-\sqrt{-3}}{2}$, -1, $\frac{-1-\sqrt{-3}}{2}$ ja $\frac{-1-\sqrt{-3}}{2}$.



Kuva 1.1: Gaussin kokonaislukujen hila. Joitain kokonaislukurenkaan perussuunnikkaita on esitetty vihreällä. Kokonaislukurenkaan primäärinen perussuunnikas on esitetty punaisella.



Kuva 1.2: Eisensteinin kokonaislukurenkaan hila. Luvun 1 juuret muodostavat säännöllisen kuusikulmion. Joitain kokonaislukurenkaan perussuunnikkaita on esitetty vihreällä. Kokonaislukurenkaan primäärinen perussuunnikas on esitetty punaisella.

Määritelmä 1.6. Olkoon $L \subset \mathbb{R}^2$ hila ja olkoon $a, b \in \mathbb{R}^2$ siten, että $ar \neq b$ millään $r \in \mathbb{R}$ ja $\{an + bm : n, m \in \mathbb{Z}\} = L$. Määritellään hilan *perussuunnikas* joukoksi

$$\{x = ar_1 + br_2 \in \mathbb{R}^2 : 0 \leq r_1 \leq 1, 0 \leq r_2 \leq 1\}.$$

Lemma 1.7. *Hilalla L on olemassa perussuunnikas.*

Todistus. Koska jollain $\epsilon > 0$ pätee $\|a - b\| \geq \epsilon$ kaikilla $a, b \in L$, on olemassa piste x, jolle $|x| \leq |a|$ kaikille $a \in L - \{0\}$. Nyt hilan määritelmän mukaan on olemassa pisteen x kanssa lineaarisesti riippumaton piste y, jolle vastaavasti $|y| \leq |b|$ kaikille $b \in L - (a\mathbb{R})$. Joukko

$$P = \{z = xr_1 + yr_2 \in \mathbb{R}^2 : 0 \leq r_1 \leq 1, 0 \leq r_2 \leq 1\}$$

on perussuunnikas. Todistetaan väite antiteesillä. Jos P ei ole perussuunnikas, on piste $l \in L$, jolle $l \notin x\mathbb{Z} + y\mathbb{Z}$. Nyt on olemassa piste l_1 siten, että $l_1 = l - (sx + ty) \in P$ jollain $s, t \in \mathbb{Z}$, jolle $l_1 \neq 0$, $l_1 \neq x$, $l_1 \neq y$ ja $l_1 \neq x + y$. Täten pisteen l_1 etäisyys perussuunnikkaan P johonkin kulmapisteeseen p_i on pienempi kuin $|y|$. Täten $|l_1 - p_i| < |y|$. Pisteen y valinnan mukaan piste l_1 rajoittuu joukkoon $l_1 - p_i \in a\mathbb{R}$. Määritellään nyt $l_2 = l_1 - p_i - sx = ra$ jollain $s \in \mathbb{Z}$ ja $0 < r < 1$. Täten on piste $l_2 \in L$, jolle $|l_2| < |x|$ aiheuttaen ristiriidan pisteiden x ja y valinnan kanssa. □

On hyvä huomioida, että perussuunnikas ei ole uniikki. Huomataan kuitenkin, että toisen asteen lukukunnan kokonaislukurengas on Lemman 1.4

$$\{n + \omega m : n, m \in \mathbb{Z}\},$$

missä $\omega = \frac{1+\sqrt{d}}{2}$, kun $d \equiv 1 \bmod 4$, ja muutoin $\omega = \sqrt{d}$. Täten yksi imaginäärisen toisen asteen lukukunnan kokonaislukujen hilan perussuunnikas on joukko $\{x = r_1 + r_2\omega \in \mathbb{C} : 0 \leq r_1 \leq 1, 0 \leq r_2 \leq 1\}$. Tämä perussuunnikas on ominaisuuksiltaan riittävä tässä työssä.

Määritelmä 1.8. Olkoon $\mathbb{Q}(\sqrt{d})$ toisen asteen imaginäärinen lukukunta. Kunnan $\mathbb{Q}(\sqrt{d})$ kokonaislukujen renkaan *primäärinen perussuunnikas* on

$$\{x = r_1 + r_2\omega \in \mathbb{C} : 0 \leq r_1 \leq 1, 0 \leq r_2 \leq 1\},$$

missä $\omega = \frac{1+\sqrt{d}}{2}$, kun $d \equiv 1 \bmod 4$, ja muutoin $\omega = \sqrt{d}$.

Nyt esimerkiksi Eisensteinin kokonaislukujen primäärisen perussuunnikkaan kärjet ovat luvut 0, 1, $\frac{1+\sqrt{-3}}{2}$ ja $1 + \frac{1+\sqrt{-3}}{2}$. Perussuunnikkaan määritelmästä huomaa myös, että perussuunnikas sisältää tasan neljä hilan pistettä, jotka ovat suunnikkaan neljä kulmapistettä.

Määritellään lopuksi vielä tapa vertailla hilojen kokoja.

Määritelmä 1.9. Olkoon hila H hilan L osajoukko. Määritellään kaikille joukon L pisteille $x, y \in L$ ekvivalenssi

$$x = y,$$

jos

$$x - y \in H$$

ja merkitään joukon L pisteiden ekvivalenssiluokkien joukkoa L/H. Hilan H *indeksi* hilassa L määritellään

$$[L : H] = \#(L/H).$$

2 Ideaalit

2.1 Ideaali

Algebrallisten ominaisuuksien käsittelyssä voi olla hyödyllisempää käsitellä yksittäistä alkiota laajempaa joukkoa. Ideaalit ovat merkittävä osa algebrallista lukuteoriaa.

Määritelmä 2.1. Kommutatiivisen renkaan R osajoukko $I \subset R$ on *ideaali*, jos $(I, +)$ on ryhmän $(R, +)$ aliryhmä ja jos $ir \in I$ kaikilla $i \in I$ ja $r \in R$.

Määritelmästä huomataan, että rengas on aina itsensä ideaali. Tätä kutsutaan triviaaliksi ideaaliksi. On myös hyvä huomioida, että summan nollaalkio muodostaa ideaalin $\{0\}$. Määritelmän tuloehdosta voidaan myös huomata, että valitsemalla mikä tahansa renkaan R alkioiden joukko $A \subset R$ voidaan määritellä pienin ideaali, joka sisältää joukon A. Tällöin sanotaan, että valitut alkiot virittävät ideaalin. Jos ideaali I sisältää renkaan R yksiköt, ideaali on koko rengas. Huomataan myös, että toisen asteen imaginäärisen lukukunnan kokonaislukujen renkaassa ideaali on myös hila. Tämä mahdollistaa ideaalien geometrisen käsittelyn, mikä on relevanttia kappaleen kolme todistuksissa. On usein myös hyödyllistä esittää ideaali sen virittävillä alkioilla.

Määritelmä 2.2. Alkiot $\alpha_1, \alpha_2, \ldots, \alpha_n \in R$ virittävät ideaalin

$$\langle \alpha_1, \alpha_2, \ldots, \alpha_n \rangle = \{\sum_{k=1}^{n} r_k \alpha_k \in R : r \in R\}.$$

Yksittäisen alkion $a \in R$ virittämää ideaalia $\langle a \rangle = \{ar \in R : r \in R\}$ kutsutaan *pääideaaliksi*.

Se, että ideaali on pääideaali, on erityisen hyödyllinen ominaisuus. On hyvä huomioida, että ideaalin esittäminen virittävien alkioiden avulla ei välttämättä ole yksikäsitteistä. Esitys kuitenkin mahdollistaa intuitiivisemman ymmärryksen ideaaleihin. Määrittelemällä ideaalin J ja renkaan R alkion a tulo

$$aJ = \{aj \in R : j \in J\}$$

huomataan pääideaalin määritelmästä, että renkaan R pääideaalille pätee $\langle a \rangle = aR$. Määritellään seuraavaksi summan ja tulon laskutoimitukset ideaaleille.

Määritelmä 2.3. Olkoon $I, J \subset R$ renkaan R ideaaleja. Ideaalien summa määritellään

$$I + J = \{a + b : a \in I, b \in J\}.$$

Ideaalien tulo määritellään

$$IJ = \{a_1b_1 + a_2b_2 + \cdots + a_nb_n : a_k \in I, b_k \in J, n \in \mathbb{N}\}.$$

Lemma 2.4. *Ideaalien tulo IJ ja summa $I + J$ ovat ideaaleja.*

Todistus. Olkoon $a = i_1 + j_1 \in I + J$ ja $b = i_2 + j_2 \in I + J$ jollain $i_1, i_2 \in I$ ja $j_1, j_2 \in J$. Olkoon lisäksi alkiot

$$c = i_1j_1 + \cdots + i_nj_n \in IJ$$

ja

$$d = i_{n+1}j_{n+1} + \cdots + i_mj_m \in IJ$$

jollain $i_1, \ldots, i_n, \ldots, i_m \in I$ ja $j_1, \ldots, j_n, \ldots, j_m \in J$ sekä olkoon $r \in R$. Nyt

$$ra = rj_1 + ri_1$$

ja

$$a + b = i_1i_2 + i_1j_2 + i_2j_1 + j_1j_2,$$

missä ideaalin määritelmän mukaan $ri_1, i_1i_2, i_1j_2, i_2j_1 \in I$ ja $rj_1, j_1j_2 \in J$. Nyt $ra, a + b \in I + J$. Vastaavasti

$$rc = ri_1j_1 + \cdots + ri_nj_n,$$

ja

$$c + d = i_1j_1 + \cdots + i_nj_n + i_{n+1}j_{n+1} + \cdots + i_mj_m,$$

missä $ri_1, \ldots, ri_n \in I$. Nyt ideaalien tulon määritelmän perusteella saadaan $rc, c + d \in IJ$. Täten IJ ja $I + J$ ovat ideaaleja. □

On helppo huomata, että renkaan ideaalille $J \subset R$ ja alkiolle $a \in R$ pätee $aJ = \langle a \rangle J$. On hyvä lisäksi huomioida, että määritelmän mukaan ideaalien yhdiste sisältyy ideaalien summaan $I \cup J \subset I + J$ ja ideaalien tulo sisältyy ideaalien leikkaukseen $IJ \subset I \cap J$. Nyt pääideaalien tulolle huomioidaan seuraava ominaisuus.

Lemma 2.5. *Pääideaalien tulolle pätee* $\langle a \rangle \langle b \rangle = \langle ab \rangle$.

Todistus. Todistetaan lemma pääideaalien ja ideaalitulon määritelmän kautta. Yhtälö

$$\begin{aligned} \langle a \rangle \langle b \rangle &= \{ar_1bt_1 + ar_2bt_2 + \cdots + ar_nbt_n : r_k, t_k \in R, n \in \mathbb{N}\} \\ &= \{abr : r \in R\} \\ &= \langle ab \rangle \end{aligned}$$

todistaa lemman. □

Huomioidaan vielä toisen asteen imaginäärisessä lukukunnassa ideaalille hyödyllinen geometrinen tulkinta.

Lemma 2.6. *Toisen asteen imaginäärisen lukukunnan kokonaislukujen renkaan ideaali* $I \neq \langle 0 \rangle$ *on hila.*

Todistus. Huomataan aluksi, että $0 \in I$ ja I on ryhmän $(R, +)$ aliryhmä. Lisäksi kokonaislukujen renkaassa alkioille $a, b \in I$ $a \neq b$ pätee $|a - b| \geq 1$. Täten riittää todistaa, että ideaalissa on alkiot x ja y jolle pätee $x \neq ry$ kaikilla $r \in \mathbb{R}$. Toisen asteen imaginäärisen lukukunnan kokonaislukurenkaassa on alkio $\sqrt{-d} \notin \mathbb{R}$. Täten valitsemalla $x \in I - \{0\}$ saadaan alkiot $x, \sqrt{-d}x \in I$, joille $x \neq r\sqrt{-d}x$ millään $r \in \mathbb{R}$. □

Nyt toisen asteen imaginäärisen lukukunnan ideaalia voidaan käsitellä geometrisesti hilana. Käyttämällä kappaleessa 1 määriteltyjä hilan ominaisuuksia voidaan todistaa seuraava merkittävä seuraus.

Seuraus 2.7. *Olkoon* K *toisen asteen imaginäärinen lukukunta ja* $\mathcal{O}_K$ *sen kokonaislukujen rengas. Ideaalille* $I \subset \mathcal{O}_K$ *on olemassa alkiot* $a, b \in I$*, joille* $\langle a, b \rangle = I$.

Todistus. Jos $I = \langle a \rangle$ valitsemalla $b = a$ $\langle a, b \rangle = \langle a \rangle = I$. Lemman 2.6 mukaan ideaalia I voidaan tarkastella hilana. Lemman 1.7 perusteella on olemassa alkiot a ja b, joille $\{an + bm : n, m \in \mathbb{Z}\} = I$. Koska lukukunnassa K $\mathbb{Z} \subset \mathcal{O}_K$, voidaan päätellä

$$I = \{an + bm : n, m \in \mathbb{Z}\} \subset \{ar_1 + br_2 : r_1, r_2 \in \mathcal{O}_K\} = \langle a, b \rangle.$$

Huomioimalla vielä, että kaikille alkioille $a, b \in I$, jos $c \in \langle a, b \rangle$, saadaan $c = ar_1 + br_2 \in I$. Täten $I = \langle a, b \rangle$. □

Nyt kaikki toisen asteen imaginäärisen lukukunnan ideaalit voidaan esittää kahdella alkiolla. On hyvä huomioida, että kokonaislukurenkaassa $\mathcal{O}_K$ pätee $\langle 1 \rangle = \mathcal{O}_K$ kaikilla $a \in \mathcal{O}_K$. Seuraavaksi käyttäen seurausta 2.7 voidaan todistaa lukukunnan ideaaleille vielä yksi keskeinen ominaisuus.

Lemma 2.8. *Olkoon K toisen asteen imaginäärinen lukukunta ja kokonaislukurenkaan ideaalit $I \subset J \subset \mathcal{O}_K$. On olemassa ideaali $H \subset \mathcal{O}_K$ jolle $HJ = I$.*

Todistus. Ideaalin J alkioiden konjugaatit muodostavat kokonaislukurenkaan ideaalin $\bar{J}$.

Todistetaan ensin, että $J\bar{J}$ on kokonaislukurenkaan pääideaali. Seurauksen 2.7 mukaan on olemassa alkiot $x, y \in J$ jolle $\langle x, y \rangle = J$ ja vastaavasti $\langle \bar{x}, \bar{y} \rangle = \bar{J}$. Huomataan, että $\bar{J}J = \langle |x|^2, x\bar{y}, y\bar{x}, |y|^2 \rangle$. Olkoon b kokonaislukujen $|x|^2, |y|^2, x\bar{y} + \bar{x}y \in \mathbb{R}$ suurin yhteinen tekijä, jolloin

$$\langle b \rangle = \langle |x|^2, |y|^2, x\bar{y} + \bar{x}y \rangle.$$

Todistetaan, että $\bar{J}J$ on kokonaislukurenkaan pääideaali $\langle b \rangle$, todistamalla, että

$$x\bar{y}, y\bar{x} \in \langle b \rangle.$$

Todistetaan, että $x\bar{y} \in \langle b \rangle$. Huomataan, että $\frac{|x|^2|y|^2}{b^2}, \frac{x\bar{y}+y\bar{x}}{b} \in \mathbb{Z}$. Täten yhtälö

$$x^2 - \frac{x\bar{y} + y\bar{x}}{b} + \frac{|x|^2|y|^2}{b^2}$$

on kokonaislukukertoiminen. Sillä on ratkaisut $\frac{x\bar{y}}{b}$ ja $\frac{y\bar{x}}{b}$ eli

$$\frac{x\bar{y}}{b}, \frac{y\bar{x}}{b} \in \mathcal{O}_K.$$

Täten saadaan $x\bar{y}, y\bar{x} \in \langle b \rangle$ ja $J\bar{J}$ on kokonaislukurenkaan pääideaali.

Nyt, koska $I \subset J$, saadaan $I\bar{J} \subset \langle b \rangle$ ja kaikki ideaalin $I\bar{J}$ alkiot ovat jaollisia luvulla b. Olkoon $H = \{x \in \mathcal{O}_K : xb \in I\bar{J}\}$. Huomataan, että kaikille $h_1, h_2 \in H$ ja $r \in \mathcal{O}_\mathbb{K}$, koska $bh_1 + bh_2 \in I\bar{J}$, $h_1 + h_2 \in H$ ja, koska $brh_1 \in I\bar{J}$, $rh_1 \in H$. Täten H on ideaali ja saadaan ideaalitulo $\langle b \rangle H = I\bar{J}$. Nyt yhtälö $I\bar{J}J = I\langle b \rangle = \langle b \rangle HJ$ osoittaa, että $I = HJ$. □

2.2 Dedekindin rengas ja luokkaluku

Seuraavaksi käsitellään Dedekindin renkaita. Ne ovat renkaita joilla on tiettyjä lukuteorian kannalta hyödyllisiä ominaisuuksia. Jotta kuitenkin Dedekindin renkaat voidaan määritellä, määritellään ensin alkuideaali.

Määritelmä 2.9. Kommutatiivisen renkaan R epätriviaalia ideaalia $P \subsetneq R$ kutsutaan *alkuideaaliksi*, jos kaikille $a, b \in R$, joille $ab \in P$ pätee $a \in P$ tai $b \in P$.

Alkuideaali määrittyy luonnollisesti ideaalitulosta. Alkuideaalilla on tietyissä renkaissa alkuluvun kaltaisia ominaisuuksia, mikä on lukuteorian kannalta olennaista. Tätä varten määritellään Dedekindin rengas.

Määritelmä 2.10. Kokonaisaluetta R, jossa kaikki nollasta poikkeavat epätriviaalit ideaalit ovat uniikkeja äärellisiä alkuideaalien tuloja, kutsutaan *Dedekindin renkaaksi.*

Dedekindin renkaalla on useita yhtäpitäviä määritelmiä, mutta tämän tutkielman kannalta Dedekindin renkaan merkittävin määrittelevä ominaisuus on uniikki alkuideaaleihin jako. ([14], s.39, s.42) Dedekindin renkaassa alkuideaalit eivät sisälly muihin epätriviaalisiin ideaaleihin eli niitä kutsutaan maksimaalisiksi.

Lemma 2.11. *Olkoon R Dedekindin rengas. Alkuideaalille $P \subset R$ pätee $P \subset J$ vain jos ideaali $J = P$ tai $J = R$.*

Todistus. Olkoon $P \subsetneq J$. Lemman 2.8 mukaan on olemassa ideaali $I \subset R$ jolle $JI = P$. Jos ideaali J ei ole triviaali, sillä on uniikki alkuideaaleihinjako $J = P_1P_2 \dots P_n$ ja, koska $P \neq J$ ja $IJ = P$, I ei myöskään ole triviaali ja sillä on uniikki alkuideaaleihinjako $I = Q_1Q_2 \dots Q_m$. Nyt ideaalilla P on kaksi ei uniikkia alkuideaaleihinjakoa P ja $P_1P_2 \dots P_nQ_1Q_2 \dots Q_m$, mikä muodostaa ristiriidan Dedekindin renkaan määritelmän kanssa. □

Seuraavaksi huomioidaan, että lukukunnan kokonaislukurenkaalla on tämä hyödyllinen ominaisuus.

Lemma 2.12. *Lukukunnan kokonaislukurengas on Dedekindin rengas.*

Vaikka lukukuntien kokonaislukurenkaiden jako uniikkeihin alkuideaalien tuloihin on tämän tutkielman kannalta merkittävä ominaisuus, tuloksen perusteellinen todistaminen ei ole tämän tutkielman kannalta mielekästä. Todistus on esitty esimerkiksi lähteen [2] sivulla 394 sekä lähteen [14] sivulla 40.
Todistetaan seuraavaksi, että toisen asteen imaginäärisessä lukukunnassa valitsemalla minkä tahansa alkio $a \in I$ ideaali I voidaan esittää muodossa $I = \langle a, b \rangle$ jollain $b \in I$. Tulos on Lemman 2.7 vahvempi muoto, joka pätee erityisesti Dedekindin renkaassa. Tätä tulosta varten on hyödyllistä todistaa seuraavat lemmat.

Lemma 2.13. *Olkoot* $I = P_1^{\alpha_1}P_2^{\alpha_2}\dots P_n^{\alpha_n}$ *ja* $J = P_1^{\beta_1}P_2^{\beta_2}\dots P_n^{\beta_n}$ *toisen asteen lukukunnan kokonaislukurenkaan* $\mathcal{O}_K$ *ideaaleja joillain alkuideaaleilla* $P_1, P_2, \dots, P_n \subset \mathcal{O}_K$ *ja kokonaislukukertoimilla* $\alpha_i \geq 0$ *ja* $\beta_i \geq 0$. *Tällöin pätee*

$$I + J = \prod_{i=1}^{n} P_i^{\min\{\alpha_i, \beta_i\}}.$$

Todistus. Jos $I \subset J$, niin $I + J = J = P_1^{\beta_1}P_2^{\beta_2}\dots P_n^{\beta_n}$. Lisäksi Lemman 2.8 perusteella $\alpha_i \leq \beta_i$ kaikilla $1 \leq i \leq n$.

Oletetaan täten, että $I \not\subset J$ ja $J \not\subset I$. Huomioidaan aluksi

$$I + J = (\prod_{\beta_i > \alpha_i} P_i^{\beta_i} + \prod_{\alpha_i > \beta_i} P_i^{\alpha_i}) \prod_{i=1}^{n} P_i^{\min\{\alpha_i, \beta_i\}}.$$

Täten riittää todistaa, että

$$\prod_{\beta_i > \alpha_i} P_i^{\beta_i} + \prod_{\alpha_i > \beta_i} P_i^{\alpha_i} = \mathcal{O}_K.$$

Uniikin alkuideaaleihinjaon perusteella ideaalin $\prod_{\beta_i > \alpha_i} P_i^{\beta_i}$ kaikki tekijät ovat muotoa $\prod_{i \in A} P_i^{\beta_i}$ jollain $A \subset \{i \in \mathbb{N} : \beta_i > \alpha_i\}$. Koska

$$\prod_{\beta_i > \alpha_i} P_i^{\beta_i} \subset \prod_{\beta_i > \alpha_i} P_i^{\beta_i} + \prod_{\alpha_i > \beta_i} P_i^{\alpha_i},$$

Lemman 2.8 perusteella $\prod_{\beta_i > \alpha_i} P_i^{\beta_i} + \prod_{\alpha_i > \beta_i} P_i^{\alpha_i}$ on ideaalin $\prod_{\beta_i > \alpha_i} P_i^{\beta_i}$ tekijä, mutta koska $I \not\subset J$ ideaali $\prod_{\alpha_i > \beta_i} P_i^{\alpha_i}$ ei sisälly ideaaliin $\prod_{i \in A} P_i^{\beta_i}$ millään $A \neq \{0\}$. Täten

$$\prod_{\beta_i > \alpha_i} P_i^{\beta_i} + \prod_{\alpha_i > \beta_i} P_i^{\alpha_i} ? \mathcal{O}_K$$

ja lemma on todistettu. ([7], 124-125) □

Lemma 2.14. *Toisen asteen lukukunnan kokonaislukurenkaan nollasta poikkeaville ideaaleille* $J \subset I \subset \mathcal{O}_K$ *pätee* $I = J + \langle a \rangle$ *jollekin* $a \in J$.

Todistus. Olkoon $J = P_1^{\beta_1}P_2^{\beta_2}\dots P_n^{\beta_n}$ ideaaleihinjako joillain alkuideaaleilla $P_1, P_2, \dots, P_n \subset \mathcal{O}_K$ ja kokonaislukukertoimilla $\beta_i > 0$. Vastaavasti olkoon $I = P_1^{\alpha_1}P_2^{\alpha_2}\dots P_n^{\alpha_n}$ joillain kokonaisluvuilla $\beta_i \geq \alpha_i \geq 0$. Määritellään

$$I_i = I \prod_{j \in \{1,2,\dots,n\} - \{i\}} P_j$$

kaikilla $1 \leq i \leq n$ ja valitaan $a_i \in I_i - (I_i P_i)$. Esimerkiksi saadaan

$$a_1 \in (P_1^{\alpha_1} P_2^{\alpha_2+1} \dots P_n^{\alpha_n+1}) - (P_1^{\alpha_1+1} P_2^{\alpha_2+1} \dots P_n^{\alpha_n+1}).$$

Kaikilla $1 \leq i \leq n$ ideaali $\langle a_i \rangle$ voidaan esittää muodossa $I_i Q_i$ jollain ideaalilla Q_i, jolle P_i ei ole tekijä. Määritellään

$$H = \langle a_1 \rangle + \langle a_2 \rangle + \cdots + \langle a_n \rangle,$$

jolle pätee induktiolla lemman 2.13 mukaan

$$H = Q \prod_{i=1}^{n} P_i^{\alpha_i}$$

jollain ideaalilla Q, jonka uniikissa alkuideaaleihinjaossa ei esiinny yksikään ideaali P_i. Määritellään seuraavaksi

$$a = a_1 + a_2 + \cdots + a_n \in H.$$

Nyt $\langle a \rangle \subset H$ eli $\langle a \rangle = W \prod_{i=1}^{n} P_i^{\alpha_i}$ jollain ideaalilla $W \subset Q$. Jos P_i olisi ideaalin W tekijä jollain i, $P_i^{\alpha_i+1}$ olisi ideaalin $\langle a \rangle$ tekijä. Tällöin, koska $P_i^{\alpha_i+1}$ on ideaalien $\langle a_j \rangle$ tekijä kaikilla $j \neq i$, yhtälöistä

$$a_i = a - \sum_{j \in (\{1,2,\dots,n\} - \{i\})} a_j$$

ja $I_i Q_i = \langle a_i \rangle$ seuraa, että P_i on ideaalin Q_i tekijä muodostaen ristiriidan. Täten P_i ei ole ideaalin W tekijä millään i. Täten lemman 2.13 perusteella

$$J + \langle a \rangle = P_1^{\beta_1} P_2^{\beta_2} \dots P_n^{\beta_n} + P_1^{\alpha_1} P_2^{\alpha_2} \dots P_n^{\alpha_n} W = I.$$

([7], 125-126) □

Nyt Lemmasta 2.14 saadaan välittömästi haluttu hyödyllinen seuraus.

Seuraus 2.15. *Olkoon ideaali $I \subset \mathcal{O}_K$ ja sen alkio $a \in I$. On olemassa alkio $b \in I$, joille $\langle a, b \rangle = I$.*

Todistus. Valitsemalla jokin $a \in I - \{0\}$ saadaan, koska $\langle a \rangle \subset I$, lemman 2.14 perusteella $\langle a \rangle + \langle b \rangle = I$ jollain $b \in I$. □

Seuraavaksi on hyödyllistä laajentaa kunnan renkaan ideaalin määritelmää vastaaviin kunnan osajoukkoihin. Tätä varten tarvitaan seuraava algebrallinen määritelmä.

Määritelmä 2.16. Olkoon R rengas. Abelin ryhmä $(M, +)$ ja tulo-operaatio $\cdot : R \times M \to M$ muodostavat *R-moduulin*, jos kaikille $a, b \in R$ ja $x, y \in M$ pätee yhtälöt

$$r \cdot (x + y) = r \cdot x + r \cdot y,$$

$$(r + s) \cdot x = r \cdot x + s \cdot x,$$

$$(rs) \cdot x = r \cdot (s \cdot x)$$

ja

$$1 \cdot x = x.$$

R moduulin M osajoukko $N \subset M$ on R alimoduuli, jos N on ryhmän $(M, +)$ aliryhmä ja $r \cdot n \in N$ kaikilla $n \in N$ ja $r \in R$.

Alimoduulin määritelmällä voidaan laajentaa ideaalien teoriaa kunnan alkioihin renkaan ulkopuolella.

Määritelmä 2.17. Olkoon K lukukunta ja kokonaisalue $\mathcal{O}_K$ sen kokonaislukujen rengas. Kunnan K alimoduuli I on *murtoideaali*, jos on olemassa $r \in \mathcal{O}_K - \{0\}$ siten, että $\langle r \rangle I \subset \mathcal{O}_K$. Murtoideaalien joukkoa lukukunnassa K merkataan $\mathcal{M}_K$.
Murtoideaalien $I, J \subset K$ summa ja murtoideaalien tulo määritellään vastaavasti kuin ideaalisumma ja -tulo renkaassa

$$I + J = \{a + b : a \in I, b \in J\}$$

$$IJ = \{a_1 b_1 + a_2 b_2 + \cdots + a_n b_n : a_k \in I, b_k \in J, n \in \mathbb{N}\}.$$

Lemma 2.18. *Murtoideaalien $I, J \subset K$ summa ja tulo ovat murtoideaaleja.*

Todistus. Todistus vastaa lemman 2.4 todistusta. Täten riittää osoittaa, että murtoideaalien tulolla IJ ja summalla $I + J$ on kokonaislukurenkaan alkiot $x, y \in \mathcal{O}_K$, joille

$$\langle x \rangle IJ, \langle y \rangle (I + J) \subset \mathcal{O}_K.$$

Olkoon $a, b \in \mathcal{O}_K$ siten, että $\langle a \rangle I \subset \mathcal{O}_K$ ja $\langle b \rangle J \subset \mathcal{O}_K$. Lemman 2.5 mukaan

$$\langle ab \rangle (I + J) = \langle b \rangle \langle a \rangle I + \langle a \rangle \langle b \rangle J \subset \mathcal{O}_K$$

ja

$$\langle ab \rangle IJ = \langle a \rangle I \langle b \rangle J \subset \mathcal{O}_K.$$

Täten kokonaislukurenkaan alimoduuleille IJ ja $I + J$ on olemassa alkio $ab \in \mathcal{O}_K$, jolle $\langle ab \rangle IJ$ ja $\langle ab \rangle (I + J)$ ovat kokonaislukurenkaan ideaaleja. □

Huomataan, että $\mathcal{O}_K$ on kunnan K murtoideaalien tulon neutraalialkio. Murtoideaalit mahdollistavat kunnan ominaisuuksien tutkimisen renkaan ideaaleja laajemmin. Määritelmästä näkee välittömästi, että kokonaisluujen renkaan ideaalit ovat myös murtoideaaleja. Intuitiivisesti murtoideaalit käyttäytyvät jossainmäärin murtolukujen kaltaisella tavalla. Esimerkiksi murtoideaalille on murtoluvun nimittäjää vastaavaa alkio $\langle r\rangle \in R-\{0\}$, jolle rI on renkaan ideaali. Vastaavasti seuraava määritelmä vastaa intuitiivisesti käänteisluvun määritelmää.

Määritelmä 2.19. Olkoon K lukukunta, kokonaisalue R sen kokonaislukujen rengas ja I kunnan nollasta poikkeava ei triviaali murtoideaali. Murtoideaalin I *käänteisideaali* I^{-1} on murtoideaali, joka määritellään

$$I^{-1} = \{x \in K : \langle x\rangle I \subseteq R\}.$$

Huomioidaan, että toisen asteen imaginäärisessä lukukunnassa K nollasta poikkeavalle ei triviaalille ideaalille I, alkioille $a, b \in I^{-1}$ ja alkiolle $r \in \mathcal{O}_K$ pätee $\langle a+b\rangle I \subset \mathcal{O}_K$ ja $\langle ra\rangle I \subset \mathcal{O}_K$ eli $a+b, ra \in I^{-1}$. Lisäksi, koska murtoideaalin määritelmän perusteella jollain $m \in \mathcal{O}_K$ pätee $\langle m\rangle I \subset \mathcal{O}_K$ ja Lemman 2.7 perusteella jollain $c, d \in \mathcal{O}_K - \{0\}$ pätee $\langle m\rangle I = \langle c, d\rangle$, $\langle c\rangle \subset I$ ja täten $\langle c\rangle I^{-1} \subset \mathcal{O}_K$. Täten ollaan todistettu, että käänteisideaali I^{-1} on murtoideaali.

Lemma 2.20. *Olkoon K toisen asteen imaginäärinen lukukunta, $\mathcal{O}_K$ sen kokonaislukujen rengas ja I kunnan murtoideaali. Tällöin $II^{-1} = \mathcal{O}_K$.*

Todistus. Koska $\langle r\rangle I \subset \mathcal{O}_K$ jollain $r \in \mathcal{O}_K - \{0\}$ riittää osoittaa, että kokonaisalueen ideaalilla J pätee $JJ^{-1} = \mathcal{O}_K$.

Renkaasta $\mathcal{O}_K$ poikkeavalle kokonaislukuideaalille J on olemassa alkio $x \in K - \mathcal{O}_K$, jolle $\langle x\rangle J \subseteq \mathcal{O}_K$. Tämä voidaan todistaa valitsemalla nollasta poikkeava $a \in J$. Selkeästi $\langle a\rangle \subset J$. Lemman 2.8 mukaan $\langle a\rangle = HJ$ jollain kokonaislukurenkaan ideaalilla H. Koska Dedekindin renkaassa ideaalien $\langle a\rangle$ ja J tekijöihinjaot ovat uniikit, on alkuideaalit $P_1, P_2, \dots P_n,$, joille pätee $P_1P_2 \dots P_n = \langle a\rangle$. Nyt ideaalin J jokin alkuideaali on $P_k = P$ jollain indeksillä $1 \leq k \leq n$. Valitaan $P_n = P$. Voidaan valita $b \in (P_1 \dots P_{n-1}) - \langle a\rangle$. Määritellään alkio $x = a^{-1}b \notin \mathcal{O}_K$ ja

$$\langle x\rangle J \subset \langle a^{-1}\rangle\langle b\rangle P \subset \langle a^{-1}\rangle P_1 \dots P_{n-1}P_n = \langle a^{-1}\rangle\langle a\rangle = \mathcal{O}_K$$

Todistetaan nyt lemma antiteesillä. Jos $JJ^{-1} \neq \mathcal{O}_K$, ideaali JJ^{-1} on silti käänteisideaalin määritelmän mukaan kokonaislukuideaali ja täten on $x \in K - \mathcal{O}_K$ siten, että $\langle x\rangle JJ^{-1} \subset \mathcal{O}_K$. Täten käänteisideaalin J^{-1} määritelmän mukaan $\langle x\rangle J^{-1} \subset J^{-1}$ eli $\langle x\rangle^n J^{-1} \subset J^{-1}$ kaikilla kokonaisluvuilla

luvuilla $n > 0$. Nollasta poikkeaville alkioille $a \in J \subset \mathcal{O}_K$ ja $j \in J^{-1}$ pätee $ajx^n \notin \mathcal{O}_K$ jollain n. Tämä on ristiriita, koska $jx^n \in \langle x \rangle^n J^{-1} \subset J^{-1}$, jolloin käänteisideaalin määritelmän mukaan $ajx^n \in \mathcal{O}_K$ kaikilla $a \in J$. Täten $JJ^{-1} = \mathcal{O}_K$. □

Lemma mahdollistaa Dedekindin renkaassa ja erityisesti lukukunnassa yhtälön kertomisen puolittain käänteisideaalilla ideaalin hävittämiseksi. Määritellään vielä ideaaliluokka. Tämä on hyödyllinen käsite renkaan alkioiden tekijöihinjakoa tutkiessa.

Määritelmä 2.21. Olkoon R kokonaisalue, K sen murtolukujen kunta ja I sen murtoideaali. Joukko

$$I^{\#} = \{J \in \mathcal{M}_K : \langle a \rangle I = \langle b \rangle J, a, b \in R\}$$

on murtoideaalin I *ideaaliluokka*. Ideaaliluokkien joukkoa merkataan $\mathcal{J}_K$. Kunnan K *luokkaluku* on $|\mathcal{J}_K|$.

Luokkaluvun merkittävin ominaisuus on se, että toisen asteen imaginäärisen lukukunnan K kokonaislukurenkaassa $\mathcal{O}_K$ on nollasta poikkeaville alkioille luvun 1 juuria lukuun ottamatta yksikäsitteinen tekijöihinjako, jos ja vain jos kunnan K luokkaluku on 1.

Tämä johtuu siitä, että luokkaluvun ollessa 1 kaikille ideaaleille I pätee $I^{\#} = \mathcal{O}_K^{\#}$ eli ideaaliluokan määritelmän mukaan $I = \langle ba^{-1} \rangle \mathcal{O}_K$ jollain alkioilla $a, b \in \mathcal{O}_K$. Nyt kaikki kokonaislukurenkaan ideaalit ja erityisesti alkuideaalit ovat pääideaaleja.

Täten ideaalilla $\langle a \rangle \subset \mathcal{O}_K$, jossa $a \neq 0$, on Dedekindin renkaassa uniikki alkutekijöihinjako $\langle a \rangle = \langle p_1 \rangle \langle p_2 \rangle \dots \langle p_n \rangle \neq \langle 0 \rangle$. Nyt $a \in \langle p_1 \rangle \langle p_2 \rangle \dots \langle p_n \rangle$ eli $a = bp_1 p_2 \dots p_n$ jollain $b \in \mathcal{O}_K - \{0\}$.

Huomioimalla $|p_1 p_2 \dots p_n| \geq |xa|$ kaikilla $x \in \mathcal{O}_K - \{0\}$, jos b ei ole luvun 1 juuri, niin

$$|p_1 p_2 \dots p_n| < |xa|$$

kaikilla $x \in \mathcal{O}_K - \{0\}$. Tällöin $p_1 p_2 \dots p_n \notin \langle a \rangle$ muodostaen ristiriidan. Täten $a = bp_1 p_2 \dots p_n$ jollain luvun 1 juurella b.

Todistetaan vielä, että alkioiden p valinta on yksikäsitteistä luvun 1 juuria lukuun ottamatta. Olkoon alkuideaali $\langle p \rangle = \langle p' \rangle$. Tällöin $p = p'x$ ja $p' = py$ eli $p = pyx$ ja $xy = 1$ jollain $x, y \in \mathcal{O}_K$. Nyt x ja y ovat toisen asteen imaginäärisen lukukunnan kokonaislukurenkaan esityksen perusteella selvästi luvun 1 juuria ja täten kaikilla alkiolla $a \in \mathcal{O}_K$ on luvun 1 juuria lukuun ottamatta uniikki alkutekijöihinjako $a = p_1 p_2 \dots p_n$.

3 Kiinalainen jäännöslause ja Minkowskin lause

Tässä kappaleessa esitellään Kiinalainen jäännöslause ja Minkowskin lause, jotka ovat kaksi merkittävää lukuteorian lausetta.

3.1 Kiinalainen jäännöslause

Kiinalainen jäännöslause on todennäköisesti jo 200-luvulla muotoiltu lukuteorian lause, joka esiintyy keskeisesti ideaaliteoriassa. ([13], luku 5.3) Se on muotoiltu alunperin kokonaisluvuille, mutta tässä kappaleessa esitelty muotoilu ja seuraus 3.2 sekä niiden todistukset on esitelty lähteen [8] sivuilla 265, 266 ja 768.

Lause 3.1 (Kiinalainen jäännöslause (Sunzin lause))**.** *Olkoot I_1, I_2, ..., I_k kommutatiivisen renkaan R ideaaleja. Kuvaus*

$$\phi : R \to R/I_1 \times R/I_2 \times ... \times R/I_k$$

määriteltynä

$$\phi(r) = (r + I_1, r + I_2, ..., r + I_k)$$

on homomorfismi ja sen ydin on $I_1 \cap I_2 \cap \cdots \cap I_k$. Jos $I_i + I_j = R$ kaikilla $1 \leq i < j \leq k$, niin ϕ on surjektiivinen ja $I_1 \cap I_2 \cap \cdots \cap I_k = I_1 I_2 \dots I_k$.

Todistus. Todistetaan lause induktiolla.
Olkoon $k = 2$. Nyt kuvaus $\phi : R \to R/I_1 \times R/I_2$ on määritelty

$$\phi(r) = (r \bmod I_1, r \bmod I_2).$$

Koska ϕ on renkaan R projektio tekijäavaruuksien R/I_1 ja R/I_2 tuloavaruuteen, se on rengas-homomorfismi. Kuvauksen ydin muodostuu pisteistä, jotka ovat ideaaleissa I_1 ja I_2 eli ydin on $I_1 \cap I_2$.
Olkoon $I_1 + I_2 = R$. Täten on olemassa alkiot $a \in I_1$ ja $b \in I_2$ siten, että $a + b = 1$. Nyt, koska alkio $a = 1 - b \in 1 + I_2$, saadaan $\phi(a) = (0, 1)$ ja vastaavasti $\phi(b) = (1, 0)$. Täten kaikille pisteille

$$(r_1 \bmod I_1, r_2 \bmod I_2) \in R/I_1 \times R/I_2$$

on olemassa piste $r_2 a + r_1 b \in R$ siten, että

$$\begin{aligned} \phi(r_2 a + r_1 b) &= \phi(r_2)\phi(a) + \phi(r_1)\phi(b) \\ &= (r_2 \bmod I_1, r_2 \bmod I_2)(0, 1) + (r_1 \bmod I_1, r_1 \bmod I_2)(1, 0). \\ &= (r_1 \bmod I_1, r_2 \bmod I_2) \end{aligned}$$

Täten kuvaus ϕ on surjektio.
Lopulta huomioidaan, että pisteelle $c \in I_1 \cap I_2$ pätee $c = c1 = ca + cb$, jollain $a + b = 1$ siten, että $a \in I_1$ ja $b \in I_2$. Nyt $ca, cb \in I_1 I_2$ ja täten $I_1 \cap I_2 \subseteq I_1 I_2$ todistaen lauseen, kun $k = 2$.
Oletetaan että lause pätee, kun $k = n - 1$. Olkoon $k = n$. Nyt saadaan $\phi(r) = (\phi_{n-1}(r), r \bmod I_n)$. Koska projektio renkaasta R joukkoon R/I_n on homomorfismi ja oletuksen mukaan ϕ_{n-1} on homomorfismi, kuvaus ϕ on myös homomorfismi, jonka ydin on ideaalien I_j leikkaus. Olkoon $I_i + I_j = R$ kaikilla $1 \leq i < j \leq n$. Nyt kaikille $1 \leq i < n$ on olemassa $a_i \in I_i$ ja $b_i \in I_n$ siten, että $a_i + b_i = 1$. Täten

$$1 = \prod_{i=1}^{n-1} (a_i + b_i) \in (I_1 \dots I_{n-1}) + I_n.$$

Tämä todistaa, että $(I_1 \dots I_{n-1}) + I_n = R$. Nyt vastaavalla päättelyllä kuin kohdassa $k = 2$, kuvaus ϕ on surjektio ja $(I_1 \dots I_{n-1}) \cap I_n \subseteq I_1 \dots I_n$. Täten induktio-oletuksen perusteella $I_1 \cap I_2 \cap \dots \cap I_n \subseteq I_1 \dots I_n$ viimeistellen todistuksen. □

Kiinalainen jäännöslause on merkittävä lukuteoreettinen tulos, joka esiintyy useissa konteksteissa. Se muotoillaan tyypillisesti algebrallisessa lukuteoriassa yllä esitetyllä tavalla ideaaleille. Tässä työssä relevantteja ovat seuraavat lauseesta johdetut seuraukset.

Seuraus 3.2. *Olkoon I_1, I_2, ..., I_k renkaan R ideaaleja. Jos $I_i + I_j = R$ kaikilla $1 \leq i < j \leq k$, niin*

$$R/(I_1 I_2 \dots I_k) = R/(I_1 \cap I_2 \cap \dots \cap I_k) \cong R/I_1 \times R/I_2 \times \dots \times R/I_k.$$

Todistus. Ensimmäinen yhtäsuuruus tulee suoraan Kiinalaisesta jäännöslauseesta ja koska funktion $\phi : R \to R/I_1 \times R/I_2 \times \dots \times R/I_k$ määriteltynä

$$\phi(r) = (r + I_1, r + I_2, ..., r + I_k)$$

ydin on $I_1 \cap I_2 \cap \dots \cap I_k$, renkaat $R/(I_1 \cap I_2 \cap \dots \cap I_k)$ ja $R/I_1 \times R/I_2 \times \dots \times R/I_k$ ovat isomorfiset. □

3.2 Ideaalin normi

Lukuteorian kannalta on hyödyllistä vertailla ideaalien kokoja. Tätä varten määritellään kokonaislukurenkaan ideaalin normi.

Määritelmä 3.3. Olkoon K imaginäärinen lukukunta ja $I \subset \mathcal{O}_K$ nollasta poikkeava ideaali. Ideaalin normi määritellään

$$N(I) = n \in [1, \infty]$$

siten, että $I\bar{I} = \langle n \rangle$, missä $\bar{I}$ on ideaalin I alkioiden konjugaattien muodostama ideaali.

Nyt imaginäärisessä lukukunnassa K pätee $N(n\mathcal{O}_K) = n^2$ kaikilla $n \in \mathbb{Z}$. Erityisesti $N(\mathcal{O}_K) = 1$. Huomioidaan myös, että imaginäärisellä ideaalilla ja sen alkioiden konjugaattien muodostamalla ideaalilla on sama normi $N(I) = N(\bar{I})$. Kokonaislukurenkaan ideaalin normi määrittyy hyvin luonnollisesti ja sillä on käteviä ominaisuuksia. Erityisesti ideaalinormi ja sen ominaisuudet ovat hyödyksi Minkowskin lauseen todistuksessa. Aloitetaan määrittämällä ideaalinormin ja ideaalitulon yhteys. Verrataan lisäksi toisen asteen lukukunnan pääideaalin normia kompleksiluvun normiin. Käyttämällä kiinalaisen jäännöslauseen seurauksia tulokset saadaan todistettua. On lisäksi tärkeää huomioida, että $N(I) = \#(\mathcal{O}_K/I)$. ([2], s.398)

Lemma 3.4. *Olkoon kokonaislukurenkaan ideaalien I ja J normit äärelliset. Tällöin $N(IJ) = N(I)N(J)$*

Todistus. Olkoon $N(I) = n$ ja $N(J) = m$. Tällöin ideaalin normin määritelmän mukaan $I\bar{I} = \langle n \rangle$ ja $J\bar{J} = \langle m \rangle$. Nyt

$$IJ\overline{IJ} = I\bar{I}J\bar{J} = \langle n \rangle \langle m \rangle = \langle nm \rangle$$

ja täten $N(IJ) = nm = N(I)N(J)$. ([7], s.397) □

Lemma 3.5. *Imaginäärisen toisen asteen lukukunnan kokonailukurenkaan $\mathcal{O}_K$ pääideaalin normille pätee $N(\langle a \rangle) = |a|^2$.*

Todistus. Huomioidaan aluksi, että $N(\langle a \rangle) = N(\langle \bar{a} \rangle)$. Tällöin

$$N(\langle a \rangle)^2 = N(\langle a \rangle)N(\langle a \rangle) = N(\langle a \rangle)N(\langle \bar{a} \rangle).$$

Nyt Lemman 3.4 perusteella

$$N(\langle a \rangle)N(\langle \bar{a} \rangle) = N(\langle |a|^2 \rangle) = N(\langle |a| \rangle)^2.$$

Täten riittää todistaa lemma kokonaisluvulle $a \in \mathbb{Z}$. Nyt kokonaisluvulle a pätee ideaalin normin määritelmän perusteella $N(\langle a \rangle) = a^2$. □

3.3 Minkowskin lause

Minkowskin lause on toinen lukuteoriaan keskeinen lause. Se on alunperin muotoiltu vuonna 1910 Hermann Minkowskin teoksessa Geometrie der Zahlen.[15] Tämä lauseen alkuperäinen muotoilu on kuitenkin yleisempi, kuin mitä tässä tutkielmassa tarvitaan. Täten lause ja sen seuraukset muotoillaan vain toisen asteen imaginäärisessä lukukunnassa.

Lause 3.6 (Minkowski lause)**.** *Olkoon $\mathcal{O}_K \subset \mathbb{R}^2$ algebrallisten kokonaislukujen hila toisen asteen imaginäärisessä lukukunnassa K sekä olkoon Δ kokonaislukujen hilan perussuunnikkaan pinta-ala. Konveksi origon suhteen symmetrinen joukko, jonka pinta-ala on suurempi kuin 4Δ sisältää vähintään yhden kokonaislukupisteen.*

Todistus. Todistetaan lause geometrisesti tulkitsemalla $\mathcal{O}_K$ avaruuden $\mathbb{R}^2$ hilana. Olkoon A konveksi origon suhteen symmetrinen joukko, jonka tilavuus on suurempi kuin 4Δ. Nyt joukon

$$B = \left\{ (\frac{x_1}{2}, \frac{x_2}{2} : (x_1, x_2) \in A \right\}$$

pinta-ala on suurempi kuin Δ. Täten tekijäkuvaus $x \mapsto x + \mathcal{O}_K$ kuvaa jotkin joukon B pisteet $a = (a_1, a_2) \neq b = (b_1, b_2)$ samaksi pisteeksi. Nyt saadaan $b - a \in \mathcal{O}_K - \{0\}$. Olkoon $x = (-2a_1, -2a_2)$ ja $y = (2b_1, 2b_2)$. Joukon B määritelmän ja origon suhteen symmetrisyyden perusteella $x, y \in A$. Pisteiden välinen keskipiste

$$\frac{x+y}{2} = \frac{(2b_1 - 2a_1, 2b_2 - 2a_2)}{2} = b - a \in \mathcal{O}_K - \{0\}$$

on konveksisuuden takia myös joukossa A. Täten A sisältää kokonaislukupisteen. □

Vaikka Minkowskin lause vaikuttaa puhtaasti geometriselta, koska kokonaislukurenkaan ideaali muodostavaa hilan, se on hyvin hyödyllinen tutkiessa ideaaleja. Minkowskin lauseen seurauksena voidaan arvioida raja kokonaislukurenkaan ideaalin normille. Seuraava lause ja sen todistus perustuvat lähteen [3] luvussa 5.3 esitettyyn yleisesti lukukuntiin pätevään lauseeseen. Tässä tutkielmassa esitetään lause suppeammin toisen asteen imaginäärisessä lukukunnassa.

Lause 3.7 (Minkowski epäyhtälö)**.** *Imaginäärisen toisen asteen lukukunnan nollasta poikkeavalle murtoideaalille I on ideaali $J \subseteq \mathcal{O}_{\mathbb{Q}(\sqrt{-d})}$ siten, että $J \in I^{\#}$ ja*

$$N(J) \leq \frac{2}{\pi}|D|^{1/2} = M,$$

missä D on lukukunnan diskriminantti.

Todistus. Aloitetaan todistamalla ideaalinormista riippuva yläraja kokonaislukujen renkaan ideaalin $I \subset \mathcal{O}_{\mathbb{Q}(\sqrt{-d})}$ alkiolle.

Olkoon ideaali $I \subset \mathcal{O}_{\mathbb{Q}(\sqrt{-d})}$ ja $B_t = \{z \in \mathbb{C} : 2|z| \leq t\}$ origon suhteen symmetrinen kiekko, jonka pinta-ala $V(B_t) = \frac{t^2\pi}{4}$. Nyt valitaan t siten, että kiekon pinta-alalle pätee $V(B_t) = 4\Delta_I$, missä Δ_I on ideaalin I perussuunnikkaan pinta-ala. Huomioidaan, että kokonaislukujen renkaan ideaalin I perussuunnikkaan pinta-alalle pätee

$$\Delta_I = \Delta\#(\mathcal{O}_{\mathbb{Q}(\sqrt{-d})}/I) = \Delta N(I),$$

missä Δ on kokonaislukujen renkaan perussuunnikkaan pinta-ala. Täten saadaan $V(B_t) = 4N(I)\Delta$. Jos $d \not\equiv 1 \bmod 4$, perussuunnikkaan pinta-ala on $\Delta = \sqrt{|d|} = \frac{\sqrt{D}}{2}$ ja muutoin $\Delta = \mathrm{Im}(\frac{1+\sqrt{d}}{2}) = \frac{\sqrt{|d|}}{2} = \frac{\sqrt{D}}{2}$. Yhdistämällä yhtälöt saadaan

$$t^2 = \frac{8}{\pi}\sqrt{D}N(I).$$

Huomioidaan, että lauseen 3.6 mukaan on piste $z' \in B_t \cap I$. Joukon B_t määritelmän mukaan $|z'| \leq \frac{t}{2}$. Saadaan epäyhtälö

$$|z'|^2 \leq \frac{2}{\pi}\sqrt{D}N(I). \tag{3.1}$$

Nyt voimme todistaa lauseen. Olkoon $J \neq \langle 0\rangle$ murtoideaali. Murtoideaalin määritelmän mukaan on olemassa pääideaali $\langle a\rangle$, jolle pätee yhtälö $J^{-1}\langle a\rangle \subset \mathcal{O}_{\mathbb{Q}(\sqrt{-d})}$. Ideaaliluokan määritelmästä nähdään $J^{\#} = (J\langle a\rangle^{-1})^{\#}$. Selkeästi $(J\langle a\rangle^{-1})^{-1} = J^{-1}\langle a\rangle$ ja täten voidaan valita ideaaliluokan edustaja J, jolle J^{-1} on kokonaislukujen renkaan ideaali. Nyt valitaan piste $z \in J^{-1}$, joka toteuttaa epäyhtälön 3.1. Olkoon ideaali $I = \langle z\rangle J \in J^{\#}$. Huomataan, että, koska $\langle z\rangle \subset J^{-1}$ pisteelle $x \in I$, pätee $x \in J$ ja $x \in J^{-1}$ eli $x \in J^{-1}J = \mathcal{O}_{\mathbb{Q}(\sqrt{-d})}$. Täten I on myös kokonaislukujen renkaan ideaali. Lisäksi lemmojen 3.4 ja 3.5 perusteella

$$N(I)N(J^{-1}) = N(\langle z\rangle) = |z|^2 \leq \frac{2}{\pi}\sqrt{D}N(J^{-1})$$

ja täten supistamalla $N(J^{-1})$ lause on todistettu. □

Minkowskin lause ja epäyhtälö esitetään tyypillisesti yleisessä $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ avaruudessa, mutta tämän työn kannalta, toisen asteen imaginääristen lukukuntien tapaus on riittävä. Epäyhtälön ylärajan tarkka arvo ei ole tässä tutkielmassa merkittävä. On riittävää tietää, että normin yläraja on vain lukukunnasta riippuva äärellinen luku.

3.4 Luokkaluvun ominaisuudet

Seuraavaksi todistetaan toisen asteen imaginäärisen lukukunnan luokkaluvulle muutama hyödyllinen ominaisuus. Aloitetaan todistamalla Minkowskin epäyhtälöä käyttäen, että luokkaluku on äärellinen.

Lemma 3.8. *Olkoon K toisen asteen imaginäärinen lukukunta. Ideaaliluokkien joukko $\mathcal{J}_K$ on äärellinen.*

Todistus. Lauseen 3.7 mukaan jokaisessa ideaaliluokassa on kokonaislukujen renkaan ideaali I, jolle

$$N(I) \leq \frac{2}{\pi}|D|^{1/2} = M.$$

Täten riittää osoittaa, että on äärellinen määrä ideaaleja I, joille $N(I) \leq M$. Tulkiten ideaalia I hilana

$$N(I) = \#(\mathcal{O}_K/I) = [\mathcal{O}_K : I].$$

Täten riittää todistaa, että on äärellinen määrä hiloja $L \subset \mathcal{O}_K$, joille hilaindeksi $[\mathcal{O}_K : L] \leq M$.
Olkoon $[\mathcal{O}_K : L] = n$. Täten tekijäavaruudessa $\mathcal{O}_K/L$ on n alkiota, eli tekijäavaruudessa $x = x + n$. Nyt kaikille $a \in \mathcal{O}_K/L$ pätee $na = 0$. Täten $an \in L$ kaikilla $a \in \mathcal{O}_K$ eli $n\mathcal{O}_K \subset L$. Osoitetaan, että on äärellinen määrä hiloja L joille pätee $n\mathcal{O}_K \subset L \subseteq \mathcal{O}_K$. Olkoon P hilan $n\mathcal{O}_K$ perussuunnikas, jonka kärjet ovat joukossa

$$\{0, \alpha_1, \alpha_2, \alpha_1 + \alpha_2\}.$$

Nyt joukossa $\mathcal{O}_K \cap P$ on geometrisesti tarkasteltuna korkeintaan $(n+1)^2$ pistettä ja täten joukossa $L \cap P$ on myös äärellinen määrä pisteitä. Nyt pisteelle $a \in L$ pätee tekijäavaruudessa tutkittuna yhtälö

$$a + n\mathcal{O}_K = b + n\mathcal{O}_K$$

jollain $b \in L \cap P$. Täten hila L voidaan esittää muodossa

$$L = \{l + z \in \mathcal{O}_K : l \in (L \cap P), z \in n\mathcal{O}_K\}.$$

Täten hila L, jonka indeksi on n, voidaan määritellä uniikisti joukon $\mathcal{O}_K \cap P$ pisteillä. Koska on olemassa vain äärellinen määrä permutaatioita pisteitä joukossa $\mathcal{O}_K \cap P$, on olemassa vain äärellinen määrä uniikkeja hiloja

$$L = (L \cap P) + n\mathcal{O}_K.$$

([2], s.406, s.430) □

Lemma 3.9. *Toisen asteen imaginäärisen lukukunnan K ideaaliluokkien joukko $\mathcal{J}_K$ varustettuna ideaaliluokkien tulolla $I^{\#}J^{\#} = (IJ)^{\#}$ on Abelin ryhmä.*

Todistus. Ideaaliluokkien tulo määrittyy ideaalitulon kautta ja on täten liitännäinen ja vaihdannainen. Koska murtoideaalien tulo on murtoideaali, ideaaliluokkien tulo on myös ideaaliluokka. Ideaaliluokkien ryhmän neutraalialkio on $\mathcal{O}_K^{\#}$, koska kaikille murtoideaaleille $I \subset K$ pätee

$$\mathcal{O}_K^{\#} I^{\#} = (\mathcal{O}_K I)^{\#} = I^{\#}.$$

Lopulta huomioidaan, että ideaaliluokalle $I^{\#}$ on olemassa käänteisalkio $(I^{-1})^{\#}$ eli $I^{\#}(I^{-1})^{\#} = (II^{-1})^{\#} = \mathcal{O}_K^{\#}$. □

Nyt, koska luokkaluku on äärellinen kokonaisluku, kaikille ideaaliluokkien ryhmän alkioille $I^{\#}$ on olemassa kokonaisluku n jolle $(I^{\#})^n = (I^n)^{\#} = \mathcal{O}_K^{\#}$. Todistetaan seuraavaksi ideaaliluokille esitys murtoideaalien avaruutena.

Lemma 3.10. *Olkoon K toisen asteen imaginäärinen lukukunta $\mathcal{J}_K$ sen ideaaliluokkien ryhmä ja $\mathcal{M}_K$ sen murtoideaalien joukko. Tällöin*

$$\mathcal{J}_K = \mathcal{M}_K/(K - \{0\}).$$

Todistus. Ideaaliluokan määritelmän mukaan ideaaleille $I, J \subset K$ on olemassa kokonaisluvut $a, b \in \mathcal{O}_K - \{0\}$, joille $\langle a\rangle I = \langle b\rangle J$ eli $I = \langle a\rangle^{-1}\langle b\rangle J$, jos ja vain jos J ja I kuuluvat samaan ideaaliluokkaan. Käänteisideaalin määritelmästä nähdään, että $\langle a\rangle^{-1} = \langle \frac{1}{a}\rangle$. Täten $I = \langle \frac{b}{a}\rangle J$, jos ja vain jos $J \in I^{\#}$. □

Lemma antaa paremman käsityksen ideaaliluokkien avaruudesta ja mahdollistaa Riemannin pallon pisteen ideaaliluokkan yhdistämisen.

4 Hyperbolinen geometria

Seuraavissa kappaleissa käsitellään algebrallisia ominaisuuksia hyperbolisessa avaruudessa. Täten on hyvä määritellä tarvittavia ominaisuuksia hyperbolisessa geometriassa. n-ulotteinen hyperbolinen avaruus on luokka metrisiä avaruuksia $(\mathbb{H}^n, d)$, jotka ovat isometrisiä keskenään. ([16], s. 49) Tässä tutkielmassa käsitellään kolmiuloitteista hyperbolista geometriaa puoliavaruusmallissa.

4.1 Hyperbolisen avaruuden määritelmä

Määritelmä 4.1. Hyperbolinen avaruus on $\mathbb{C}\times\mathbb{R}^+$, jonka pisteitä merkitään $P = (p_1, p_2, p_3) = z + jr$, missä $z = x + iy \in \mathbb{C}, r \in \mathbb{R}^+$, varustettuna hyperbolisella metriikalla

$$d((p_1,p_2,p_3),(q_1,q_2,q_3)) = \operatorname{arcosh}\Big(1 + \frac{|((p_1,p_2,p_3)-(q_1,q_2,q_3)|^2}{2p_3q_3}\Big) \in [0,\infty[.$$

Yllä määriteltyä metriikkaa kutsutaan hyperboliseksi metriikaksi. Hyperbolisella metriikalla varustetulla puoliavaruudella on euklidisesta avaruudesta poikkeavia algebrallisesti hyödyllisiä ominaisuuksia. Hyperbolisessa avaruudessa geodesinen suora on joko kompleksitasoon ortogonaalinen suora tai Euklidinen ympyrän, jonka keskipiste on kompleksitasossa, kaaren puolikas. Vastaavasti hyperboliset tasot ovat kompleksitason kanssa ortogonaalisia Euklidisia tasoja tai Euklidisia puolipallojen, joiden keskipisteet ovat kompleksitasossa, reunoja. Hyperbolinen taso jakaa avaruuden kahteen hyperboliseen puoliavaruuteen. Lisäksi hyperbolisen monitahokkaat ovat hyperbolisten puoliavaruuksien leikkauksia. ([16], luku 5.3)

Hyperbolisen geometrian kannalta on hyödyllistä tutkia avaruutta rajaavaa kompleksitasoa äärettömyyspisteellä laajennettuna. Jotta kompleksitasoa olisi helpompi käsitellä, määritellään projektiivinen kompleksiavaruus.

Määritelmä 4.2. Projektiivinen kompleksiavaruus $\mathbb{P}^n(\mathbb{C})$ on joukko pisteiden $z \in \mathbb{C}^{n+1} - \{0\}$ ekvivalenssiluokkia määrittäen, että kompleksiavaruuden pisteet $z, z' \in \mathbb{C}^{n+1} - \{0\}$ ovat ekvivalentit, jos $z = \lambda z'$ jollain $\lambda \in \mathbb{C} - \{0\}$. Määritellään Riemannin pallo projektiiviseksi kompleksiavaruudeksi $\mathbb{P}^1\mathbb{C}$. Pisteen $(z_1, z_2) \in \mathbb{C}^2 - \{0\}$ ekvivalenssiluokkaa merkitään $[z_1, z_2]$ ja määritellään ekvivalenssi $[z_1, z_2] = [\lambda z_1, \lambda z_2]$ kaikilla $\lambda \in \mathbb{C} - \{0\}$.

Huomioidaan nyt, että Riemannin pallo $\mathbb{P}^1\mathbb{C}$ ja äärettömyyspisteellä laajennettu kompleksitaso $\mathbb{C}\cup\{\infty\}$ ovat isometriset esimerkiksi kuvaamalla piste $[z_1, z_2]$ pisteeksi $\frac{z_1}{z_2}$, kun $z_2 \neq 0$ ja piste $[z_1, 0]$ pisteeksi ∞. ([5], luku 1.3)

4.2 $\mathbf{PSL}_2(\mathbb{C})$ -kuvaukset

Tutkitaan seuraavaksi joitain hyödyllisiä hyperbolisen puoliavaruuden isometrioita. Täten on tarkeää huomioida hyperbolisen puoliavaruuden isometrioiden ryhmän ominaisuuksia. Aloitetaan määrittelemällä erityinen ryhmä matriiseja.

Määritelmä 4.3. Olkoon R rengas. Renkaan yleinen lineaarinen ryhmä $\mathbf{GL}_n(R)$ on ryhmä, joka muodostuu $n \times n$ matriiseista, joilla on kääntei-

salkio ja joiden alkiot ovat renkaassa R. Vastaavasti renkaan erityinen lineaarinen ryhmä $\mathbf{SL}_n(R)$ on $n \times n$ matriisien ryhmä, joiden alkiot ovat renkaassa R ja joiden determinantti on 1. Projektiivinen erityinen lineaarinen ryhmä $\mathbf{PSL}_n(R)$ on $\mathbf{SL}_n(R)/\mathbf{SZ}_n(R)$. $\mathbf{SZ}_n(R)$ on $n \times n$ matriisien skalaarikuvausten, joiden determinantti on 1, ryhmä, eli matriisien $a \cdot I$ ryhmä, missä I on identiteettimatriisi ja alkiolle $a \in R$ pätee $a^n = 1$. Erityisesti $\mathbf{SL}_n(\mathbb{C})$ on vastaavalla tavalla $n \times n$ matriisien ryhmä, jonka alkiot ovat kompleksilukuja. $\mathbf{PSL}_n(\mathbb{C})$ määritellään tekijäavaruutena $\mathbf{SL}_n(\mathbb{C})/\mathbf{SZ}_n(\mathbb{C})$, missä $\mathbf{SZ}_n(\mathbb{C})$ on $n \times n$ matriisien skalaarikuvausten ryhmä, joiden determinantti on 1 ja joiden alkiot ovat kompleksilukuja.

Tässä työssä on erityisen hyödyllistä käsitellä joukkoa $\mathbf{PSL}_2(\mathcal{O}_K)$. On täten hyvä huomioida, että toisen asteen lukukunnan kokonaislukujen renkaassa $\mathcal{O}_K$ pätee $\mathbf{SZ}_2(\mathcal{O}_K) = \left\{ \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}$. Lisäksi on tärkeää huomioida, että toisen asteen lukukunnan kokonaislukurenkaan yleisen lineaarisen ryhmän $\mathbf{GL}_n(\mathcal{O}_K)$ matriisien determinantit ovat luvun 1 juuria. Määritellään nyt joukolle $\mathbf{SL}_2(\mathbb{C})$ kuvaus Riemannin pallolla.

Määritelmä 4.4. Olkoon $a, b, c, d \in \mathbb{C}$ siten, että $ad \neq bc$. Määritellään kuvaus $\mathbb{C} \cup \infty \to \mathbb{C} \cup \infty$ $z \mapsto \frac{az+b}{cz+d}$, kun $z \notin \{\frac{-d}{c}, \infty\}$. Lisäksi määritellään $\frac{-d}{c} \mapsto \infty$ ja $\infty \mapsto \frac{a}{c}$. Kuvausta kutsutaan *Möbius-kuvaukseksi*.

Möbius-kuvaus on hyperbolisilta ominaisuuksiltaan geometrisesti merkittävä kuvausten luokka. ([11], luvut 1.7, 1.8, 2.7) Möbiuskuvausten esitys, ei ole uniikki, esimerkiksi $(z \mapsto z) = (z \mapsto \frac{az}{a})$ kaikilla $a \in \mathbb{C}$. Todistetaan seuraavaksi, että Möbiuskuvaukset muodostavat ryhmän $\mathbf{PSL}_2(\mathbb{C})$ kanssa isomorfisen ryhmän.

Lemma 4.5. *Möbiuskuvaukset varustettuna yhdistetyllä kuvauksella muodostavat ryhmän* **Möb**.

Todistus. Yhdistetyt kuvaukset ovat liitännäisiä. Lisäksi huomataan, että Möbiuskuvaus $z \mapsto \frac{z+0}{0z+1} = z$ on selkeästi identiteetti. Täten riittää todistaa, että kuvaukselle $T(z) = \frac{az+b}{cz+d}$ on olemassa käänteiskuvaus, joka on Möbiuskuvaus. Määritellään

$$T' = \frac{-dz + b}{cz - a}.$$

Nyt, jos $z \notin \{\frac{-d}{c}, \infty\}$, saadaan

$$T'(T(z)) = \frac{-adz - bd + bcz + bd}{acz + cb - acz - ad} = z\frac{bc - ad}{cb - ad} = z.$$

Lisäksi määritelmän mukaan

$$T'(T(\infty)) = T'(\frac{a}{c}) = \infty$$

ja

$$T'(T(\frac{-d}{c})) = T'(\infty) = (\frac{-d}{c}).$$

Täten $T' = T^{-1}$ todistaen lemman. □

Lemma 4.6. *Kuvaus* $\Phi : \mathbf{SL}_2(\mathbb{C}) \to \mathbf{M\ddot{o}b}$ *määriteltynä*

$$\Phi(\begin{pmatrix} a & b \\ c & d \end{pmatrix}) = (z \mapsto \frac{az+b}{cz+d})$$

on surjektiivinen homomorfismi, jonka ydin on $\left\{ \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}$.

Todistus. Aloitetaan todistamalla surjektiivisuus. Alkioille $a, b, c, d \in \mathbb{C}$, joille $ad - bc \neq 0$ on olemassa $\lambda \in \mathbb{C}$, jolle $\lambda^2 = \frac{1}{ad-bc}$. Nyt kaikille kuvauksille $(z \mapsto \frac{az+b}{cz+d} = \frac{\lambda az+\lambda b}{\lambda cz+\lambda d})$ on olemassa matriisi $\begin{pmatrix} \lambda a & \lambda b \\ \lambda c & \lambda d \end{pmatrix} \in \mathbf{SL}_2(\mathbb{C})$, jolle $\Phi(\begin{pmatrix} \lambda a & \lambda b \\ \lambda c & \lambda d \end{pmatrix}) = \frac{az+b}{cz+d}$.
Todistetaan seuraavaksi, että kuvaus on homomorfismi. Olkoot

$$\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}, \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} \in \mathbf{SL}_2(\mathbb{C}).$$

Huomioidaan aluksi yhtälö

$$\begin{aligned} \Phi(\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix}) &= \Phi(\begin{pmatrix} a_1a_2 + b_1c_2 & a_1b_2 + b_1d_2 \\ c_1a_2 + d_1c_2 & c_1b_2 + d_1d_2 \end{pmatrix}) \\ &= (z \mapsto \frac{(a_1a_2 + b_1c_2)z + a_1b_2 + b_1d_2}{(c_1a_2 + d_1c_2)z + c_1b_2 + d_1d_2}). \end{aligned}$$

Tutkitaan nyt Möbiuskuvausten $z \mapsto \frac{a_1z+b_1}{c_1z+d_1}$ ja $z \mapsto \frac{a_2z+b_2}{c_2z+d_2}$ yhdistettyä kuvausta:

$$\begin{aligned} \frac{a_2z + b_2}{c_2z + d_2} &\mapsto \frac{a_1\frac{a_2z+b_2}{c_2z+d_2} + b_1}{c_1\frac{a_2z+b_2}{c_2z+d_2} + d_1} \\ &= \frac{a_2a_1z + b_2a_1 + c_2b_1z + b_2d_1}{c_1a_2z + b_2c_1 + c_2d_1z + d_2d_1} \\ &= \frac{(a_1a_2 + b_1c_2)z + a_1b_2 + b_1d_2}{(c_1a_2 + d_1c_2)z + c_1b_2 + d_1d_2} \end{aligned}$$

täten osoittaen, että $\Phi(\gamma) \circ \Phi(\gamma') = \Phi(\gamma\gamma')$ kaikilla $\gamma, \gamma' \in \mathbf{SL}_2(\mathbb{C})$.
Lopulta huomioidaan, että kuvauksen ytimen muodostavat matriisit

$$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \in \left\{ \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}.$$

□

Täten $\mathbf{SL}_2(\mathbb{C})$ on ryhmä ja ryhmät $\mathbf{M\ddot{o}b}$ ja $\mathbf{PSL}_2(\mathbb{C})$ ovat isomorfisia. On myös hyvä huomioida, että matriisille $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{SL}_2(\mathcal{O}_K)$ käänteisalkiolle pätee $\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \begin{pmatrix} -d & b \\ c & -a \end{pmatrix} \in \mathbf{SL}_2(\mathcal{O}_K)$. Lisäksi, koska $0, 1 \in \mathcal{O}_K$, identiteettimatriisi kuuluu joukkoon $\mathbf{SL}_2(\mathcal{O}_K)$ ja täten se on ryhmän $\mathbf{SL}_2(\mathbb{C})$ aliryhmä. Jotta Möbiuskuvauksia voidaan käyttää hyödyksi hyperbolisessa geometriassa, on hyvä määritellä joitain hyperbolisen puoliavaruuden isometrioita.

Lemma 4.7. *Olkoon $P = z + jr \in \mathbb{H}$. Kuvaukset*

- $T_b(P) = P + b$, *missä* $b \in \mathbb{C}$
- $L_\lambda(z + jr) = \lambda z + j|\lambda| r$, *missä* $\lambda \in \mathbb{C}$
- $S(P) = \frac{P}{|P|^2}$
- $U(z + jr) = \bar{z} + jr$

sekä näiden kuvausten yhdistetyt kuvaukset ovat kolmiulotteisen hyperbolisen avaruuden isometrioita.

Todistus. Todistus perustuu lähteen [16] sivuihin 59 ja 60.

Todistetaan yksi kerrallaan, että kuvaukset ovat isometrioita:

- $d(T_b(x), T_b(y)) = \operatorname{arcosh}\left(1 + \dfrac{|(x+b) - (y+b)|^2}{2x_3 y_3}\right) = d(x, y)$
- $$\begin{aligned} d(L_\lambda(x), L_\lambda(y)) &= \operatorname{arcosh}\left(1 + \frac{|\lambda x - \lambda y|^2}{2|\lambda| x_3 |\lambda| y_3}\right) \\ &= \operatorname{arcosh}\left(1 + \frac{|\lambda|^2 |x - y|^2}{|\lambda|^2 2 x_3 y_3}\right) \\ &= d(x, y) \end{aligned}$$

- $d(S(x), S(y)) = \operatorname{arcosh}\left(1 + |\frac{x}{|x|^2} - \frac{y}{|y|^2}|^2 \frac{|x|^2|y|^2}{2x_3y_3}\right)$
$= \operatorname{arcosh}\left(1 + |\frac{x|y|^2 - y|x|^2}{|x|^2|y|^2}|^2 \frac{|x|^2|y|^2}{2x_3y_3}\right)$
$= \operatorname{arcosh}\left(1 + \frac{|x|^2|y|^4 - 2|xy||x|^2|y|^2 + |x|^4|y|^2}{|x|^2|y|^2 2x_3y_3}\right)$
$= \operatorname{arcosh}\left(1 + \frac{|y|^2 - 2|xy| + |x|^2}{2x_3y_3}\right)$
$= d(x, y)$

- $d(U_\theta(x), U(y)) = \operatorname{arcosh}\left(1 + \frac{|\bar{x} - \bar{y}|^2}{2x_3y_3}\right) = d(x, y).$

Koska kuvaukset ovat isometrioita, selkeästi myös niiden yhdistetyt kuvaukset ovat isometrioita. □

Yhdistämällä yllä määriteltyjä isometrioita voidaan muodostaa uusia isometrioita. Määritellään täten hyödyllinen Möbiuskuvauksen kaltainen neljän muuttujan määrittämä hyperbolisen avaruuden kuvaus.

Määritelmä 4.8. Olkoon $P = z + jr \in \mathbb{H}$ ja $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{PSL}_2(\mathbb{C})$. Määritellään kuvaus

$$\gamma P = \frac{(az + b)(\bar{c}\bar{z} + \bar{d}) + a\bar{c}r^2}{|cz + d|^2 + |c|^2r^2} + j\frac{r}{|cz + d|^2 + |c|^2r^2}.$$

Kuvausta γ kutsutaan *Möbiuskuvauksen Poincarén laajennukseksi.* ([4], kappaleet 4.1 ja 4.2.)

Huomioidaan, että Määritelmän 4.8 kuvaus voidaan laajentaa jatkuvasti kompleksitason pisteelle, jolloin, kun r lähestyy nollaa, kuvaus lähestyy muotoa $\gamma z = \frac{az+b}{cz+d}$. On kuitenkin huomioitava, ettei hyperbolinen metriikka ole määritelty hyperbolisen avaruuden reunalla ja täten Määritelmän 4.8 kuvausta käsitellään laajentamatta kompleksitasoon. Tarkempi yhteys yllä määriteltyjen kuvausten ja kompleksitason Möbius-kuvausten välillä on myös esitelty Beardonin kirjan The Geometry of Discrete Groups [4] luvussa 4. Vastaavasti, jos pistettä tulkitaan projektiivisen avaruuden pisteenä, saadaan Möbius-kuvaus $\gamma[z_1, z_2] = [az_1 + bz_2, cz_1 + dz_2]$. Huomioidaan, että $\gamma[\lambda z_1, \lambda z_2] = [\lambda(az_1 + bz_2), \lambda(cz_1 + dz_2)] = \gamma[z_1, z_2]$, joten kuvaus on hyvin määritelty. Seuraavaksi todistetaan, että määritelty kuvaus on isometria hyperbolisessa puoliavaruudessa.

Lemma 4.9. *Olkoon* $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{PSL}_2(\mathbb{C})$ *on isometria joukossa* $\mathbb{H}$

Todistus. Osoitetaan, että kuvaus muodostuu lemman 4.7 kuvausten yhdistettynä kuvauksena. Huomioidaan aluksi, että joukon $\mathbf{PSL}_2(\mathbb{C})$ matriiseille $ad - bc = 1$. Nyt yhdistetty kuvaus

$$T_{ac^{-1}}(L_{-c^{-1}}(U(L_{\frac{c}{|c^2|}}(S(U(T_{dc^{-1}}(z + jr))))))))$$

on hyperbolisen avaruuden isometria. Avataan kuvausta

$$\begin{aligned}
&T_{ac^{-1}}(L_{-c^{-1}}(U(L_{\frac{c}{|c^2|}}(S(U(T_{dc^{-1}}(z + jr))))))))\\
&= T_{ac^{-1}}(L_{-c^{-1}}(U(L_{\frac{c}{|c^2|}}(\frac{z + d/c + jr}{|z + d/c + jr|^2}))))\\
&= T_{ac^{-1}}(L_{-c^{-1}}(U(|c^{-2}|\frac{cz + d + |c|jr}{|z + d/c + jr|^2})))\\
&= T_{ac^{-1}}(L_{-c^{-1}}(\frac{\overline{cz + d} + |c|jr}{|cz + d + j|c|r|^2}))\\
&= -\frac{c^{-1}\overline{(cz + d)} + jr}{|cz + d + j|c|r|^2} + \frac{a}{c},
\end{aligned}$$

mistä, koska $ad - bc = 1$ ja täten $adc^{-1} = b$, saadaan yhtälö

$$\begin{aligned}
&= -\frac{c^{-1}\overline{(cz + d)} + jr}{|cz + d + j|c|r|^2} + \frac{a}{c}\\
&= -\frac{c^{-1}\overline{(cz + d)} + jr - a\bar{c}|z + d/c + jr|^2}{|cz + d|^2 + |c|^2r^2}\\
&= \frac{-c^{-1}\overline{(cz + d)} + jr + a\bar{c}|c|^{-2}(cz + d)(\overline{cz + d}) - a\bar{c}r^2}{|cz + d|^2 + |c|^2r^2}\\
&= \frac{c^{-1}\overline{(cz + d)}(a(cz + d)) + jr - a\bar{c}r^2}{|cz + d|^2 + |c|^2r^2}\\
&= \frac{\overline{(cz + d)}(az + adc^{-1})) + jr - a\bar{c}r^2}{|cz + d|^2 + |c|^2r^2}\\
&= \frac{\overline{(cz + d)}(az + b) + jr - a\bar{c}r^2}{|cz + d|^2 + |c|^2r^2}
\end{aligned}$$

todistaen lemman. ([4], kappale 4.1) □

5 Geometrian ja luokkaluvun yhteys

Tässä kappaleessa määritellään bijektio kunnan projektiivisen avaruuden pisteiden ja ideaaliluokkien välillä. Täten kunnan luokkaluvulle saadaan geometrinen esitys Riemannin pallolla.

5.1 Ideaaliluokkien ja kunnan alkion yhdistävä bijektio

Tässä kappaleessa esitetään bijektio joukolta $\mathbf{PSL}_2(\mathcal{O}_K)\backslash\mathbb{P}^1K$ ideaaliluokkien joukkoon. Merkinnällä $\mathbf{PSL}_2(\mathcal{O}_K)\backslash\mathbb{P}^1K$ tarkoitetaan projektiivisen avaruuden pisteitä $\mathbb{P}^1K$ varustettuna ekvivalenssireaktiolla $[z_1, z_2] = \sigma[z_1, z_2]$ kaikilla $[z_1, z_2] \in \mathbb{P}^1K$ ja $\sigma \in \mathbf{PSL}_2(\mathcal{O}_K)$. Merkitään pisteen $[z_1, z_2]$ ekvivalenssiluokkaa $[z_1, z_2]^{\#}$. Tässä kappaleessa esiteltävän kuvauksen tavoitteena on muodostaa linkki luokkaluvun ja hyperbolisen geometrian välillä. Ennen määritelmää on kuitenkin vielä todistettava seuraava hyödyllinen lemma. Seuraavassa lemmassa tulkitaan ryhmän $\mathbf{SL}_2(\mathcal{O}_K)$ toimintaa lineaarisena toimintana avaruudessa $K \times K$ eli matriisitulona. Käytännössä tämä tarkoittaa, että matriiille

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{SL}_2(\mathcal{O}_K)$$

ja alkiolle $(x, y) \in K \times K$) määritellään

$$\gamma(x, y) = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}.$$

Lemma 5.1. *Olkoon pisteet $(x_1, x_2), (y_1, y_2) \in K \times K$. Tällöin seuraavat väittämät ovat ekvivalentteja:*
1) $\langle x_1, x_2\rangle = \langle y_1, y_2\rangle$
2) On olemassa $\sigma \in \mathbf{SL}_2(\mathcal{O}_K)$ siten, että $\sigma(x_1, x_2) = (y_1, y_2)$.

Todistus. Jos kohta (2) pätee, on olemassa $a, b, c, d \in \mathcal{O}_K$, jolle

$$(ax_1 + bx_2, cx_1 + dx_2) = \sigma(x_1, x_2) = (y_1, y_2),$$

joten $\langle y_1, y_2\rangle \subset \langle x_1, x_2\rangle$. Vastaavasti

$$(x_1, x_2) = \sigma^{-1}(y_1, y_2).$$

Jos kohta (1) pätee, olkoon $I = \langle x_1, x_2\rangle = \langle y_1, y_2\rangle$. Jos $I = \langle 0\rangle$, saadaan $(x_1, x_2) = (y_1, y_2) = (0, 0)$ ja jokainen matriisi kiinnittää pisteen $(0, 0)$. Jos $I \neq \langle 0\rangle$, lemmojen 3.8 ja 3.9 mukaan, koska $I \in \mathcal{M}_K$ ja $\mathcal{J}_K$ on äärellinen ryhmä, on olemassa äärellinen luonnollinen luku n siten, että $I^n \in (\mathcal{O}_K)^{\#}$.

Nyt lemman 3.10 mukaan on olemassa $\theta \in K - \{0\}$, jolle $I^n = \langle\theta\rangle$. Täten alkioille (x_1, x_2) ja (y_1, y_2) on olemassa alkiot $\alpha_1, \alpha_2, \beta_1, \beta_2 \in I^{n-1}$ siten, että $x_1\alpha_1 + x_2\alpha_2 = \theta = y_1\beta_1 + y_2\beta_2$. Määrittelemällä matriisi

$$\sigma = \begin{pmatrix} \frac{y_1\alpha_1 + x_2\beta_2}{\theta} & \frac{y_1\alpha_2 - x_1\beta_2}{\theta} \\ \frac{y_2\alpha_1 - x_2\beta_1}{\theta} & \frac{y_2\alpha_2 + x_1\beta_1}{\theta} \end{pmatrix},$$

jolle pätee

$$\begin{aligned} \det(\sigma) &= \frac{(y_1\alpha_1 + x_2\beta_2)(y_2\alpha_2 + x_1\beta_1)}{\theta^2} - \frac{(y_2\alpha_1 - x_2\beta_1)(y_1\alpha_2 - x_1\beta_2)}{\theta^2} \\ &= \frac{y_1\alpha_1 y_2\alpha_2 + x_2\beta_2 y_2\alpha_2 + y_1\alpha_1 x_1\beta_1 + x_1\beta_1 x_2\beta_2}{\theta^2} \\ &- \frac{y_2\alpha_1 y_1\alpha_2 - x_2\beta_1 y_1\alpha_2 - y_2\alpha_1 x_1\beta_2 + x_2\beta_1 x_1\beta_2}{\theta^2} \\ &= \frac{y_2\beta_2 x_2\alpha_2 + x_1\alpha_1 y_1\beta_1 + y_1\beta_1 x_2\alpha_2 + x_1\alpha_1 y_2\beta_2}{\theta^2} \\ &= \frac{(x_1\alpha_1 + x_2\alpha_2)(y_1\beta_1 + y_2\beta_2)}{\theta^2} \\ &= 1. \end{aligned}$$

Koska matriisin σ alkioiden osoittajille pätee $x_i\alpha_i, x_i\beta_i, y_i\alpha_i, y_i\beta_i \in I^n = \langle\theta\rangle$, luku θ jakaa osoittajat ja täten matriisi on kokonaislukukertoiminen. Lopulta yhtälö

$$\begin{aligned} \sigma(x_1, x_2) &= \begin{pmatrix} \frac{x_1(y_1\alpha_1 + x_2\beta_2) + x_2(y_1\alpha_2 - x_1\beta_2)}{\theta} \\ \frac{x_1(y_2\alpha_1 - x_2\beta_1) + x_2(y_2\alpha_2 + x_1\beta_1)}{\theta} \end{pmatrix} \\ &= \begin{pmatrix} \frac{y_1(x_1\alpha_1 + x_2\alpha_2)}{\theta} \\ \frac{y_2(x_1\alpha_1 + x_2\alpha_2)}{\theta} \end{pmatrix} \\ &= (y_1, y_2) \end{aligned}$$

todistaa lemman. ([9], s.314) □

Lemma 5.1 yhdistää kunnan tuloavaruuden $K \times K$ pisteet, alkioiden virittämiin ideaaleihin. Nyt, jotta voidaan muodostaa geometrinen yhteys luokkalukuun on määriteltävä kuvaus kunnan pisteiltä ideaaliluokkaan.

Määritelmä 5.2. Määritellään kuvaus $\tilde{j} : \mathbb{P}^1 K \to \mathcal{J}_K$

$$\tilde{j}([x_1, x_2]) = \langle x_1, x_2\rangle^{\#}$$

([9], s.315)

Koska $\langle x_1, x_2\rangle^\# = \langle \lambda x_1, \lambda x_2\rangle^\#$ kaikilla $\lambda \in K$, kuvaus $\tilde{j}$ on hyvin määritelty. Se yhdistää Riemannin pallon pisteen ideaaliluokkaan. Kuvauksen avulla saadaan muodostettua linkki kuntalaajennoksen geometrian ja luokkaluvun välillä.

Lause 5.3. *$j : \mathbf{PSL}_2(\mathcal{O}_K)\backslash\mathbb{P}^1K = \mathcal{J}_K$ määriteltynä*

$$j([x_1, x_2]^\#) = \langle x_1, x_2\rangle^\#$$

on bijektio. ([9], s.315)

Todistus. Aloitetaan toteamalla, että kuvaus j on hyvin määritelty. Koska kuvaus $\tilde{j}$ on hyvin määritelty, riittää osoittaa, että $j([x_1, x_2]) = j(\sigma[y_1, y_2])$ kaikilla $\sigma \in \mathbf{PSL}_2(\mathcal{O}_K)$. Lemma 5.1 osoittaa, että $\langle x_1, x_2\rangle = \langle y_1, y_2\rangle$ kaikille $\sigma[x_1, x_2] = [y_1, y_2]$.

Todistetaan seuraavaksi kuvauksen j surjektiivisuus. Seurauksen 2.7 mukaan mille tahansa ideaalille I on olemassa alkiot $x_1, x_2 \in \mathcal{O}_K$ siten, että $\langle x_1, x_2\rangle = I$. Nyt

$$j([x_1, x_2]) = I^\#$$

todistaen surjektiivisuudeen.

Todistetaan seuraavaksi kuvauksen injektiivisyys. Olkoon pisteet

$$[x_1, x_2], [y_1, y_2] \in \mathbb{P}^1K$$

siten, että $\sigma_1[x_1, x_2] \neq \sigma_2[y_1, y_2]$ kaikilla $\sigma_1, \sigma_2 \in \mathbf{PSL}_2(\mathcal{O}_K)$. Nyt Lemman 5.1 mukaan $\lambda_1\langle x_1, x_2\rangle \neq \lambda_2\langle y_1, y_2\rangle$ millään $\lambda_1, \lambda_2 \in \mathcal{C}$ eli

$$\langle x_1, x_2\rangle^\# \neq \langle y_1, y_2\rangle^\#.$$

□

Täten on todistettu konkreettinen yhdistävä tekijä kunnan K antamien Riemann-pallon pisteiden ja idealiluokkien välillä.

6 Algebrallinen kärki

6.1 Algebrallisen kärjen määritelmä

Edellisessä kappaleessa on tuotettu lause, joka yhdistää ideaaliluokat ja ryhmän $\mathbf{PSL}_2(\mathcal{O}_K)$ määrittämien kunnan K antamien Riemannin pallon pisteiden ekvivalenssiryhmät. Nyt, jotta Riemanin pallon pisteiden yhteyttä hyperboliseen geometriaan voidaan tutkia tarkemmin, on määriteltävä algebralllinen kärki. Määritelmä muodostuu diskreettien ryhmien kautta.

Määritelmä 6.1. Aliryhmä $\Gamma \subset \mathbf{PSL}_2(\mathbb{C})$ on *diskreetti*, jos kaikille jonoille uniikkeja kuvauksia $(T_n)_{n\geq 1} \subset \Gamma$ eli $T_n = T_m$, jos ja vain jos $n = m$ ja kaikille pisteille $P \in \mathbb{H}$ pätee, että jono $(T_n P)_{n\geq 1}$ ei suppene.

On tärkeää huomioida, että $\mathbf{PSL}_2(\mathcal{O}_K)$ on diskreetti aliryhmä. ([4], s.95) Määritellään ryhmille seuraava merkittävä ominaisuus.

Määritelmä 6.2. Olkoon G ryhmä. Aliryhmät $\Gamma_1, \Gamma_2 \subset G$ ovat *yhteismitalliset*, jos

$$[\Gamma_1 : \Gamma_1 \cap \Gamma_2] \text{ ja } [\Gamma_2 : \Gamma_1 \cap \Gamma_2]$$

ovat äärellisiä.

Yhteismitalllisuus on hyödyllinen tapa varmistaa, että kaksi ryhmää käyttäytyy vastaavalla tavalla.

Lemma 6.3. *Olkoon G ryhmä ja $\Gamma_1, \Gamma_2, \Gamma_3 \subset G$ sen aliryhmiä. Jos ryhmät Γ_1 ja Γ_2 ovat yhteismitalliset ja ryhmät Γ_2 ja Γ_3 ovat yhteismitalliset, niin ryhmät Γ_1 ja Γ_3 ovat yhteismitaliset.*

Todistus. Määritellään kuvaus

$$\Phi : \Gamma_1 \cap \Gamma_2 / \Gamma_1 \cap \Gamma_2 \cap \Gamma_3 \to \Gamma_2 / \Gamma_2 \cap \Gamma_3$$

määrittelemällä

$$\Phi(a(\Gamma_1 \cap \Gamma_2 \cap \Gamma_3)) = a(\Gamma_2 \cap \Gamma_3).$$

Jos $a(\Gamma_1 \cap \Gamma_2 \cap \Gamma_3) = b(\Gamma_1 \cap \Gamma_2 \cap \Gamma_3)$, saadaan $b^{-1}a \in \Gamma_1 \cap \Gamma_2 \cap \Gamma_3$ eli erityisesti $b^{-1}a \in \Gamma_2 \cap \Gamma_3$, joten $a(\Gamma_2 \cap \Gamma_3) = b(\Gamma_2 \cap \Gamma_3)$. Täten funktio on hyvin määritelty. Määritellään alkiot $a, b \in \Gamma_1 \cap \Gamma_2$ siten, että yhtälö $\Phi(a(\Gamma_1 \cap \Gamma_2 \cap \Gamma_3)) = \Phi(b(\Gamma_1 \cap \Gamma_2 \cap \Gamma_3))$ pätee. Koska $a, b \in \Gamma_1$ ja Γ_1 on ryhmä, saadaan $b^{-1}a \in \Gamma_1$. Lisäksi määritelmän mukaan $b^{-1}a \in \Gamma_2 \cap \Gamma_3$, joten $b^{-1}a \in \Gamma_1 \cap \Gamma_2 \cap \Gamma_3$. Nyt $a(\Gamma_1 \cap \Gamma_2 \cap \Gamma_3) = b(\Gamma_1 \cap \Gamma_2 \cap \Gamma_3)$ eli kuvaus Φ on injektiivinen ja $\#(\Gamma_1 \cap \Gamma_2 / \Gamma_1 \cap \Gamma_2 \cap \Gamma_3) \leq \#(\Gamma_2 / \Gamma_2 \cap \Gamma_3)$.

Olkoon nyt ryhmät Γ_1 ja Γ_2 ovat yhteismitalliset ja ryhmät Γ_2 ja Γ_3 ovat yhteismitalliset. Täten saadaan epäyhtälö

$$\begin{aligned}
\#(\Gamma_1 / \Gamma_1 \cap \Gamma_3) &\leq \#(\Gamma_1 / \Gamma_1 \cap \Gamma_2 \cap \Gamma_3) \\
&= \#(\Gamma_1 / \Gamma_1 \cap \Gamma_2) \#(\Gamma_1 \cap \Gamma_2 / \Gamma_1 \cap \Gamma_2 \cap \Gamma_3) \\
&\leq \#(\Gamma_1 / \Gamma_1 \cap \Gamma_2) \#(\Gamma_2 / \Gamma_2 \cap \Gamma_3).
\end{aligned}$$

Huomioidaan myös, että yhteismitallisuuden määritelmän perusteella luvut $\#(\Gamma_1 / \Gamma_1 \cap \Gamma_2)$ ja $\#(\Gamma_2 / \Gamma_2 \cap \Gamma_3)$ ovat äärelliset eli $\#(\Gamma_1 / \Gamma_1 \cap \Gamma_3)$ on äärellinen. Vastaavalla päättelyllä $\#(\Gamma_3 / \Gamma_1 \cap \Gamma_3)$ on äärellinen.

Täten yhteismitallisuus on transitiivinen ominaisuus. □

Todistetaan seuraavaksi hyödyllinen lemma ryhmälle $\mathbf{PSL}_2(\mathcal{O}_K)$ käyttäen yhteismitallisuutta.

Lemma 6.4. *Olkoon K toisen asteen imaginäärinen lukukunta ja $\gamma \in \mathbf{PSL}_2(K)$. Ryhmät $\mathbf{PSL}_2(\mathcal{O}_K)$ ja $\gamma^{-1}\mathbf{PSL}_2(\mathcal{O}_K)\gamma$ ovat yhteismitalliset.*

Todistus. Osoitetaan ensin, että ryhmät $\mathbf{GL}_2(\mathcal{O}_K)$ ja $\gamma^{-1}\mathbf{GL}_2(\mathcal{O}_K)\gamma$ ovat yhteismitalliset kaikilla $\gamma \in \mathbf{GL}_2(K)$. Todistus seuraa lähteen [9] sivun 76 todistusta.
Valitaan $\lambda \in \mathcal{O}_K$ siten, että $\lambda ab \in \mathcal{O}_K$ kaikilla matriisin γ alkioilla a ja matriisin γ^{-1} alkioilla b. Lisäksi määritellään

$$\Gamma = \{\omega \in \mathbf{GL}_2(\mathcal{O}_K) : \omega = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod \lambda\mathcal{O}_K\},$$

missä $\omega = \omega' \bmod \lambda\mathcal{O}_K$, jos ja vain jos matriisin $\omega - \omega'$ kertoimet ovat ideaalissa $\lambda\mathcal{O}_K$. Määritellään kuvaus

$$\Phi : \mathbf{GL}_2(\mathcal{O}_K) \to \mathbf{GL}_2(\mathcal{O}_K/\lambda\mathcal{O}_K)$$

$$\Phi \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a + \lambda\mathcal{O}_K & b + \lambda\mathcal{O}_K \\ c + \lambda\mathcal{O}_K & d + \lambda\mathcal{O}_K \end{pmatrix}.$$

Huomataan, että Φ on homomorfismi, jonka ydin on selkeästi Γ. Ryhmän $\mathbf{GL}_2(\mathcal{O}_K/\lambda\mathcal{O}_K)$ alkiot ovat 2×2-matriiseja joiden kertoimet ovat renkaassa $\mathcal{O}_K/\lambda\mathcal{O}_K$. Täten osoittamalla, että $\mathcal{O}_K/\lambda\mathcal{O}_K$ on äärellinen, saadaan todistettua, että $\#(\mathbf{GL}_2(\mathcal{O}_K)/\Gamma)$ on äärellinen. Huomioidaan, että $(\bar{\lambda}\lambda)\mathcal{O}_K \subset \lambda\mathcal{O}_K$ ja täten

$$\#(\mathcal{O}_K/(\bar{\lambda}\lambda)\mathcal{O}_K) \geq \#(\mathcal{O}_K/\lambda\mathcal{O}_K).$$

Koska $\bar{\lambda}\lambda \in \mathbb{Z}$, ideaalin $(\bar{\lambda}\lambda)\mathcal{O}_K$ primäärisessä perussuunnikkaassa on korkeintaan $(\bar{\lambda}\lambda + 1)^2$ kokonaislukurenkaan $\mathcal{O}_K$ hilapistettä eli

$$\#(\mathcal{O}_K/(\bar{\lambda}\lambda)\mathcal{O}_K) \leq (\bar{\lambda}\lambda + 1)^2.$$

Nyt $\#(\mathbf{GL}_2(\mathcal{O}_K)/\Gamma)$ on äärellinen. Lisäksi, jos

$$\lambda A \in \Gamma,$$

niin matriisin A kertoimet ovat ideaalissa $\lambda\mathcal{O}_K$ ja yhtälö

$$\gamma(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + A)\gamma^{-1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \gamma A\gamma^{-1} \in \mathbf{GL}_2(\mathcal{O}_K)$$

osoittaa, että, koska matriisin $\gamma A\gamma^{-1}$ alkiot ovat kokonaislukurenkaassa luvun λ valinnan mukaan, Γ on ryhmän $\gamma^{-1}\mathbf{GL}_2(\mathcal{O}_K)\gamma$ aliryhmä. Täten

$$\#\Big(\mathbf{GL}_2(\mathcal{O}_K)/(\gamma^{-1}\mathbf{GL}_2(\mathcal{O}_K)\gamma)\cap\mathbf{GL}_2(\mathcal{O}_K)\Big)\leq\#(\mathbf{GL}_2(\mathcal{O}_K)/\Gamma)$$

on äärellinen. Vastaavalla päättelyllä myös

$$\#\Big(\gamma^{-1}\mathbf{GL}_2(\mathcal{O}_K)\gamma/(\gamma^{-1}\mathbf{GL}_2(\mathcal{O}_K)\gamma)\cap\mathbf{GL}_2(\mathcal{O}_K)\Big)$$

on äärellinen.

Nyt determinantti on homomorfismi ryhmältä $\mathbf{GL}_2(\mathcal{O}_K)$ kokonaislukujen renkaaseen. Se on surjektiivinen luvun 1 juurille, joita on Lemmasta 1.4 päättelemällä korkeintaan 6. Determinanttikuvauksen ydin muodostuu matriiseista, joiden determinantti on 1 eli $\mathbf{SL}_2(\mathcal{O}_K)$. Täten

$$\#\Big(\mathbf{GL}_2(\mathcal{O}_K)/(\mathbf{GL}_2(\mathcal{O}_K)\cap\mathbf{SL}_2(\mathcal{O}_K))\Big)<\infty$$

eli $\mathbf{GL}_2(\mathcal{O}_K)$ ja $\mathbf{SL}_2(\mathcal{O}_K)$ ovat yhteismitallisen. Koska matriisin $\gamma\in\mathbf{SL}_2(K)$ determinantti on 1, vastaavalla päättelyllä

$$\gamma^{-1}\mathbf{GL}_2(\mathcal{O}_K)\gamma$$

ja

$$\gamma^{-1}\mathbf{SL}_2(\mathcal{O}_K)\gamma$$

ovat yhteismitalliset. Vastaavasti, koska $\mathbf{SZ}_2(\mathcal{O}_K)=\left\{\pm\begin{pmatrix}1&0\\0&1\end{pmatrix}\right\}$ on äärellinen, ryhmän $\mathbf{PSL}_2(\mathcal{O}_K)$ määritelmän mukaan se on yhteismitallinen ryhmän $\mathbf{SL}_2(\mathcal{O}_K)$ kanssa. Täten Lemman 6.3 perusteella $\mathbf{PSL}_2(\mathcal{O}_K)$ ja $\gamma^{-1}\mathbf{PSL}_2(\mathcal{O}_K)\gamma$ ovat yhteismitalliset. ([9], s.76) □

Määritellään seuraavaksi kuvauksien aliryhmän osajoukko, joka ei siirrä jotain avaruuden pistettä.

Määritelmä 6.5. Olkoon $\Gamma\subset\mathbf{PSL}_2(\mathbb{C})$ aliryhmä. Pisteen $P\in\mathbb{H}\cup\mathbb{P}^1\mathbb{C}$ *stabilisoija* on aliryhmä

$$\Gamma_P=\{\gamma\in\Gamma:\gamma P=P\}.$$

Jokaisella hyperbolisen aruuden pisteellä on epätyhjä stabilisoija, koska neutraalialkio sisältyy aina stabilisoijaan. Eri pisteiden stabilisoijissa on kuitenkin eroa ja täten määritellään pisteiden stabilisoijien avulla algebrallinen kärki (englanniksi cusp). Algebralliset kärjet ovat hyödyllinen joukko pisteitä ryhmän operaatioiden tutkimiseen geometrisesti.

Määritelmä 6.6. Olkoon joukolla $\Gamma \subset \mathbf{PSL}_2(\mathbb{C})$ diskreetti aliryhmä. Jos Riemannin pallon pisteen $P \in \mathbb{P}^1\mathbb{C}$ stabilisoijalla Γ_P on aliryhmä, joka on isomorfinen additiivisen ryhmän $(\mathbb{Z}^2, +)$ kanssa, kutsutaan pistettä P *algebralliseksi kärjeksi*. Aliryhmän Γ algebrallisten kärkien joukkoa merkitään C_Γ.

Äärettömyyspisteen stabilisoija Γ_∞ muodostuu matriiseista γ, joille pätee yhtälö $\gamma[1,0] = [\lambda, 0]$, jollain $\lambda \in \mathbb{C} - \{0\}$. Täten nähdään, että $\gamma = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$, missä $ad = 1$ eli $\Gamma_\infty = \Gamma \cap (\mathbf{PSL}_2(\mathbb{C}))_\infty$. Joukon esittämiseksi on hyödyllistä määritellä seuraava ryhmä.

Määritelmä 6.7. Määritellään matriisitulon suhteen ryhmä

$$\mathbf{N}(\mathcal{O}_K) = \Big\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : b \in \mathcal{O}_K \Big\}.$$

Ryhmän $\mathbf{N}(\mathcal{O}_K)$ alkioille $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \in \mathbf{N}(\mathcal{O}_K)$ pätee $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+b \\ 0 & 1 \end{pmatrix}$. Nyt matriisitulo joukossa $\mathbf{N}(\mathcal{O}_K)$ on suljettu ja liitännäinen. Lisäksi neutraalialkio $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ ja alkion $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \in \mathbf{N}(\mathcal{O}_K)$ käänteisalkio $\begin{pmatrix} 1 & -b \\ 0 & 1 \end{pmatrix}$ sisältyvät joukkoon $\mathbf{N}(\mathcal{O}_K)$. Täten joukko $\mathbf{N}(\mathcal{O}_K)$ on ryhmä.

Nyt, jos diskreetti aliryhmä Γ sisältää esimerkiksi ryhmän matriiseja muotoa $\begin{pmatrix} 1 & z \\ 0 & 1 \end{pmatrix}$, missä kompleksilukujen z arvot muodostavat kompleksitason hilan, niin $\infty \in C_\Gamma$. Esimerkiksi ryhmässä $\mathbf{SL}_2(\mathcal{O}_K)$ piste ∞ on algebrallinen kärki, koska $\Big\{ \begin{pmatrix} 1 & z \\ 0 & 1 \end{pmatrix} : z \in \mathcal{O}_K \Big\} \subset \mathbf{SL}_2(\mathcal{O}_K)$.

6.2 Algebralliset kärjet kompleksitasossa

Tässä kappaleessa todistetaan, että algebralliset kärjet voidaan suoraan yhdistää toisen asteen lukukunnan pisteiksi Riemannin pallossa. Tämä mahdollistaa lukukunnan käsittelyn geometrisesti ryhmässä $\mathbf{PSL}_2(K)$. Tätä varten todistetaan ensin seuraava lyhyt lemma.

Lemma 6.8. *Olkoon G ryhmä ja H ja K sen aliryhmiä. Tällöin pätee*

$$[H : H \cap K] \leq [G : K].$$

Todistus. Määritellään kuvaus

$$\Phi : H/(H \cap K) \to G/K$$

määrittelemällä

$$\Phi(x(H \cap K)) = xK.$$

Jos $x(H \cap K) \neq y(H \cap K)$, niin $y^{-1}x \notin H \cap K$. Koska H on ryhmä, saadaan $y^{-1}x \in H$ ja täten $y^{-1}x \notin K$ eli $xK \neq yK$. Täten kuvaus Φ on injektio eli

$$\#(H/H \cap K) \leq \#(G/K).$$

□

Nyt voidaan todistaa haluttu lause.

Lause 6.9. *Olkoon K toisen asteen imaginäärinen lukukunta. Tällöin, jos $\Gamma \subseteq \mathbf{PSL}_2(K)$ on ryhmän $\mathbf{PSL}_2(\mathcal{O}_K)$ kanssa yhteismitallinen aliryhmä, niin $C_\Gamma = \mathbb{P}^1 K$.*

Todistus. Todistetaan ensin, että $\mathbb{P}^1 K \subseteq C_\Gamma$.

Olkoon $\Gamma \subseteq \mathbf{PSL}_2(K)$ ryhmän $\mathbf{PSL}_2(\mathcal{O}_K)$ kanssa yhteismitallinen aliryhmä. Huomioidaan aluksi, että ryhmän Γ_∞ alkiot ovat muotoa $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ alkioilla $a, d \in K$, joille $ad = 1$, ja mielivaltaisella $b \in K$. Koska oletuksen mukaan

$$\#\Big(\mathbf{PSL}_2(\mathcal{O}_K)/\Gamma \cap \mathbf{PSL}_2(\mathcal{O}_K)\Big)$$

on äärellinen, Lemman 6.8 mukaan

$$\#\Big(\mathbf{N}(\mathcal{O}_K)/\mathbf{N}(\mathcal{O}_K) \cap \Gamma \cap \mathbf{PSL}_2(\mathcal{O}_K)\Big)$$

on äärellinen ja täten joukossa $\Gamma \cap \mathbf{PSL}_2(\mathcal{O}_K)$ on äärettömästi alkioita muotoa

$$\begin{pmatrix} 1 & t_1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & t_2 \\ 0 & 1 \end{pmatrix} \in \Gamma$$

jollain $t_1, t_2 \in \mathcal{O}_K$, missä pisteet t_1 ja t_2 määrittävät kompleksitason hilan. Täten pisteen ∞ stabilisoija ryhmässä Γ sisältää ryhmän, joka on isomorfinen additiivisen ryhmän $(\mathbb{Z}^2, +)$ kanssa. Vastaavasti, koska Lemman 6.4 perusteella ryhmä $\gamma\Gamma\gamma^{-1}$ on yhteismitallinen ryhmän $\mathbf{PSL}_2(\mathcal{O}_K)$ kanssa kaikilla $\gamma \in \mathbf{PSL}_2(K)$,

$$\#\Big(\mathbf{N}(\mathcal{O}_K)/\mathbf{N}(\mathcal{O}_K) \cap \gamma\Gamma\gamma^{-1} \cap \mathbf{PSL}_2(\mathcal{O}_K)\Big)$$

on äärellinen. Täten $\infty \in C_{\gamma\Gamma\gamma^{-1}}$ kaikilla $\gamma \in \mathbf{PSL}_2(K)$.

Pisteelle $P = [z_1, z_2] \in \mathbb{P}^1K - \{\infty\}$, jolle pätee $z_1 \neq 0$, määritellään kuvaus $\gamma = \begin{pmatrix} 0 & -z_2^{-1} \\ z_2 & -z_1 \end{pmatrix}$. Huomioidaan, että, koska $z_1, z_2 \in K$, niin saadaan $z_1^{-1}, -z_2^{-1} \in K$ ja $\det(\gamma) = 1$. Täten $\gamma P = \infty$ ja $\gamma \in \mathbf{PSL}_2(K)$. Nyt kaikille $\sigma \in (\gamma\Gamma\gamma^{-1})_\infty$ pätee

$$\gamma^{-1}\sigma\gamma P = \gamma^{-1}\sigma\infty = \gamma^{-1}\infty = P$$

eli

$$\gamma^{-1}(\gamma\Gamma\gamma^{-1})_\infty\gamma = \Gamma_P.$$

Koska piste ∞ sisältyy joukkoon $C_{\gamma\Gamma\gamma^{-1}}$, joukko Γ_∞ on isomorfinen ryhmän $(\mathbb{Z}^2, +)$ kanssa. Huomioimalla, että γ on isomorfismi, joukko Γ_P on isomorfinen ryhmän $(\mathbb{Z}^2, +)$ kanssa. Täten piste $P \in C_\Gamma$ ja $\mathbb{P}^1K \subseteq C_\Gamma$.

Seuraavaksi todistetaan $C_\Gamma \subseteq \mathbb{P}^1K$. Olkoon Γ ryhmän $\mathbf{SL}_2(K)$ aliryhmä, joka on yhteismitallinen ryhmän $\mathbf{SL}_2(\mathcal{O}_K)$ kanssa. Olkoon piste $P = [z_1, z_2] \in C_\Gamma$. On olemassa $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{PSL}_2(\mathbb{C})$, jolle $\gamma P = \infty$. Lisäksi on olemassa aliryhmä $H \subset \Gamma_P$, joka on isomorfinen additiivisen ryhmän $(\mathbb{Z}^2, +)$ kanssa. Lemman 6.8 perusteella saadaan

$$\begin{aligned} \#(H/(H \cap \mathbf{PSL}_2(\mathcal{O}_K))) &= \#(H/(H \cap \mathbf{SL}_2(\mathcal{O}_K) \cap \Gamma)) \\ &\leq \#(\Gamma/(\Gamma \cap \mathbf{PSL}_2(\mathcal{O}_K))). \end{aligned}$$

Yhteismitallisuuden perusteella $\#(\Gamma/(\Gamma \cap \mathbf{SL}_2(\mathcal{O}_K)))$ on äärellinen ja täten, koska ryhmä H on ääretön, joukko $H \cap \mathbf{SL}_2(\mathcal{O}_K)$ on myös ääretön.

Osoitetaan, että joukossa $H \cap \mathbf{SL}_2(\mathcal{O}_K)$, on äärettömästi alkioita, joiden jälki on ± 2. Huomioimalla, että

$$(\gamma\Gamma\gamma^{-1})_\infty \subset \mathbf{N}(\mathbb{C})$$

ja

$$\gamma^{-1}(\gamma\Gamma\gamma^{-1})_\infty\gamma = \Gamma_P$$

huomataan, että

$$H \subset \Gamma_P \subset \gamma^{-1}\mathbf{N}(\mathbb{C})\gamma.$$

Nyt matriisille $A \in \mathbf{N}(\mathbb{C})$ pätee

$$\begin{aligned} \gamma^{-1}A\gamma &= \begin{pmatrix} -d & b \\ c & -a \end{pmatrix} \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \\ &= \begin{pmatrix} -d & -dx + b \\ cy & cx - a \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \\ &= \begin{pmatrix} bc - cdx - ad & bd - bd - d^2x \\ c^2x + ac - ac & bc + cdx - ad \end{pmatrix} \end{aligned}$$

saadaan laskettua

$$\begin{aligned}\operatorname{tr}(\gamma A\gamma^{-1}) &= bc - cdx - ad + bc + cdx - ad \\ &= 2(bc - ad) \\ &= \pm 2\end{aligned}$$

eli kaikille $\sigma \in H$ pätee $\operatorname{tr}(\sigma) = \pm 2$. Olkoon nyt $\sigma \in H - \left\{ \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}$ kuvaus, jonka jälki on ± 2. Täten matriisi σ määrittäää kuvauksen tekijäavaruudessa $\mathbf{PSL}_2(K)$, jolle saadaan esitys $\sigma = \begin{pmatrix} e & f \\ g & 2-e \end{pmatrix} \in \mathbf{PSL}_2(K)$ joillain alkioilla $e, f, g \in K$. Yhtälöstä

$$\sigma P = \frac{eP + f}{gP + 2 - e} = P$$

saadaan ratkaistua

$$gP^2 + 2(1-e)P - f = 0$$

eli

$$\begin{aligned}P &= \frac{2(1-e) \pm \sqrt{4(1-e)^2 + 4gf}}{2g} \\ &= \frac{(1-e) \pm \sqrt{(e^2 - 2e + 1) + (2e - e^2 - 1)}}{g} \\ &= \frac{1-e}{g}.\end{aligned}$$

Nyt huomataan, että σ stabilisoi pisteen $[\frac{1-e}{g}, 1]$. Jos σ stabilisoi pisteet P ja P', niin $\gamma\sigma\gamma^{-1}$ stabilisoi pisteet ∞ ja $\gamma P'$. Tällöin $\gamma P' = \gamma P' + z$ jollain $z \in \mathbb{C} - \{0\}$ eli $\gamma P' = \infty$ ja täten $P = P'$. Täten

$$P = [\frac{1-e}{g}, 1] = [1 - e, g]$$

jollain $e, g \in K$, mikä todistaa, että $P \in \mathbb{P}^1 K$ todistaen lemman. ([9], s.315) □

Täten algebralliset kärjet ovat toisen asteen imaginäärisen lukukunnan K pisteitä Riemann-pallossa. Onkin hyödyllistä määritellä hyperbolisen avaruuden joukko, joka toimii algebrallisen kärjen kanssa vastaavalla tavalla.

7 Perusalueen geometria

7.1 Perusalueen määritelmä ja konstruktio

Ryhmälle isometrioita voidaan määritellä geometrinen alue, joka peittää avaruuden ryhmän toiminnoilla ilman, että sen sisäpisteet leikkaavat toisiaan. Tätä geometristä aluetta kutsutaan perusalueeksi.

Määritelmä 7.1. Olkoon Γ ryhmä isometrioita metrisessä avaruudessa S. Suljettu joukko $F \subset S$ on ryhmän Γ *perusalue*, jos $\bigcup_{\gamma\in\Gamma} \gamma F = S$ ja joukolla $\gamma_1 F \cap \gamma_2 F$ ei ole sisäpisteitä millään $\gamma_1, \gamma_2 \in \Gamma$, $\gamma_1 \neq \gamma_2$.

Esimerkiksi nyt perussuunnikas on kokonaislukurenkaan summaoperaatioiden ryhmän perusalue. Toisen asteen imaginäärisen lukukunnan K ryhmässä $\mathbf{PSL}_2(\mathcal{O}_K)$ hyperbolinen perusalue konstruoidaan ensin ja todistetaan myöhemmin perusalueeksi. Määritelmä on esitetty lähteen [9] kappaleessa 7.

Määritelmä 7.2. Olkoon $K = \mathbb{Q}(\sqrt{d}), d < 0$, missä d on neliötön ja D_K on diskriminantti. Määritellään joukot

$$\mathcal{B}_K = \{z+rj \in \mathbb{H} : |cz+d|^2+|c|^2r^2 \geq 1, \text{kaikille } c,d \in \mathcal{O}_K \text{ joille } \langle c,d\rangle = \mathcal{O}_K\}$$

ja

$$\mathcal{P}_K = \{z : 0 \leq \mathrm{Re}(z) \leq 1,\ 0 \leq \mathrm{Im}(z) \leq \sqrt{|D_K|}/2\}.$$

Jos $d \neq -3$ ja $d \neq -1$, määritellään

$$\mathcal{F}_K = \mathcal{P}_K.$$

Lisäksi määritellään

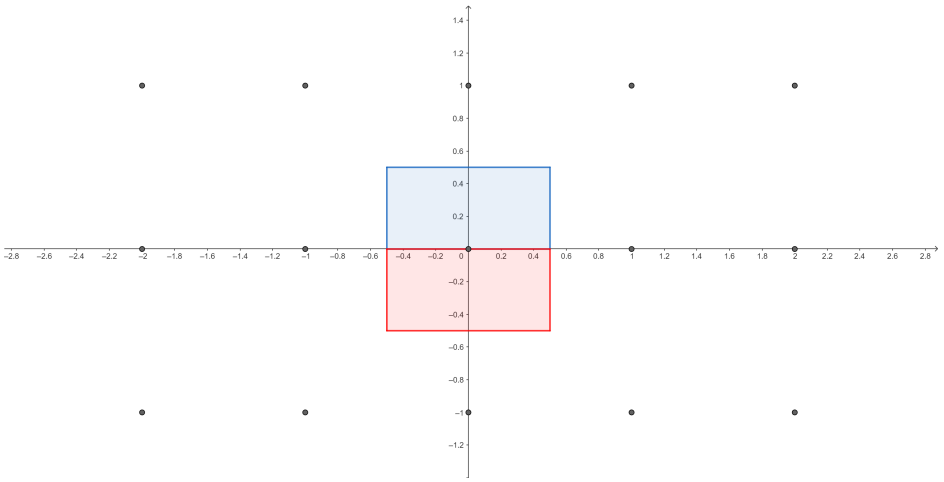
$$\mathcal{F}_{\mathbb{Q}(i)} = \Big\{z \in \mathbb{C} : 0 \leq |\mathrm{Re}(z)| \leq \frac{1}{2},\ 0 \leq \mathrm{Im}(z) \leq \frac{1}{2}\Big\}$$

ja

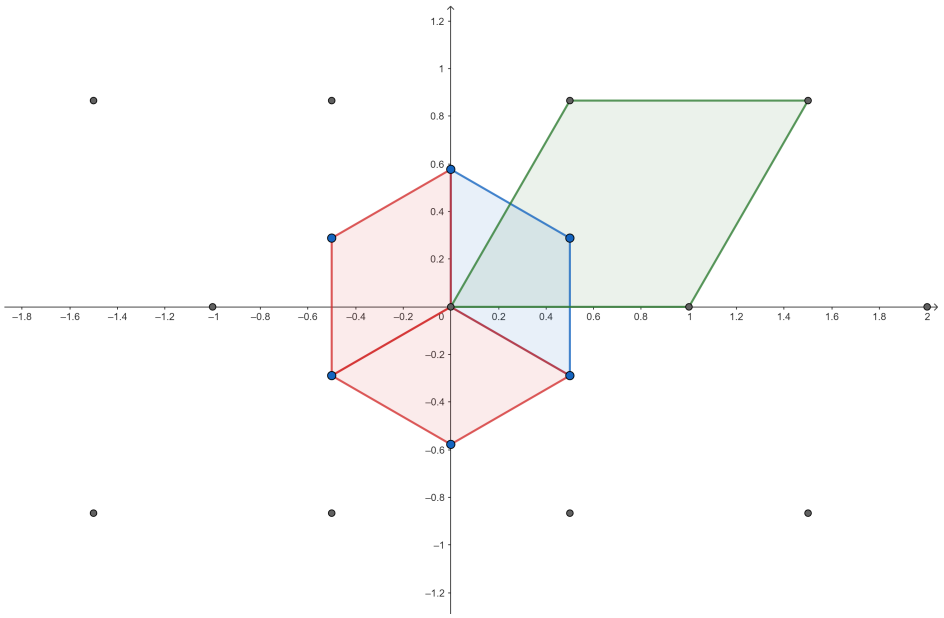
$$\begin{aligned}\mathcal{F}_{\mathbb{Q}(\sqrt{-3})} = &\Big\{z \in \mathbb{C} : 0 \leq \mathrm{Re}(z), \mathrm{Re}(z)\frac{\sqrt{3}}{3} \leq \mathrm{Im}(z) \leq (1-\mathrm{Re}(z))\frac{\sqrt{3}}{3}\Big\}\\ &\cup \Big\{z \in \mathbb{C} : 0 \leq \mathrm{Re}(z) \leq \frac{1}{2}, -\mathrm{Re}(z)\frac{\sqrt{3}}{3} \leq \mathrm{Im}(z) \leq \mathrm{Re}(z)\frac{\sqrt{3}}{3}\Big\}\end{aligned}$$

Lopulta määritellään

$$\mathbf{F}_K = \Big\{z + rj \in \mathcal{B}_K : z \in \mathcal{F}_K\Big\}.$$



Kuva 7.1: $\mathcal{F}_{\mathbb{Q}(i)}$ sinisellä ja sen rotaatio $-1\mathcal{F}_{\mathbb{Q}(i)}$ punaisella.



Kuva 7.2: $\mathcal{F}_{\mathbb{Q}(\sqrt{-3})}$ sinisellä ja sen rotaatiot $\frac{-1+\sqrt{-3}}{2}\mathcal{F}_{\mathbb{Q}(\sqrt{-3})}$ ja $\frac{-1-\sqrt{-3}}{2}\mathcal{F}_{\mathbb{Q}(\sqrt{-3})}$ punaisella. Lukukunnan primääriperussuunnikas on merkitty vihreällä. Sen pinta-ala $\Delta = \frac{\sqrt{3}}{2}$ on kolminkertainen joukon $\mathcal{F}_{\mathbb{Q}(\sqrt{-3})}$ pinta-alaan verrattuna.

Huomataan, että $\mathcal{P}_K$ on primäärinen perussuunnikas kokonaislukuhilalle. Joukot $\mathcal{F}_{\mathbb{Q}(i)}$ ja $\mathcal{F}_{\mathbb{Q}(\sqrt{-3})}$ on määritelty muista kunnista poiketen eri tavalla, koska tarkoituksena on määritellä $\mathcal{F}_K$ perusalueeksi matriisien ryhmälle $\mathbf{PSL}_2(\mathcal{O}_K)_\infty$ ja kunnat $\mathbb{Q}(i)$ ja $\mathbb{Q}(\sqrt{-3})$ puolestaan sisältävät luvun 1 juuria $\zeta^n = 1$, jolle $n > 2$. Nyt asettamalla $a = \zeta$ ja $d = \zeta^{n-1}$ kuvaus $z \mapsto \zeta z/\zeta^{(n-1)} = z\zeta^2 \neq z$ on ryhmässä $\mathbf{PSL}_2(\mathcal{O}_K)_\infty$ ja täten joukko $\mathcal{F}_K$ on hilan $\mathcal{O}_K$ perussuunnikasta pienempi osajoukko. Tarkemmin sanottuna kunnassa $\mathbb{Q}(i)$ asettamalla $a = i$ ja $d = -i$,

$$(z \mapsto -z) \in \mathbf{PSL}_2(\mathbb{Z}[i])_\infty$$

ja täten perusalue on puolet kokonaislukurenkaan perussuunnikkaasta kuten kuvasta 7.1 näkee.

Vastaavasti kuten kuvasta 7.2 huomaa kunnassa $\mathbb{Q}(\sqrt{-3})$ perusalueen pinta-ala on kolmasosa perussuunnikkaan pinta-alasta.

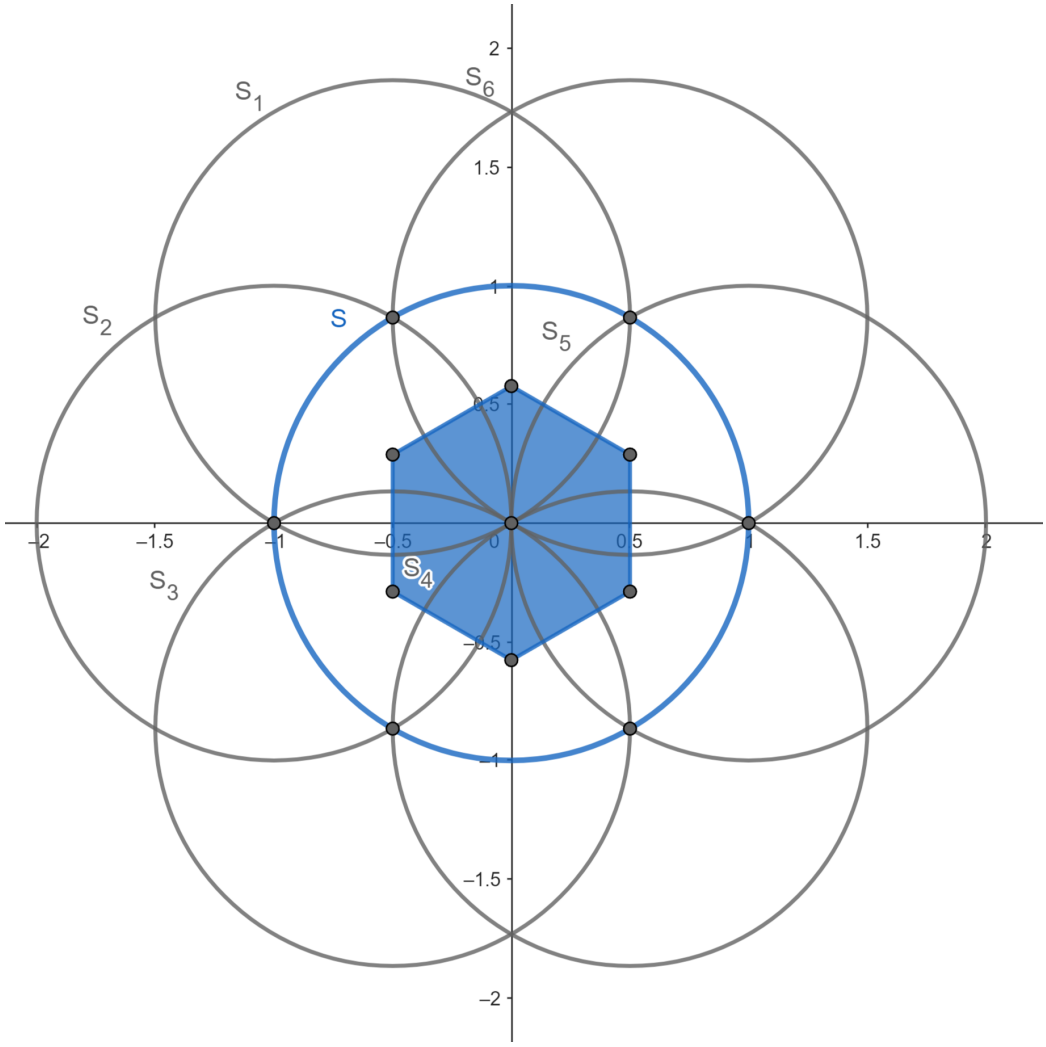
Joukko $\mathcal{B}_K$ on puolestaan Euklidisten puolipallojen rajaama alue. Yhtälö $|z+\frac{d}{c}|^2+r^2 = \frac{1}{|c|^2}$ kertoo, että puolipallojen säteet on $\frac{1}{|c|}$ ja niiden keskipisteet ovat kompleksitasossa pisteissä $\frac{-d}{c}$. Kuva 7.3 kuvaa aluetta $\mathcal{B}_{\mathbb{Q}(\sqrt{-3})}$ ylhäältä päin. Kuvasta voidaan huomata, että kunnassa $\mathbb{Q}(\sqrt{-3})$ joukko $\mathcal{B}_{\mathbb{Q}(\sqrt{-3})}$ muodostaa heksagonaalisen laatoituksen.

Vastaavasti kuva 7.4 kuvaa aluetta $\mathcal{B}_{\mathbb{Q}(\sqrt{-5})}$ ylhäältä päin. Todetaan, että kunnan kokonaisluvut $\mathbb{Z}[\sqrt{-5}]$ voidaan virittää

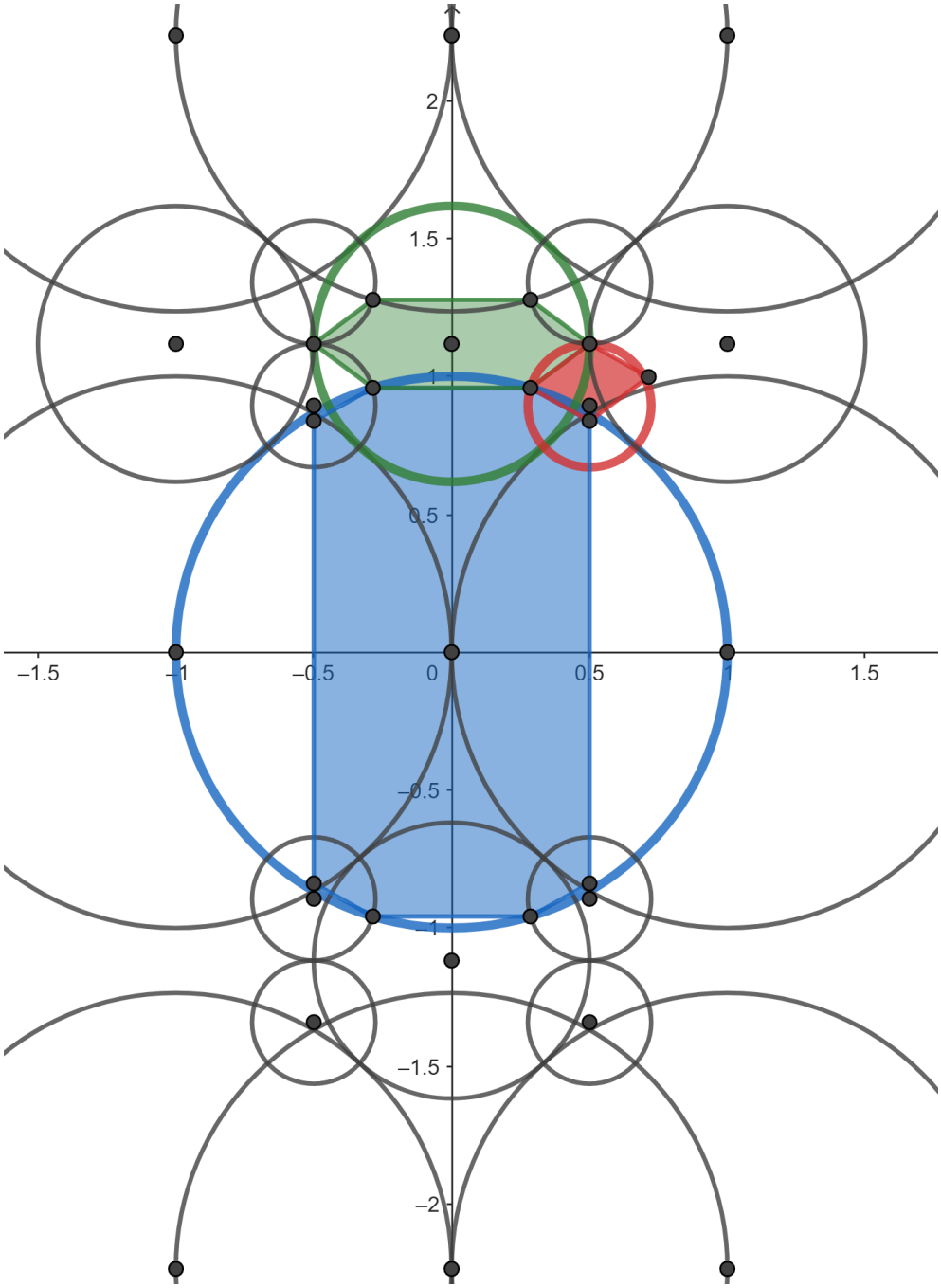
$$\langle 1, 0\rangle = \langle 2, \sqrt{-5}\rangle = \langle 2\sqrt{-5}, 4 + \sqrt{-5}\rangle = \mathbb{Z}[\sqrt{-5}].$$

Väite todistetaan kappaleessa 8.3. Huomataan, että primäärisessä perussuunnikkaassa ainakin murtolukupisteiden $\frac{\sqrt{-5}}{2}$ ja $\frac{1}{2} + \frac{2i}{\sqrt{5}}$ keskeiset puolipallot rajaavat joukkoa $\mathcal{B}_{\mathbb{Q}(\sqrt{-5})}$. Kuvasta huomataan, että kunnassa $\mathbb{Q}(\sqrt{-5})$ joukko $\mathcal{B}_{\mathbb{Q}(\sqrt{-5})}$ seuraa kolmen monikulmion muodostamaa laatoitusta.

Vastaavia joukon $\mathcal{B}_K$ laatoituksia on esitelty lähteen [10] sivulla 346.



Kuva 7.3: Alue $\mathcal{B}_{\mathbb{Q}(\sqrt{-3})}$ origon ympärillä ylhäältä päin kuvattuna. Sinisellä merkityllä alueella puolipallolla S on ympäröiviä puolipalloja S_i korkeampia pisteitä eli kyseisellä alueella S on joukon $\mathcal{B}_{\mathbb{Q}(\sqrt{-3})}$ ainoa merkittävä rajaava puolipallo.



Kuva 7.4: Alue $\mathcal{B}_{\mathbb{Q}(\sqrt{-5})}$ origon ympärillä ylhäältä päin kuvattuna. Sinisellä merkityllä alueella origokeskeisellä puolipallolla on ympäröiviä puolipalloja korkeampia pisteitä. Vastaavasti vihreällä alueella $\frac{1}{2}$ säteinen $\frac{\sqrt{-5}}{2}$ keskeinen puolipallo on korkein ja punaisella alueella $\frac{1}{\sqrt{-5}}$ säteinen $\frac{1}{2} + \frac{2i}{\sqrt{5}}$ keskeinen puolipallo on korkein. Väritetyillä alueilla nämä pallot ovat joukkojen ainoa merkittävät rajaavat puolipallot.

7.2 Todistus, että $\mathbf{F}_K$ on perusalue

Seuraavaksi käydään läpi todistus, että yllä muotoiltu $\mathbf{F}_K$ on ryhmän $\mathbf{PSL}_2(\mathcal{O}_K)$ perusalue. Ennen todistusta osoitetaan hyödyllinen lemma.

Lemma 7.3. *Joukolla $\mathcal{B}_K$ on seuraavat ominaisuudet:*

1. *Piste $P = z + rj \in \mathbb{H}$ sisältyy joukkoon $\mathcal{B}_K$, jos ja vain jos jokaiselle kuvaukselle $\gamma \in \mathbf{PSL}_2(\mathcal{O}_K)$ piste $\gamma P = z' + r'j$ toteuttaa $r' \leq r$.*
2. *Jokaiselle pisteelle $P \in \mathbb{H}$ on olemassa kuvaus $\gamma \in \mathbf{PSL}_2(\mathcal{O}_K)$ siten, että $\gamma P \in \mathcal{B}_K$.*
3. *Olkoon $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{PSL}_2(\mathcal{O}_K)$ siten, että $c \neq 0$. Tällöin $\mathcal{B}_K \cap \gamma\mathcal{B}_K = \mathcal{B}_K \cap \{z + rj : |cz + d|^2 + |c|^2 r^2 = 1\}$.*
4. *$\mathcal{B}_K = \gamma\mathcal{B}_K$, kaikilla $\gamma \in \mathbf{PSL}_2(\mathcal{O}_K)_\infty$.*

Todistus. 1. Olkoon $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{PSL}_2(\mathcal{O}_K)$. Pisteille $P = z + rj \in \mathcal{B}_K$ ja $\gamma P = z' + r'j$, koska

$$|cz + d|^2 + |c|^2 r^2 \geq 1,$$

pätee Määritelmän 4.8 mukaan yhtälö

$$r' = \frac{r}{|cz + d|^2 + |c|^2 r^2} \leq r.$$

Pisteelle $P \notin \mathcal{B}_K$ on määritelmän mukaan olemassa γ siten, että

$$|cz + d|^2 + |d|^2 r^2 < 1$$

ja täten

$$r' = \frac{r}{|cz + d|^2 + |d|^2 r^2} > r.$$

2. Olkoon $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{PSL}_2(\mathcal{O}_K)$, piste $P = z + ri$ ja vakio $M > 0$. Huomioidaan, että

$$|cz + d|^2 + r^2|c|^2 \geq r^2|c|^2$$

ja

$$|cz + d|^2 + r^2|c|^2 \geq ||cz| - |d||^2.$$

Täten on olemassa vain äärellinen määrä kokonaislukuja $c, d \in \mathcal{O}_K$, joille $|cz + d|^2 + r^2|c|^2 \leq M$, koska karkeasti arvioiden saadaan $|c| \leq \sqrt{\frac{M}{r^2}}$ ja

$|d| \leq \sqrt{M}+|zc| \leq \sqrt{M}+\sqrt{\frac{M}{r^2}}|z|$. Kaikilla $c, d \in \mathcal{O}_K$, joille pätee $\langle c, d\rangle = \mathcal{O}_K$, on $a, b \in \mathcal{O}_K$, jolle $ad - bc = 1$ ja täten voidaan valita

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{PSL}_2(\mathcal{O}_K)$$

siten, että $|cz + d|^2 + r^2|c|^2$ on minimaalinen, eli

$$|cz + d|^2 + r^2|c|^2 \leq |\alpha z + \beta|^2 + r^2|\alpha|^2$$

kaikilla $\alpha, \beta \in \mathcal{O}_K$, joille $\langle \alpha, \beta\rangle = \mathcal{O}_K$. Kuvausten $\mathbf{PSL}_2(\mathcal{O}_K)$ määritelmän mukaan pisteen γP j-komponentti on maksimaalinen. Täten kohdan (1) perusteella $\gamma P \in \mathcal{B}_K$.

3. Pisteelle $\gamma P \in \mathcal{B}_K$ kohdan 1 perusteella $r' = r$ ja täten

$$\mathcal{B}_K \cap \gamma\mathcal{B}_K = \mathcal{B}_K \cap \{z + rj : |cz + d|^2 + |c|^2 r^2 = 1\}.$$

4. Olkoon $z + rj \in \mathcal{B}_K$. Kuvaukselle $\gamma \in \mathbf{PSL}_2(\mathcal{O}_K)_\infty$ pätee

$$\gamma(z + rj) = \epsilon z + w + rj$$

jollain kompleksiluvulla $w \in \mathbb{C}$ ja luvun 1 juurella $\epsilon^n = 1$. Riittää osoittaa, että $z + w + rj \in \mathcal{B}_K$ ja $\epsilon z + rj \in \mathcal{B}_K$.

Määritelmän 4.8 perusteella, jos ryhmän $\mathbf{PSL}(\mathcal{O}_K)_\infty$ kuvaus kuvaa pisteen $z + rj \mapsto z' + r'j$, niin se kuvaa myös pisteen $\epsilon z + w + rj \mapsto w' + r'j$ jollain $w' \in \mathbb{C}$. Kohdan 1 perusteella, koska $z + rj \in \mathcal{B}_K$, $r \geq r'$ kaikilla ryhmän $\mathbf{PSL}(\mathcal{O}_K)$ kuvauksilla $z + w + rj \mapsto w' + r'j$ ja täten riittää osoittaa, että $\epsilon z + rj \in \mathcal{B}_K$.

Pisteille $c, d \in \mathcal{O}_K$ pätee $\langle c, d\rangle = \mathcal{O}_K$, jos ja vain jos $xc + yd = 1$ jollain $x, y \in \mathcal{O}_K$. Nyt pisteelle ϵc pätee $\epsilon^{n-1}x\epsilon c + yd = 1$ eli $\langle \epsilon c, d\rangle = \mathcal{O}_K$. Nyt yhtälö

$$|\epsilon cz + d|^2 + c^2|r|^2 \leq 1$$

pätee kaikilla $c, d \in \mathcal{O}_K$, joille $\langle c, d\rangle = \mathcal{O}_K$. Täten $\epsilon z + rj \in \mathcal{B}_K$. ([9], s.319) □

Lemman 7.3 avulla voidaan osoittaa, että $\mathbf{F}_K$ on ryhmän $\mathbf{PSL}_2(\mathcal{O}_K)$ perusalue.

Lause 7.4. $\mathbf{F}_K = \{z + rj \in \mathcal{B}_K : z \in \mathcal{F}_K\}$ *on ryhmän* $\mathbf{PSL}_2(\mathcal{O}_K)$ *perusalue.*

Todistus. Tarkistetaan määritelmän 7.1 vaatimukset. $\mathcal{F}_K$ ja $\mathcal{B}_K$ ovat hyperbolisen avaruuden suljettujen puoliavaruuksien leikkauksia ja täten perusalue $\mathbf{F}_K = \mathcal{F}_K \cap \mathcal{B}_K$ on myös suljettujen puoliavaruuksien leikkaus. Huomioidaan, että $\mathcal{F}_K$ on ryhmän $\mathbf{PSL}_2(\mathcal{O})_\infty$ perusalue kompleksitasossa. Nyt lemma 7.3 osoittaa, että $\bigcup_{\gamma \in \mathbf{PSL}_2(\mathcal{O})} \gamma \mathbf{F}_K = \mathbb{H}$. On selkeää, että joukon $\mathcal{B}_K$ reuna sisältyy joukkoon $\bigcup_{\langle c,d \rangle = \mathcal{O}} \{z + rj : |cz + d|^2 + |d|^2 r^2 = 1\}$. Täten ryhmän $\mathbf{PSL}_2(\mathcal{O}_K)$ kuvaukselle $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, jossa $c \neq 0$, lemman 7.3 mukaan $\mathrm{int}(\mathcal{B}_\mathcal{K}) \bigcap \mathrm{int}(\gamma \mathcal{B}_\mathcal{K}) = \emptyset$. Täten

$$\mathrm{int}(\mathbf{F}_\mathcal{K}) \cap \mathrm{int}(\gamma \mathbf{F}_\mathcal{K}) = \mathrm{int}(\mathbf{F}_\mathcal{K} \cap \gamma \mathbf{F}_\mathcal{K}) = \emptyset$$

kaikille $\gamma \in \mathbf{PSL}_2(\mathcal{O})$, $\gamma \neq I$. ([9], s.319-320) □

Koska $\mathbf{F}_K \subset \mathcal{B}_K$, joukko $\mathcal{B}_K$ rajoittaa perusalueen ja kompleksitason leikkausta. Määritellään täten kompleksitason pisteet, jotka voivat olla joukon sulkeuman $\mathcal{B}_K$ alkioita.

Määritelmä 7.5. Olkoon K toisen asteen imaginäärinen lukukunta. Piste $s \in \mathbb{C}$ on *singulaaripiste* kunnassa K, jos $|cs + d| \geq 1$ kaikilla $\langle c, d \rangle = \mathcal{O}_K$. Kunnan K singulaaristen pisteiden joukkoa merkitään S_K. ([9], s.317)

Todistetaan seuraavaksi, että singulaariset pisteet ovat kunnassa K. Todistusta varten todistetaan ensin approksimaatiotulos.

Lemma 7.6. *Olkoon K toisen asteen imaginäärinen lukukunta. On olemassa vain kunnasta K riippuva vakio M, jolle kaikille $z \in \mathbb{C} - K$ on äärettömästi alkioita $c, d \in \mathcal{O}_K$ joille*

$$\left| z + \frac{d}{c} \right| \leq \frac{M}{|c|^2}.$$

Todistus. Olkoon $P = \{r_1 + \omega r_2 : 0 \leq r_1 \leq 1, 0 \leq r_2 \leq 1\}$ kunnan primääri perussuunnikas ja δ sen halkaisija. Luonnolliselle luvulle m jaetaan perussuunnikas P m^2 yhtäsuureen osaan P_t jakamalla joukko P välien $0 \leq r_1 \leq 1$ ja $0 \leq r_2 \leq 1$ suhteen m yhtäsuureen osaan. Joukon P_t halkaisija on nyt $\frac{\delta}{m}$. Koska primäärin perussuunnikkaan P kärjet ovat kokonaislukurenkaassa, joukossa $mP \cap \mathcal{O}_K$ on $(m+1)^2$ alkiota. Jos $z \notin K$, koska joukkoja P_t on vain m^2 kappaletta, on erilliset alkiot $c_1, c_2 \in mP \cap \mathcal{O}_K$ joille $c_1 z, c_2 z \in P_t$ mod $\mathcal{O}_K$ jollain P_t. Täten on alkiot $d_1, d_2 \in \mathcal{O}_K$ jolle $|c_1 z + d_1 - c_2 z - d_2| \leq \frac{\delta}{m}$. Määritellään $c = c_1 - c_2$ ja $d = d_1 - d_2$, jolloin, koska $c_1, c_2 \in mP$,

$$|c| = |c_1 - c_2| \leq |m(1 + \omega)|.$$

Täten saadaan

$$|z + \frac{d}{c}| \leq \frac{\delta}{m|c|} \leq \frac{M}{|c|^2}$$

vain kunnasta K riippuvalla vakiolla $M = \delta|1 + \omega|$. Koska $z \notin K$, ja m voi olla vapaavalintaisen suuri, alkioita $c, d \in \mathcal{O}_K$ on äärettömästi. ([9], s.315-316) □

Lemma 7.7. *Toisen asteen imaginäärisen lukukunnan singulaaripisteille pätee*

$$S_K \subset K.$$

Todistus. Olkoon $z \in \mathbb{C} - K$. Määritelmien 2.17 ja 2.21 mukaan voidaan valita jokaiselle ideaaliluokalle edustaja $I_1, I_2, \ldots, I_n \subset \mathcal{O}_K$. Määritetään

$$N = \max\{N(I_1), N(I_2), \ldots, N(I_n)\}.$$

Nyt alkioille $c, d \in \mathcal{O}_K$, joille pätee $|z + \frac{d}{c}| \leq \frac{M}{|c|^2}$, on olemassa $q \in K - \{0\}$, jolle $\langle q\rangle\langle c, d\rangle = I_i$ jollain i. Täten $|q|^2 \leq N(I_i)(N(\langle c, d\rangle))^{-1} \leq N(I_i) \leq N$. Alkioille $qa = c$, $qb = d$ saadaan

$$\begin{aligned}\left|z + \frac{b}{a}\right| &= \left|z + \frac{d}{c}\right| \\ &\leq \frac{M}{|c|^2} \\ &= \frac{M|q|^2}{|a|^2} \\ &\leq \frac{MN}{|a|^2}.\end{aligned}$$

Koska ideaaliluokkien edustajat valittiin kokonaislukurenkaassa, niin myös $qa, qb \in \mathcal{O}_K$. Täten jollekin kiinnitetylle I_i on Lemman 7.6 mukaan äärettömästi alkioita $c, d \in \mathcal{O}_K$, joille pätee $|z + \frac{d}{c}| \leq \frac{MN}{|c|^2}$ vakiolla NM ja $\langle c, d\rangle = I_i$.

Todistetaan seuraavaksi, että ideaalille $J \subset \mathcal{O}_K$ ja alkiolle $j \in J - \{0\}$ on vakio $K \in]0, \infty[$, joka riippuu vain ideaalista J ja alkiosta j siten, että, jos $\langle c, d\rangle = J$ ja $d \neq 0$, on olemassa $a, b \in \mathcal{O}_K$, joille pätee yhtälö $ac - bd = j$, epäyhtälö $|b| \leq K|d|$ ja $\langle a, b\rangle = \mathcal{O}_K$. Lemman 2.15 perusteella on $k \in J$, jolle $J = \langle j, k\rangle$. Vastaavasti kuin Lemman 5.1 todistuksessa valitaan $\theta \in K - \{0\}$, jolle $J^n = \langle\theta\rangle$ ja $\alpha_1, \alpha_2, \beta_1, \beta_2, \lambda \in J^{n-1}$ siten, että

$$c(\alpha_1 + d\lambda) + d\alpha_2 = \theta = j\beta_1 + k\beta_2$$

ja $|\alpha_1| \leq r|d|$ jollain $r \in \mathbb{R}$. Määritellään

$$b = \frac{j(\alpha_1 + d\lambda) + d\beta_2}{\theta}$$

ja

$$a = \frac{j - c\beta_2}{\theta}.$$

Nyt $ac + bd = \frac{j(c(\alpha_1+d\lambda)+d\alpha_2)}{\theta} = j$ ja $\langle a, b\rangle = \mathcal{O}_K$. Lisäksi saadaan

$$|b| \leq \Big|\frac{jr + j\lambda + \beta_2}{\theta}\Big||d| = K|d|$$

Olkoon alkio $p \in I_i - \{0\}$. Kaikille Lemman 7.6 ehdot toteuttaville pareille $c, d \in \mathcal{O}_K$, missä $d \neq 0$, voidaan nyt Lemman 2.15 perusteella valita alkiot $x, y \in \mathcal{O}_K$ jolle $|x| \leq K|d|$, $\langle x, y\rangle = \mathcal{O}_K$ ja $xc - yd = p$. Koska pareja $c, d \in \mathcal{O}_K$ on äärettömästi, kaikille vakioille $v \in \mathbb{R}$ on äärettömästi pareja, joille pätee $v < |d|$. Oletetaan, että $|d| > |p|$. Nyt

$$\begin{aligned}\Big|z - \frac{y}{x}\Big| &\leq \Big|z - \frac{c}{d}\Big| + \Big|\frac{c}{d} - \frac{y}{x}\Big| \\ &\leq \frac{MN}{|d|^2} + |\frac{cx - dy}{dx}| \\ &= \frac{MN}{|d|^2} + \frac{|p|}{|dx|}.\end{aligned}$$

Nyt, koska $|x|K^{-1} \leq |d|$, saadaan

$$\begin{aligned}\frac{MN}{|d|^2} + \frac{|p|}{|dx|} &\leq \frac{MNK^2}{|x|^2} + \frac{|p|K}{|x|^2} \\ &= \frac{C}{|x|^2},\end{aligned}$$

missä $C = MNK^2 + |p|K$. Koska $|d|$ voidaan valita epäyhtälössä mielivaltaisen suureksi saadaan äärettömästi pareja $x, y \in \mathcal{O}_K$, joille $|x, y| = \mathcal{O}_K$ ja

$$|z - \frac{y}{x}| \leq \frac{C}{|x|^2}.$$

Täten, jos $z \notin K$, voidaan valita $x, y \in \mathcal{O}_K$ joille $\langle x, y\rangle = \mathcal{O}_K$ ja $|x|^2 > C$. Tällöin $|z - \frac{y}{x}| < 1$ ja $z \notin S_K$. Täten $S_K \subset K$. ([9], s.316-318) □

Seuraava huomio on tämän tutkielman keskeinen geometrinen havainto.

Lause 7.8. *Jos ryhmän* $\mathbf{PSL}_2(\mathcal{O}_K)$ *perusalueen sulkeuma leikkaa kanonisessa muodossaan kompleksitasoa* $\mathbb{C}$*, niin ryhmässä* $\mathcal{J}_K$ *on vähintään kaksi alkiota.*

Todistus. Perusalueen määritelmän mukaan äärettömyyspiste kuuluu perusalueen sulkeumaan ja se on algebrallinen kärki. Jos perusalueen sulkeuma leikkaa kompleksitasoa pisteessä z, niin

$$z \in \mathcal{B}_K \cap \mathbb{C} \subset S_K \subset K$$

osoittaa, että perusalue leikkaa kompleksitasoa kunnan K pisteessä. Lause 6.9 osoittaa, että $z = \frac{z_1}{z_2} \in \mathbb{C}$, missä $z_2 \neq 0$, tulkittuna projektiivisen avaruuden pisteenä $[z_1, z_2] \in \mathbb{P}^1 K$ on myös algebrallinen kärki. Todistetaan antiteesillä, että kärjet eivät kuvaudu toisikseen ryhmän $\mathbf{PSL}_2(\mathcal{O}_K)$ kuvauksilla. Jos $\gamma[1,0] = [z_1, z_2]$ jollain $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{PSL}_2(\mathcal{O}_K)$, saadaan $z_1 = a$ ja $z_2 = c$, joten $z_1 d + z_2 b = 1$ ja täten $\langle z_1, z_2 \rangle = \mathcal{O}_K$. Nyt joukon $\mathcal{B}_K$ määritelmän perusteella piste $w + rj$ jollain $w \in \mathbb{C}$ sisältyy joukkoon $\mathcal{B}_K$ vain, jos $|w - \frac{z_1}{z_2}| + |z_2|^2 r^2 \geq 1$. Täten on olemassa hyperbolinen puoliavaruus, joka on z-keskeinen Euklidinen puolipallo, joka se ei leikkaa joukkoa $\mathcal{B}_K$. Täten piste z ei sisälly perusalueen sulkeumaan. Lauseen 5.3 perusteella,

$$\#(\mathcal{J}_K) = \#(\mathbf{PSL}_2(\mathcal{O}_K) \backslash C_{\mathbf{PSL}_2(\mathcal{O}_K)}) > 1.$$

□

8 Esimerkkejä perusalueiden geometriasta

Esitellään vielä esimerkeiksi algebrallisten kuntien $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{-3})$ ja $\mathbb{Q}(\sqrt{-5})$ perusalueet ja luokkaluvut. On hyvä huomioida, että $\langle 1, 0 \rangle = \mathcal{O}_K$ kaikissa kunnissa. Tämän kappaleen tulokset perustuvat lähteen [9] sivuihin 324-327.

8.1 Kunnan $\mathbb{Q}(i)$ perusalue

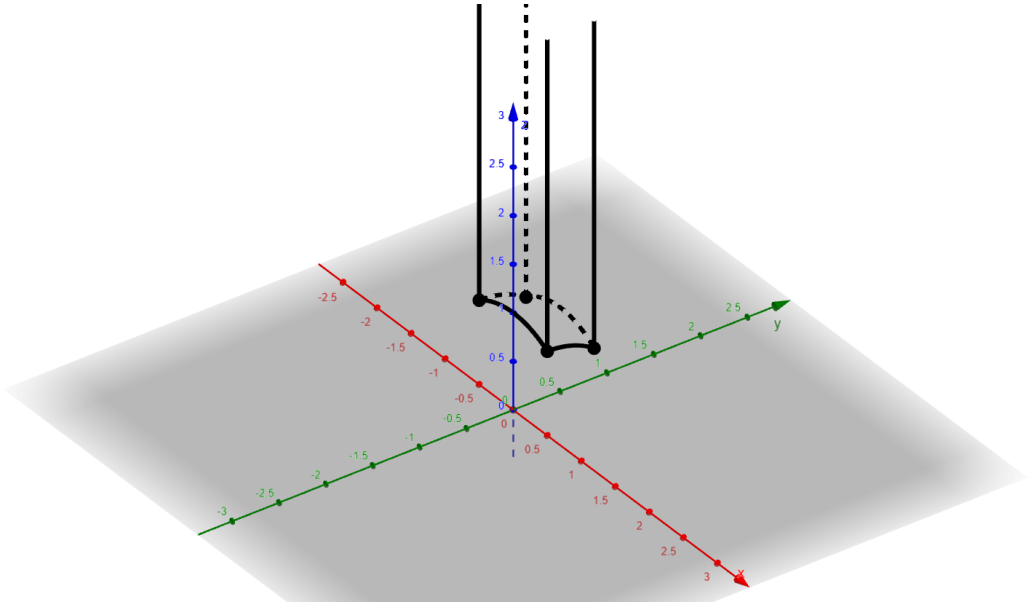
Aloitetaan esittelemällä Gaussin kokonaislukujen $\mathcal{O}_{\mathbb{Q}(i)} = \mathbb{Z}[i]$ perusalue. Gaussin kokonaisluvut on yksinkertaisin toisen asteen lukukunnan kokonaislukujen rengas ja sen perusalue on vastaavasti kohtuullisen helppo havainnoida.

Esimerkki 8.1 ($K = \mathbb{Q}(i)$)**.** Kunnassa $K = \mathbb{Q}(i)$ määritelmän perusteella

$$\mathcal{F}_{\mathbb{Q}(i)} = \left\{ z \in \mathbb{C} : 0 \leq |\mathrm{Re}(z)| \leq \frac{1}{2},\ 0 \leq \mathrm{Im}(z) \leq \frac{1}{2} \right\}$$

ja joukon $\mathcal{B}_{\mathbb{Q}(i)}$ ainoa joukon $\mathcal{F}_{\mathbb{Q}(i)}$ leikkauksessa merkittävä puolipallon rajaama joukko on

$$\{ z + rj : |z|^2 \geq 1 \} \supset \mathcal{B}_{\mathbb{Q}(i)}.$$



Kuva 8.1: Kunnan $\mathbb{Q}(i)$ perusalue hyperbolisessa puoliavaruudessa.

Täten perusalue on

$$\mathbf{F}_{\mathbb{Q}(i)} = \Big\{ z + rj \in \mathbb{H} : 0 \leq |\mathrm{Re}(z)| \leq \frac{1}{2},\ 0 \leq \mathrm{Im}(z) \leq 2, z\overline{z} \geq 1 \Big\}.$$

Huomataan, että $\mathbf{F}_{\mathbb{Q}(i)}$ on hyperbolinen pyramidi, jonka kärjet ovat pisteet $P_1 = \frac{1}{2} + j\frac{\sqrt{3}}{2}$, $P_2 = \frac{-1}{2} + j\frac{\sqrt{3}}{2}$, $P_3 = \frac{1}{2} + i\frac{1}{2} + j\frac{\sqrt{2}}{2}$, $P_4 = \frac{-1}{2} + i\frac{1}{2} + j\frac{\sqrt{2}}{2}$ ja $P_5 = \infty$. Piste $P_5 = \infty$ on sen ainoa algebrallinen kärki.

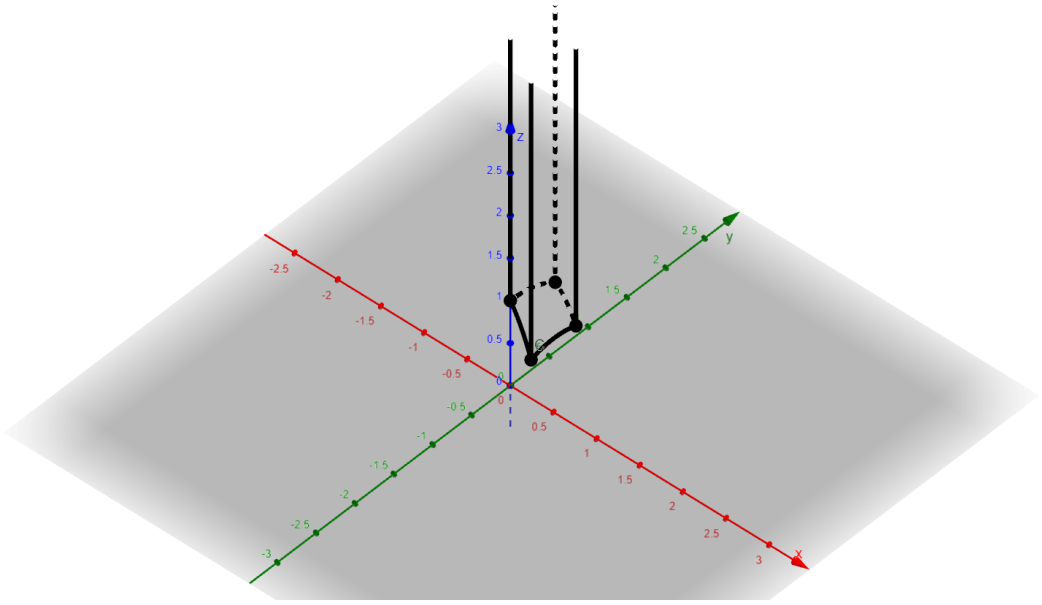
Kuten kuvasta 1 näkee, kunnan $\mathbb{Q}(i)$ perusalue ei leikkaa kompleksitasoa missään pisteessä. Täten voimme havainnoida, että kunnan $\mathbb{Q}(i)$ luokkaluku on 1.

8.2 Kunnan $\mathbb{Q}(\sqrt{-3})$ perusalue

Käsitellään seuraavaksi kunnan $\mathbb{Q}(\sqrt{-3})$ perusaluetta.

Esimerkki 8.2 ($K = \mathbb{Q}(\sqrt{-3})$)**.** Määritelmän mukaan kunnassa $\mathbb{Q}(\sqrt{-3})$

$$\begin{aligned}\mathcal{F}_{\mathbb{Q}(\sqrt{-3})} = &\Big\{ z \in \mathbb{C} : 0 \leq \mathrm{Re}(z),\ \mathrm{Re}(z)\frac{\sqrt{3}}{3} \leq \mathrm{Im}(z) \leq (1 - \mathrm{Re}(z))\frac{\sqrt{3}}{3} \Big\} \\ &\cup \Big\{ z \in \mathbb{C} : 0 \leq \mathrm{Re}(z) \leq \frac{1}{2},\ -\mathrm{Re}(z)\frac{\sqrt{3}}{3} \leq \mathrm{Im}(z) \leq \mathrm{Re}(z)\frac{\sqrt{3}}{3} \Big\}\end{aligned}$$



Kuva 8.2: Kunnan $\mathbb{Q}(\sqrt{-3})$ perusalue hyperbolisessa puoliavaruudessa.

ja joukon $\mathcal{B}_{\mathbb{Q}(\sqrt{-3})}$ ainoa joukon $\mathcal{F}_{\mathbb{Q}(\sqrt{-3})}$ leikkauksessa merkittävä puolipallon rajaama joukko on

$$\{z + rj : |z|^2 + r^2 \geq 1\} \supset \mathcal{B}_{\mathbb{Q}(\sqrt{-3})}.$$

Nyt perusalue $\mathbf{F}_{\mathbb{Q}(\sqrt{-3})}$ muodostuu leikkauksesta

$$\{z + rj \in \mathbb{H} : z \in \mathcal{F}_{\mathbb{Q}(\sqrt{-3})},\ z\overline{z} + r^2 \geq 1\}.$$

Huomioidaan, että $\mathbf{F}_{\mathbb{Q}(\sqrt{-3})}$ on myös hyperbolinen pyramidi, jonka kärjet ovat pisteet $P_1 = j$, $P_2 = \frac{1}{2} - i\frac{\sqrt{3}}{6} + j\frac{\sqrt{6}}{3}$, $P_3 = \frac{1}{2} + i\frac{\sqrt{3}}{6} + j\frac{\sqrt{6}}{3}$, $P_4 = i\frac{\sqrt{3}}{3} + j\frac{\sqrt{6}}{3}$ ja $P_5 = \infty$. Piste $P_5 = \infty$ on sen ainoa algebrallinen kärki.

Vastaavasti kuin kunnassa $\mathbb{Q}(i)$ kuvasta 8.2 näkee, että kunnan $\mathbb{Q}(\sqrt{-3})$ luokkaluku on 1. Täten molempien kuntien kokonaislukujen renkaissa on olemassa yksikäsitteinen alkutekijöihin jako. Seuraavaksi esitellään kunta, jonka luokkaluku on suurempi kuin 1.

8.3 Kunnan $\mathbb{Q}(\sqrt{-5})$ perusalue

Kun kuvaillaan kunnan $K = \mathbb{Q}(\sqrt{-5})$ perusaluetta on symmetrian kannalta hyödyllistä ensin kuvata perusalue matriisilla

$$\gamma = \begin{pmatrix} 1 & \frac{-1-\sqrt{-5}}{2} \\ 0 & 1 \end{pmatrix} \in \mathbf{PSL}_2(\mathbb{Q}(\sqrt{-5})).$$

Joukko $\gamma\mathcal{F}_{\mathbb{Q}(\sqrt{-5})} = \tilde{\mathcal{F}}_{\mathbb{Q}(\sqrt{-5})}$ on selkeästi myös äärettömän stabilisoijan perusalue, mutta kuvaus siirtää perusaluetta $\tilde{\mathcal{F}}_{\mathbb{Q}(\sqrt{-5})} = \mathcal{F}_K - \frac{1+\sqrt{-5}}{2}$. Määritellään vielä

$$\tilde{\mathbf{F}}_{\mathbb{Q}(\sqrt{-5})} = \tilde{\mathcal{F}}_{\mathbb{Q}(\sqrt{-5})} \cap \mathcal{B}_{\mathbb{Q}(\sqrt{-5})}.$$

Esimerkki 8.3 ($K = \mathbb{Q}(\sqrt{-5})$)**.** Huomataan aluksi, että

$$(\sqrt{-5}^2 + 2^2)^2 = 1$$

ja

$$(2\sqrt{-5})^2 + (4 + \sqrt{-5})(4 - \sqrt{-5}) = -20 + 21 = 1.$$

Nyt kunnan $\mathbb{Q}(\sqrt{-5})$ kokonaisluvulle $a \in \mathbb{Z}[\sqrt{-5}]$ on olemassa kokonaisluvut $b, c, d, e \in \mathbb{Z}[\sqrt{-5}]$ joille

$$\sqrt{-5}b + 2c = a(\sqrt{-5}^2 + 2^2)^2 = a$$

ja

$$2\sqrt{-5}d + (4 + \sqrt{-5})e = a((2\sqrt{-5})^2 + (4 + \sqrt{-5})(4 + \sqrt{-5} - 2\sqrt{-5})) = a.$$

Täten alkiot vitittävät kokonaislukurenkaan

$$\langle \pm 1, 0\rangle = \langle \pm 2, \pm\sqrt{-5}\rangle = \langle \pm 2\sqrt{-5}, \pm 4 \pm \sqrt{-5}\rangle = \mathcal{O}_K.$$

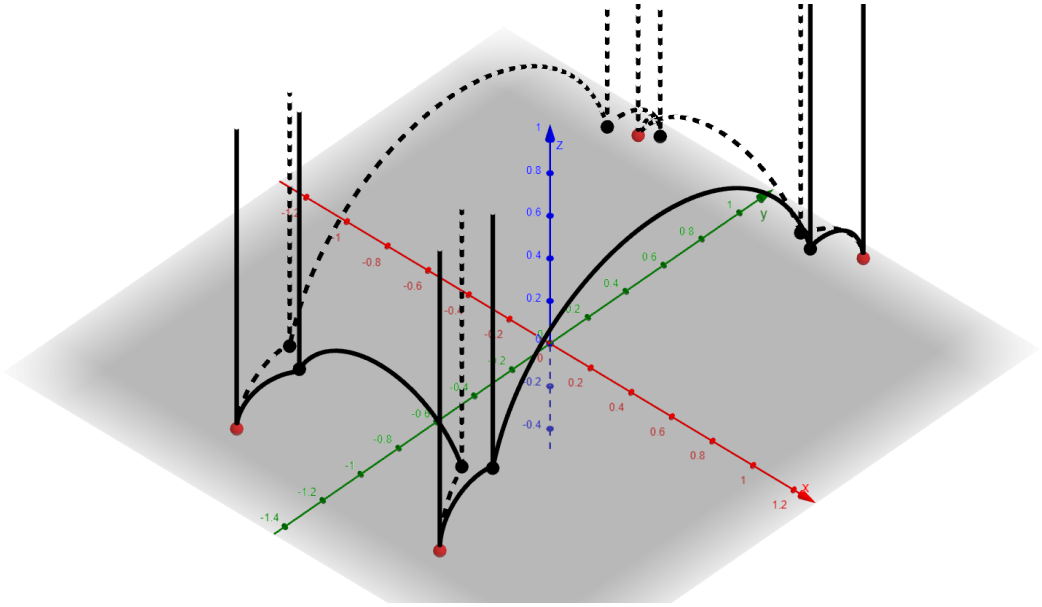
Tällöin saadaan

$$\tilde{\mathcal{F}}_{\mathbb{Q}(\sqrt{-5})} = \Big\{ z : -\frac{1}{2} \geq \mathrm{Re}(z) \geq \frac{1}{2},\ \frac{-\sqrt{5}}{2} \geq \mathrm{Im}(z) \geq \frac{\sqrt{5}}{2} \Big\}.$$

Lisäksi joukkojen $\mathcal{B}_{\mathbb{Q}(\sqrt{-5})}$ ja $\mathcal{F}_{\mathbb{Q}(\sqrt{-5})}$ leikkaus on identtinen puolipallojen rajaaman joukon

$$\Big\{ z + rj : |z|^2 + r^2 \geq 1,\ |2z \pm \sqrt{-5}|^2 + 4r^2 \geq 1,\\ |2\sqrt{-5}z \pm 4 \pm \sqrt{-5}|^2 + 20r^2 \geq 1 \Big\}$$

leikkauksen joukon $\mathcal{F}_{\mathbb{Q}(\sqrt{-5})}$ kanssa. ([18], s.65-70)



Kuva 8.3: Kunnan $\mathbb{Q}(\sqrt{-5})$ perusalue hyperbolisessa puoliavaruudessa. Algebralliset kärkipisteet P_1, P_2, P_3 ja P_4 on merkitty punaisella.

Huomataan, että perusalue on monitahokas, jonka kärjet ovat

$$P_1 = \frac{1}{2} + i\frac{\sqrt{5}}{2}, \qquad P_2 = \frac{-1}{2} + i\frac{\sqrt{5}}{2},$$
$$P_3 = \frac{1}{2} - i\frac{\sqrt{5}}{2}, \qquad P_4 = \frac{-1}{2} - i\frac{\sqrt{5}}{2},$$
$$P_5 = \frac{2}{5} + i\frac{2\sqrt{5}}{2} + j\frac{1}{5}, \qquad P_6 = \frac{-2}{5} + i\frac{2\sqrt{5}}{2} + j\frac{1}{5},$$
$$P_7 = \frac{2}{5} - i\frac{2\sqrt{5}}{2} + j\frac{1}{5}, \qquad P_8 = \frac{-2}{5} - i\frac{2\sqrt{5}}{2} + j\frac{1}{5},$$
$$P_9 = \frac{1}{2} + i\frac{3\sqrt{5}}{2} + j\frac{\sqrt{3}}{8}, \qquad P_{10} = \frac{-1}{2} + i\frac{3\sqrt{5}}{2} + j\frac{\sqrt{3}}{8},$$
$$P_{11} = \frac{1}{2} - i\frac{3\sqrt{5}}{2} + j\frac{\sqrt{3}}{8}, \qquad P_{12} = \frac{-1}{2} - i\frac{3\sqrt{5}}{2} + j\frac{\sqrt{3}}{8} \text{ ja}$$
$$P_{13} = \infty.$$

On hyvä huomioida, että pisteet P_1, P_2, P_3, P_4 ja P_{13} ovat algebrallisia kärkiä.

Nyt algebrallisista kärjistä huomataan selkeästi, että kunnan $\mathbb{Q}(\sqrt{-5})$ luokkaluku on suurempi kuin 1. Täten luokkaluvun ja hyperbolisen perusalueen välinen yhteys on selkeästi demonstroitu. Perusalueen ja kompleksitason leikkauspisteiden määrä ei kuitenkaan vielä itsessään kerro tarkkaa

luokkalukua. Tarkan luokkaluvun määrittäminen ei kuitenkaan tyypillisesti ole tarpeellista, koska kunnan kokonaislukujen renkaan alkiot voidaan jakaa alkutekijöihin vain, kun kunnan luokkaluku on 1.

Itseasiassa on tunnettua, että toisen asteen imaginäärisistä lukukunnista $\mathbb{Q}(\sqrt{d})$ vain yhdeksän luokkaluku on 1. Nämä lukukunnat ovat $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{-2})$, $\mathbb{Q}(\sqrt{-3})$, $\mathbb{Q}(\sqrt{-7})$, $\mathbb{Q}(\sqrt{-11})$, $\mathbb{Q}(\sqrt{-19})$, $\mathbb{Q}(\sqrt{-43})$, $\mathbb{Q}(\sqrt{-67})$ ja $\mathbb{Q}(\sqrt{-163})$, kuten Harold Starkin kirjassa An Introduction to Number Theory sivulla 295 on esitelty. [17] Tulos osoittaa että hyvin harvassa toisen asteen imaginäärisessä lukukunnassa on yksikäsitteinen tekijöihinjako ja vastaavasti perusalueen ja kompleksitason leikkauspisteiden tutkiminen ei pääasiallisesti ole triviaalia. Tämän lisäksi lähteen [6] sivulla 233 on esitelty algoritmi toisen asteen imaginäärisen lukukunnan luokkaluvun laskemiseen kunnan diskriminantista. Algoritmi mahdollistaa luokkalukujen laskemisen automatisoinnin ja täten kuntien $\mathbb{Q}(\sqrt{d})$ luokkaluvut onkin esitetty kaikille $d \in \{1, 2, \ldots, 1000\}$ lähteessä [12].

Lähdeluettelo

[1] Alaca S., Williams K.: *Introductory Algebraic Number Theory* Cambridge University Press, 2004

[2] Artin M.: *Algebra* toinen painos, Prentice-Hall, 2011

[3] Ash R.: *A Course In Algebraic Number Theory* Dover Publications 2010

[4] Beardon A.: *The Geometry of Discrete Groups* New York : Dover Publications, 1980

[5] Schlag W.: *A Course in Complex Analysis and Riemann Surfaces* American Mathematical Society, 2014

[6] Cohn H.: *A course in computational algebraic number theory* korjattu kolmas painos Springer-Verlag 1996, Springer-Verlag, 1993

[7] Cohn H.: *Advanced Number Theory* korjattu toinen painos Springer-Verlag 1995, Springer-Verlag, 1983

[8] Dummit D., Foote R.: *Abstract Algebra* kolmas painos, John Wiley & Sons Inc, 2004

[9] Elstrodt J., Grunewald F., Mennicke J.: *Groups Acting on Hyperbolic Spaces; Harmonic Analysis and Number Theory* Springer-Verlag, 1998

[10] Hatcher A.: *Hyperbolic Structures of Arithmetic Type on Some Link Complements* Journal of the London Mathematical Society 2, sivut 2-27, 1983

[11] Iversen B.: *Hyperbolic Geometry* Cambridge University Press, 1992

[12] Jasinski A.: sarjanumero A202084 sivustolla *The On-Line Encyclopedia of Integer Sequences*, julkaistu osoitteessa https://oeis.org, 2011 (luettu 06.05.2024)

[13] Katz V.: *History of mathematics; An Introduction* Addison-Wesley, 2009

[14] Marcus D.: *Number Fields* toinen painos Springer International Publishing AG 2018, Springer-Verlag, 1977

[15] Minkowski H.: *Geometrie der Zahlen* Leipzig, Teubner 1910

[16] Parkkonen J.: *Geometry; Lectures at the University of Jyväskylä fall semester 2020* osoitteessa http://users.jyu.fi/~parkkone/Geometry2020/Geometry2020.pdf, (luettu 20.04.2024)

[17] Stark H.: *An Introduction to Number Theory* Markham Publishing Company, 1970

[18] Swan R.: *Generators and Relations for Certain Special Linear Groups* Advances in Mathematics 1, sivut 1-77, 1971