EVERHART, LANCE M., M.A. On Generators of Hilbert Modular Groups of Totally Real Number Fields. (2016)
Directed by Dr. Sebastian Pauli. 54 pp.

In this paper we report the beginnings of the computations and tabulations of the generators of $\mathrm{PSL}_2(\mathcal{O}_K)$, where $\mathcal{O}_K$ is the maximal order of a real field of degree $n = [K : \mathbb{Q}]$. We discuss methods of obtaining generators in order to calculate the values of invariants of the congruence subgroups.

ON GENERATORS OF HILBERT MODULAR GROUPS OF TOTALLY REAL NUMBER FIELDS

by

Lance M. Everhart

A Thesis Submitted to
the Faculty of The Graduate School at
The University of North Carolina at Greensboro
in Partial Fulfillment
of the Requirements for the Degree
Master of Arts

Greensboro
2016

Approved by

_____
Committee Chair

To my family, who are always there to lift me up.

APPROVAL PAGE

This thesis written by Lance M. Everhart has been approved by the following committee of the Faculty of The Graduate School at The University of North Carolina at Greensboro.

Committee Chair _____
Sebastian Pauli

Committee Members _____
Greg Bell

_____
Dan Yasaki

_____
Date of Acceptance by Committee

_____
Date of Final Oral Examination

ACKNOWLEDGMENTS

I would like to thank my advisor Dr. Sebastian Pauli, who helped me every step of the way with my research and who is always willing to answer any question I had with great patience.

TABLE OF CONTENTS

Page

LIST OF TABLES

Page

CHAPTER I

INTRODUCTION

Let K be a totally real algebraic number field. The Hilbert modular group of K is $\mathrm{PSL}_2(\mathcal{O}_K)$ where $\mathcal{O}_K$ is the ring of integers of K.

Research on the Hilbert modular groups began around 1893 with David Hilbert, who later proposed the study of the function theory of $\mathrm{PSL}_2(\mathcal{O}_K)$ to his student Ludwig Otto Blumenthal. With this, Hilbert and Blumenthal hope to create a theory of modular functions of multiple variables that could be as important to number theory as their classical counterparts. Blumenthal [Blu03] gave a detailed outline of the function theory used in his work. However, Blumenthal's construction of a fundamental domain had a flaw where he concluded that a fundamental domain of the action had only one cusp as in the classical modular group. This was later corrected by Hans Maaß who proved that the number of cusps are equal to the class number of K [Maa].

In this thesis, we first give the background needed for understanding the Hilbert modular groups, such as definitions, theorems and their applications. We then give methods for calculating the generators of the Hibert modular groups for special cases where $K = \mathbb{Q}(\sqrt{d})$ is a real quadratic field along with methods for a general real number field of degree n.

CHAPTER II

THE MODULAR GROUP

2.1 Actions of the Special Linear Group on $\mathfrak{H}$

Definition 2.1. The *general linear group* of degree 2 over the reals, denoted $\mathrm{GL}_2(\mathbb{R})$, is defined by

$$\mathrm{GL}_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \ : \ ad - bc \neq 0, \ a, b, c, d \in \mathbb{R} \right\}.$$

Definition 2.2. The *special linear group* of degree 2 over the reals, denoted $\mathrm{SL}_2(\mathbb{R})$, is defined by

$$\mathrm{SL}_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \ : \ ad - bc = 1, \ a, b, c, d \in \mathbb{R} \right\}.$$

Definition 2.3. The *projective special linear group* of degree 2 over the reals, denoted $\mathrm{PSL}_2(\mathbb{R})$, is the quotient

$$\mathrm{PSL}_2(\mathbb{R}) = \mathrm{SL}_2(\mathbb{R})/\{E, -E\}.$$

where $E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

Let $\mathfrak{H}$ be the *complex upper half-plane*,

$$\mathfrak{H} = \{z \in \mathbb{C} : \Im z > 0\}.$$

The group $\mathrm{SL}_2(\mathbb{R})$ acts on $\mathfrak{H}$ via the Möbius transformations

$$\mathrm{SL}_2(\mathbb{R}) \times \mathfrak{H} \to \mathfrak{H}$$

where, for any $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{R})$ and any $z \in \mathfrak{H}$, we have

$$Mz = \frac{az+b}{cz+d}.$$

The following lemma that we have proven shows that this action is closed in $\mathfrak{H}$.

Lemma 2.4. *For any $M \in \mathrm{SL}_2(\mathbb{R})$ and any $z \in \mathfrak{H}$, $Mz \in \mathfrak{H}$.*

Proof. Let $M \in \mathrm{SL}_2(\mathbb{R})$, and let $z \in \mathfrak{H}$. Then we have

$$Mz = \frac{az+b}{cz+d} = \frac{(a\Re(z)+b)+ia\Im(z)}{(c\Re(z)+d)+ic\Im(z)}$$

$$= \frac{[(a\Re(z)+b)+ia\Im(z)]\,[(c\Re(z)+d)-ic\Im(z)]}{|cz+d|^2}$$

$$= \frac{ac\Re(z)^2+(bc+ad)\Re(z)+bd+ac\Im(z)^2}{|cz+d|^2} + i\frac{ad\Im(z)-cb\Im(z)}{|cz+d|^2}$$

$$= \frac{ac\Re(z)^2+(bc+ad)\Re(z)+bd+ac\Im(z)^2}{|cz+d|^2} + i\frac{\Im(z)}{|cz+d|^2}.$$

Thus, we can see that

$$\Im(Mz) = \frac{\Im(z)}{|cz+d|^2} > 0.$$

Therefore, Mz is contained in $\mathfrak{H}$.

□

Let $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{PSL}_2(\mathbb{R})$, then $M = -M$ in $\mathrm{PSL}_2(\mathbb{R})$ and, for any $z \in \mathfrak{H}$,

$$Mz = \frac{az+b}{cz+d} = \frac{-az-b}{-cz-d} = (-M)z.$$

Thus, this action descends to give an action of $\mathrm{PSL}_2(\mathbb{R})$ on $\mathfrak{H}$.

Now, we give some basic definitions pertaining to these group actions. (Compare to [Fre90] and [Hir73]).

Definition 2.5. A subgroup $\Gamma \subset \mathrm{SL}_2(\mathbb{R})$ is *discrete* if the intersection of Γ with any compact subset $K \subset \mathrm{SL}_2(\mathbb{R})$ is a finite set.

Definition 2.6. A subgroup $\Gamma \subset \mathrm{SL}_2(\mathbb{R})$ acts *discontinuously* on $\mathfrak{H}$ if for any two compact subsets $K_1,\ K_2 \subset \mathfrak{H}$, the set

$$\{M \in \Gamma :\ M(K_1) \cap K_2 \neq \emptyset\}$$

is finite.

2.2 The Modular Group

In this section we give a brief explanation of the classical modular group and some of its properties. We give more detailed results for the Hilbert modular groups later in this paper.

Definition 2.7. The *classic modular group* of $\mathbb{Q}$ is

$$\mathrm{PSL}_2(\mathbb{Z}) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{Z}, ad - bc = 1 \right\} / \{E, -E\}.$$

Remark. The group $\mathrm{PSL}_2(\mathbb{Z})$ is a discrete subgroup of $\mathrm{PSL}_2(\mathbb{R})$ that is a topological group with discrete topology.

For the rest of this section we define the special matrices of $\mathrm{PSL}_2(\mathbb{Z})$:

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \; T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Definition 2.8. Given an action of a group G on a topological space Y by homeomorphisms, a *fundamental domain* for this action is a set D of representatives for the orbits.

Theorem 2.9 ([Ser73], Chapter VII §1.2)**.** *Let D be the subset of $\mathfrak{H}$ such that*

$$D = \left\{ z : \; |z| \geq 1, \; |\Re(z)| \leq \frac{1}{2} \right\}.$$

Then D is a fundamental domain for the action of the classic modular group on $\mathfrak{H}$. In other words,

(1) *For every* $z \in \mathfrak{H}$*, there exists some* $M \in \mathrm{PSL}_2(\mathbb{Z})$ *such that* $Mz \in D$*.*

(2) *Suppose that two distinct points* $z_1, z_2 \in D$ *are congruent modulo* $\mathrm{PSL}_2(\mathbb{Z})$*. Then* $\Re(z_1) = \pm\frac{1}{2}$ *and* $z_1 = z_2 \pm 1$*, or* $|z_1| = 1$ *and* $z_2 = -\frac{1}{z_1}$*.*

(3) *Let* $z \in D$ *and let* $I(z)$ *be the stabilizer of* z *in* $\mathrm{PSL}_2(\mathbb{Z})$*. We have* $I(z) = \{1\}$ *except in the following 3 cases:*

(a) $z = i$*, in which case* $I(z) = \langle S \rangle$*;*

(b) $z = \rho = e^{2\pi i/3}$*, in which case* $I(z) = \langle ST \rangle$*;*

(c) $z = -\bar{\rho} = e^{\pi i/3}$*, in which case* $I(z) = \langle TS \rangle$*.*

Proof. We prove statement 1 by showing that for any $z \in \mathfrak{H}$ there exists $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{PSL}_2(\mathbb{Z})$ such that $Mz \in D$. We know that

$$\Im Mz = \frac{\Im z}{|cz + d|^2}.$$

Since c and d are integers, the pairs (c, d) such that $|cz + d|$ is less than a given number is finite. Thus, there exists $M' \in \mathrm{PSL}_2(\mathbb{Z})$ such that $\Im(M'z)$ is maximal. Now choose an integer m such that $T^m M'z$ has real part between $-\frac{1}{2}$ and $\frac{1}{2}$. Thus, $z' = T^m M'z \in D$ since if $|z'| < 1$, then $Sz' = -\frac{1}{z'}$ would have an imaginary part larger than z' which is impossible since we chose the (c, d) such that the imaginary part of z' is maximal.

For statements 2 and 3, let $z \in D$ and let $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ such that $Mz \in D$. We can replace the pair (M, z) with (M^{-1}, Mz), so without loss of generality, suppose that $\Im(Mz) \geq \Im(z)$. Then $|cz + d| \leq 1$, leaving only the cases $c = 0, 1, -1$. If $c = 0$, then d must be ± 1. Then M is a translation by $\pm b$, and since both $\Re(Mz)$ and $\Re(z)$ are between $-\frac{1}{2}$ and $\frac{1}{2}$, b must be 0 or ± 1.

If $c = 1$, then $|z+d| \leq 1$ means that $d = 0$ except for the case $z = \rho$ (or $-\bar{\rho}$) where we have $d = 0, \pm 1$. The case $d = 0$ gives us $|z| \leq 1$, thus $|z| = 1$. Also, this means that $b = -1$, so $Mz = a - \frac{1}{z}$. Thus a must be 0 unless $z = \rho$ (or $-\bar{\rho}$) in which case we have $a = 0, \pm 1$. The case $z = \rho, d = 1$ gives $a - b = 1$ and $M\rho = a - 1/(1+\rho) = a + \rho$, thus $a = 0, 1$. Similarly when $z = -\bar{\rho}, d = -1$. Finally, the case that $c = -1$ is equivalent to the case where $c = 1$ since $M \in \mathrm{PSL}_2(\mathbb{Z})$ implies that $M = (-E)M$ with respect to the action on $\mathfrak{H}$, where $E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Therefore, statements 2 and 3 are true. □

Theorem 2.10 ([Ser73], Chapter VII §1.2)**.** $\mathrm{PSL}_2(\mathbb{Z})$ *is generated by* S *and* T*.*

Serre gives a proof of this lemma based on the previous Theorem 2.9 for the fundamental domain of $\mathrm{SL}_2(\mathbb{Z})$, but we will not cover the proof here since it can be similarly proven with the same technique as the more difficult proof of Theorem 5.1, as $\mathbb{Z}$ is Euclidean.

CHAPTER III

TOTALLY REAL NUMBER FIELDS

3.1 Definitions and Theorems

Definition 3.1. A *number field* is a finite degree (and hence algebraic) field extension of the field of rational numbers, $\mathbb{Q}$.

Let K be a totally real number field of degree $n = [K : \mathbb{Q}]$. Then K has n different embeddings into $\mathbb{R}$ (since K is totally real):

$$\begin{aligned} K &\to \mathbb{R}, \quad 1 \leq i \leq n \\ a &\mapsto a^{(i)}, \end{aligned}$$

where $a^{(i)}$ is the i^{th} embedding of a. We will combine these embeddings together in a single mapping

$$\begin{aligned} K &\to \mathbb{R}^n. \\ a &\mapsto (a^{(1)}, a^{(2)}, \ldots, a^{(n)}). \end{aligned}$$

We use a and the n-tuple $(a^{(1)}, a^{(2)}, \ldots, a^{(n)})$ interchangeably.

Remark. Throughout this paper we give information for the general case of any totally real number field K as well as more specific information for the real quadratic field $K = \mathbb{Q}(\sqrt{d})$, where $d > 0$ is squarefree. From here on we consider K to be a general real number field unless otherwise specified.

A quadratic field is an algebraic number field of degree two. It is easily shown that there is a bijection between the set of all quadratic fields and the set of all square free integers $d \neq 0$.

Let d be a positive and square free integer, and let $K = \mathbb{Q}(\sqrt{d})$. The field K can be written as a vector space of degree two over $\mathbb{Q}$, hence $K = \mathbb{Q} + \mathbb{Q}\sqrt{d}$. The *discriminant* of K is d if $d \equiv 1 \mod 4$, and $4d$ otherwise.

Definition 3.2. Let $\alpha = a + b\sqrt{d} \in K$, where $a,\ b \in \mathbb{Q}$. The *conjugate* of α, denoted α', is

$$\alpha' = a - b\sqrt{d}$$

Let $\alpha \in K = \mathbb{Q}(\sqrt{d})$. In this case, the embedding of K into $\mathbb{R}^2$ is given by

$$\alpha \mapsto (\alpha^{(1)}, \alpha^{(2)}) = (\alpha, \alpha').$$

Definition 3.3. Let $\alpha \in K = \mathbb{Q}(\sqrt{d})$. We define the *trace* of α as

$$\mathrm{tr}_K(\alpha) = \alpha + \alpha',$$

and the *norm* of α as

$$\mathrm{N}_K(\alpha) = \alpha\alpha'.$$

Definition 3.4. The *units* of a ring R are all elements $\alpha \in K$ such that there exists an element $\beta \in R$ where $\alpha\beta = \beta\alpha = 1$.

Definition 3.5. An element $\alpha \in K$ is called an *integer of* K when α is the root to a polynomial

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$$

where $a_1, \ldots, a_{n-1}$ are elements of $\mathbb{Z}$ and α satisfies no similar equation of degree less than n. Equivalently, in the quadratic case, $\alpha \in K$ is an integer when its trace and norm are elements of $\mathbb{Z}$.

Definition 3.6. An *order* is a subring $\mathcal{O}$ of K such that

(1) $\mathcal{O}$ spans K over $\mathbb{Q}$, so that $\mathbb{Q}\mathcal{O} = K$, and

(2) $\mathcal{O}$ is a $\mathbb{Z}$-lattice in K.

Definition 3.7. The *ring of integers*, also known as the *maximal order*, of K is the subring of all integers of K. We denote the ring of integers of K as $\mathcal{O}_K$ (or $\mathcal{O}_d$ in the quadratic case).

The ring of integers, $\mathcal{O}_K$, can be represented as a ring of degree $n = [K : \mathbb{Q}]$ over $\mathbb{Z}$, and $\mathcal{O}_K$ takes the form $\mathbb{Z} + \mathbb{Z}\omega_1 + \ldots + \mathbb{Z}\omega_{n-1}$ where $1, \omega_1, \ldots, \omega_{n-1} \in \mathcal{O}_K$ is an integral basis of $\mathcal{O}_K$.
For the quadratic case, $\mathcal{O}_d$ takes the form $\mathbb{Z} + \mathbb{Z}\omega$ where

$$\omega = \begin{cases} \frac{1+\sqrt{d}}{2} & \text{if } d \equiv 1 \mod 4 \\ \\ \sqrt{d} & \text{otherwise.} \end{cases}$$

From definition 3.2, it follows that if $\alpha = a + b\omega \in \mathcal{O}_d$ with $a,\ b \in \mathbb{Z}$, the conjugate α' is

$$\alpha' = \begin{cases} a + b\frac{1-\sqrt{d}}{2} & \text{if } d \equiv 1 \mod 4 \\ \\ a - b\sqrt{d} & \text{otherwise.} \end{cases}$$

Theorem 3.8 (Dirichlet Unit Theorem)**.** *Let K be a number field with r_1 real embeddings and $2r_2$ pairs of complex conjugate embeddings. The unit group of K is generated with $r_1 + r_2 - 1$ independent generators of infinite order. Moreover, where $r = r_1 + r_2 - 1$, any order $\mathcal{O}$ in K contains multiplicatively independent units $\epsilon_1, \epsilon_2, \ldots, \epsilon_r$ of infinite order such that every unit in $\mathcal{O}$ can be uniquely written as*

$$\zeta \cdot \epsilon_1^{m_1} \cdot \epsilon_2^{m_2} \cdots \epsilon_r^{m_r}$$

where ζ is a root of unity in $\mathcal{O}$ and $m_i \in \mathbb{Z}$, $1 \leq i \leq r$. So

$$\mathcal{O}^\times \cong \mu(\mathcal{O}) \times \mathbb{Z}^{r_1+r_2-1}$$

where $\mu(\mathcal{O})$ is the finite cyclic group of roots of unity in $\mathcal{O}$.

The *unit group of* $\mathcal{O}_K$, denoted $\mathcal{O}_K^\times$, takes the form

$$\mathcal{O}_K^\times = \{(-1)^{m_0}\epsilon_1^{m_1} \cdots \epsilon_n^{m_n} :\ m_0, m_1, \ldots, m_n \in \mathbb{Z}\},$$

where $\epsilon_1, \epsilon_2, \ldots, \epsilon_n \in \mathcal{O}_K$ are units of $\mathcal{O}_K$.

For the quadratic case, we can give a more specific definition for the unit group and fundamental unit (in the quadratic case there exists only one generator of the unit group $\mathcal{O}_d^\times$).

Theorem 3.9. *Let $K = \mathbb{Q}(\sqrt{d})$ be a real quadratic field and D its discriminant. Then the unit group $\mathcal{O}_d^\times$ of the maximal order $\mathcal{O}_d$ of K is*

$$\mathcal{O}_d^\times = \langle -1, \epsilon \rangle = \{-1^a \cdot \epsilon^b : \ a \in \mathbb{Z}, \ b \in \mathbb{Z}\}$$

where $\epsilon = \frac{a+b\sqrt{D}}{2}$ and (a, b) is the smallest solution to (with respect to ϵ)

$$a^2 - Db^2 = \pm 4.$$

The element ϵ is called the fundamental unit of K.

3.2 Dedekind Domains

In this section, we give important definitions and results for Dedekind domains. These are important because $\mathcal{O}_K$ is a Dedekind domain, and taking advantage of these results makes calculations much easier in later chapters.

Definition 3.10. A *Noetherian ring* is a ring in which every non-empty set of ideal has a maximal element.

A ring is Noetherian if the ascending chain condition on ideals holds, which means, given any ideal chain:

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$$

there exist an $N \in \mathbb{N}$ such that, for all $n \geq N$, $n \in \mathbb{N}$,

$$I_n = I_N.$$

There are some useful results based on Noetherian rings that we may need.

Definition 3.11. We say that an ideal I is a *primary ideal* if whenever $\mathfrak{ab} \in I$, then either $\mathfrak{a} \in I$ or $\mathfrak{b}^m \in I$ for some $m > 0$.

Theorem 3.12 (Lasker-Noether Theorem)**.** *Let R be a Noetherian ring, then every ideal of R can be expressed as a an intersection of finitely many primary ideals.*

Definition 3.13. A *Dedekind domain* R is an integral domain satisfying

(1) R is a Noetherian ring.

(2) R is integrally closed.

(3) Every nonzero prime ideal of R is maximal.

Proposition 3.14. *Let I be a non-zero ideal in the ring of integers $\mathcal{O}_K$. Then I is a free $\mathbb{Z}$-module of rank n and generated by a $\mathbb{Q}$-basis for K.*

Theorem 3.15. *Let R be an integral domain, and let S be an integral domain that contains R. Let I be an ideal of S, and suppose I contains a non-zero element α satisfying a non-zero polynomial $f(x) \in R[x]$. Then $I \cap R \neq 0$.*

Proof. Because S is an integral domain, we may factor out any powers of x dividing $f(x)$, and can therefore assume that $f(0) \neq 0$, but

$$\alpha \mid (f(\alpha) - f(0)).$$

Thus $-f(0) = f(\alpha) - f(0) \in I \cap R$, as desired.

□

Corollary 3.16. *Let I be a non-zero ideal in a ring of integers $\mathcal{O}_K$. Then, $\mathcal{O}_K/I$ is finite.*

Proof. Suppose that I contains some non-zero integer $m \in \mathbb{Z}$. Then $\mathcal{O}_K/I$ is a quotient of $\mathcal{O}_K/(m)$, which is isomorphic as a $\mathbb{Z}$-module to $(\mathbb{Z}/m\mathbb{Z})^2$, hence both are finite. □

Definition 3.17. Let I be a non zero ideal in $\mathcal{O}_K$. The *norm* of I is defined by

$$N(I) := |\mathcal{O}_K/I|.$$

Theorem 3.18. *The ring of integers, $\mathcal{O}_K$, is a Dedekind domain. Thus, $\mathcal{O}_K$ satisfies*

(1) *$\mathcal{O}_K$ is a Noetherian ring.*

(2) *$\mathcal{O}_K$ is integrally closed.*

(3) *Every nonzero prime ideal of $\mathcal{O}_K$ is maximal.*

Lemma 3.19. *Let R be a Dedekind domain, and let a be a non-zero element in an ideal $I \subseteq R$. Then there is an element $b \in R$ such that $I = (a, b)$. In particular, every ideal in R can be generated by two or less elements.*

3.3 Class Groups

Definition 3.20. Let K be a number field and R a ring such that $R \subset K$, we say that an ideal $\mathfrak{a}$ of K is a *fractional ideal* of K if there exists an element $b \in R$ such

that

$$b\mathfrak{a} = \{bx : \ x \in \mathfrak{a}\}$$

is an ideal in R. To distinguish ideals and fractional ideals, we also call the ideals of the maximal order of K *integral ideals*.

Let K be a number field, let I_K the group of fractional ideals, and let H_K its subgroup of principal fractional ideals. Then the quotient $Cl_K := I_K/H_K$ is called the *class group* of K. The class group is a finite abelian multiplicative group, and the cardinality of this group is the *class number* of K.

Definition 3.21. Let $\mathfrak{a} \in I_K$ be a fractional ideal, and let $\mathcal{O}_K$ be the maximal order of K. Then we define

$$\mathfrak{a}^{-1} := \{b \in K \mid b\mathfrak{a} \subseteq \mathcal{O}_K\}.$$

So, $\mathfrak{a}\mathfrak{a}^{-1} = \mathcal{O}_K$

Definition 3.22. Let K be a number field. Let $\mathfrak{m}_0 \in I_K$ be an integral ideal and $\mathfrak{m}_\infty$ a formal product of real infinite places of K. Then $\mathfrak{m} := \mathfrak{m}_0\mathfrak{m}_\infty$ is called a *congruence module*.

For the next definition, we say $v_\mathfrak{p}(\alpha) = m$ if $\alpha \in \mathfrak{p}^m$ $(\mathfrak{p}^m|\alpha)$ and $\alpha \notin \mathfrak{p}^{m-1}$ $(\mathfrak{p}^{m-1} \nmid \alpha)$ where $\mathfrak{p}$ is a prime ideal.

Definition 3.23. Let $\alpha^{(i)} \in \mathbb{C}$ be the ith embedding of $\alpha \in K$. *Multiplicative congruences* with respect to a finite place contained in the congruence module are

defined by

$$\alpha \equiv 1 \bmod^{\times} \mathfrak{p}^m \text{ if and only if } v_{\mathfrak{p}}(\alpha - 1) \geq m$$

and for a real infinite place $\mathfrak{p}_\infty^{(i)}$, which is the i^{th} embedding of $\mathfrak{p}_\infty$ into $\mathbb{R}$, by

$$\alpha \equiv 1 \bmod^{\times} (\mathfrak{p}_\infty^{(i)})^m \text{ if and only if } \alpha^{(i)} > 0.$$

Definition 3.24. Let $I^{\mathfrak{m}} := \{\mathfrak{a} \in I_K : \gcd(\mathfrak{a}, \mathfrak{m}_0) = 1\}$ and $H_{\mathfrak{m}} := \{(\alpha) \in H_K \mid a \equiv 1 \bmod^{\times} \mathfrak{m}\}$. Then the *ray class group* modulo $\mathfrak{m}$ is defined as

$$Cl_{\mathfrak{m}} := I^{\mathfrak{m}}/H_{\mathfrak{m}}.$$

CHAPTER IV

HILBERT MODULAR GROUPS

4.1 Hilbert Modular Groups

Extending §3.1, we define an embedding $\mathrm{GL}_2(K) \to \mathrm{GL}(\mathbb{R})^n$ by:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = M \mapsto (M^{(1)}, M^{(2)}, \ldots, M^{(n)}), \quad \text{where } M^{(i)} = \begin{pmatrix} a^{(i)} & b^{(i)} \\ c^{(i)} & d^{(i)} \end{pmatrix}, \ 1 \leq i \leq n.$$

We use M and the n-tuple image of its embedding into $\mathrm{GL}_2(\mathbb{R})^n$ interchangeably.

Definition 4.1. The *Hilbert modular group* of K is

$$\Gamma_K = \mathrm{PSL}_2(\mathcal{O}_K) = \mathrm{SL}_2(\mathcal{O}_K)/\{\pm E\}.$$

The Hilbert modular group acts on $\mathfrak{H}^n$, the product of n copies of the upper half plane. For $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{PSL}_2(\mathcal{O}_K)$ and $z = (z_1, \ldots, z_n) \in \mathfrak{H}^n$,

$$Mz = M(z_1, \ldots, z_n) = (M^{(1)}z_1, \ldots, M^{(n)}z_n) = \left(\frac{a^{(1)}z_1 + b^{(1)}}{c^{(1)}z_1 + d^{(1)}}, \ldots, \frac{a^{(n)}z_n + b^{(n)}}{c^{(n)}z_n + d^{(n)}} \right),$$

This gives us a well defined action of Γ_K on $\mathfrak{H}^n$.

4.2 Fixed Points

Definition 4.2. Let $M \in \mathrm{PSL}_2(\mathcal{O}_K)$. We say that a point $z \in \mathfrak{H}^n$ is a *fixed point* of M when $Mz = z$.

Definition 4.3. Let $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{PSL}_2(\mathbb{R})$. We say

(1) M is *elliptic* if $|a+d| < 2$.

(2) M is *parabolic* if $|a+d| = 2$.

Similarly, we say $M \in \mathrm{PSL}_2(\mathcal{O}_K)$ is elliptic or parabolic if each embedding of M is elliptic or parabolic, respectively.

Lemma 4.4. *An element of* $\mathrm{PSL}_2(\mathcal{O}_K)$ *has a fixed point if and only if it is elliptic.*

Proof. Suppose $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{PSL}_2(\mathcal{O}_K)$ has a fixed point $z \in \mathfrak{H}^n$. From here, we will prove for only the first embedding, each other embedding follows from this. We have

$$\frac{a^{(1)}z_1 + b^{(1)}}{c^{(1)}z_1 + d^{(1)}} = z_1,$$

which implies

$$0 = c^{(1)}z_1^2 + (d^{(1)} - a^{(1)})z_1 - b^{(1)}.$$

Using the quadratic formula, we have

$$z_1 = \frac{a^{(1)} - d^{(1)} \pm \sqrt{(d^{(1)} - a^{(1)})^2 + 4b^{(1)}c^{(1)}}}{2c^{(1)}} = \frac{a^{(1)} - d^{(1)} \pm \sqrt{(d^{(1)} + a^{(1)})^2 - 4}}{2c^{(1)}}.$$

Thus, applying this to each embedding, we can see that a matrix $M \in \mathrm{PSL}_2(\mathcal{O}_K)$ where $M \neq \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ has a fixed point if and only if it is elliptic. □

Definition 4.5. For $z \in \mathfrak{H}^n$, we define the isotropy subgroup of z in a subgroup $\Gamma \subset \mathrm{PSL}_2(\mathcal{O}_K)$ as

$$\Gamma_z := \{M \in \Gamma : \ Mz = z\}.$$

Definition 4.6. An element $z \in \mathfrak{H}^n$ is called an *elliptic fixed point* of a subgroup $\Gamma \subset \mathrm{PSL}_2(\mathcal{O}_K)$ if Γ_z is nontrivial.

Definition 4.7. A group Γ is said to *act discontinuously* at a point $z \in \mathfrak{H}^n$ if there exist a neighborhood U of z such that $MU \cap U \neq \emptyset$ for at most finitely many $M \in \Gamma$, where $MU = \{Mu : \ u \in U\}$.

Definition 4.8. A subgroup $\Gamma \subset \mathrm{PSL}_2(\mathcal{O}_K)$ is *discrete* if it acts discontinually on the upper half plane.

Proposition 4.9. *Let M be a matrix in $\mathrm{PSL}_2(\mathcal{O}_K)$. Then the following are equivalent:*

(1) *M is elliptic or $M = \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.*

(2) *M is of finite order.*

(3) *M has a fixed point in $\mathfrak{H}^n$.*

Proposition 4.10. *Let $\Gamma \subset \mathrm{PSL}_2(\mathcal{O}_K)$ be a discrete subgroup. Then the stabilizer of a point in $\mathfrak{H}^n$ is a finite cyclic group.*

The cardinality and number of these isotropy subgroups in $\Gamma \subset \mathrm{PSL}_2(\mathcal{O}_K)$ (up to conjugation) are necessary pieces of information for calculating invariants of the

Hilbert modular groups and the congruence subgroups. To find these, we plan to check in the embedding of the quotient of higher levels. We discuss this embedding and the permutation representation of it in more detail later in the following section.

4.3 Congruence Subgroups

Definition 4.11. Let $\mathfrak{n}$ be an ideal of $\mathcal{O}_K$. The subgroup

$$\Gamma_K(\mathfrak{n}) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{PSL}_2(\mathcal{O}_K) : \ a, d \equiv 1 \bmod \mathfrak{n}, \ b, c \equiv 0 \mod \mathfrak{n} \right\}$$

of $\mathrm{PSL}_2(\mathcal{O}_K)$ is called a *principal congruence subgroup* of level $\mathfrak{n}$ of $\mathrm{PSL}_2(\mathcal{O}_K)$.

Definition 4.12. A *congruence subgroup* of $\mathrm{PSL}_2(\mathcal{O}_K)$ is a group Γ such that it contains a principal congruence subgroup:

$$\Gamma_K(\mathfrak{n}) \leq \Gamma \leq \mathrm{PSL}_2(\mathcal{O}_K).$$

The next theorem is well known and important for making calculations on the congruence subgroups using a homomorphism to the quotient of the congruence subgroup by the principal congruence subgroup. This will be discussed in greater detail later in the section.

Theorem 4.13 (The Fourth Group Isomorphism Theorem)**.** *Let G be a group and let N be a normal subgroup in G. There is a bijection from the set of subgroups A of G that contain N onto the set of subgroups $\overline{A} = A/N$ of $\overline{G} = G/N$. In particular, every subgroup $\overline{G}$ is of the form A/N for some subgroup A of G containing N. This bijection has the following properties: For all subgroups A, $B \subseteq G$ with $N \subseteq A$ and $N \subseteq B$,*

(1) *$A \subseteq B$ if and only if $\overline{A} \subseteq \overline{B}$,*

(2) *if $A \subseteq B$, then $[B : A] = [\overline{B} : \overline{A}]$,*

(3) *$\overline{\langle A, B\rangle} = \langle \overline{A}, \overline{B}\rangle$, where $\langle A, B\rangle$ denotes the subgroup generated by A and B,*

(4) *$\overline{A \cap B} = \overline{A} \cap \overline{B}$,*

(5) *$A \trianglelefteq G$ if and only if $\overline{A} \trianglelefteq \overline{G}$.*

Lemma 4.14. *Let $\mathfrak{n}$ be an ideal of $\mathrm{PSL}_2(\mathcal{O}_K)$. The principal congruence subgroup $\Gamma_K(\mathfrak{n})$ is normal in $\mathrm{PSL}_2(\mathcal{O}_K)$.*

Proof. Let $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{PSL}_2(\mathcal{O}_K)$ and let $\begin{pmatrix} e & f \\ g & h \end{pmatrix} \in \Gamma_K(\mathfrak{n})$. Then

$$e, h \equiv 1 \bmod \mathfrak{n} \text{ and } g, f \equiv 0 \bmod \mathfrak{n}.$$

Using these properties we get

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} e & f \\ g & h \end{pmatrix} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$
$$= \begin{pmatrix} dae + dbg - caf - cbh & a^2 f + abh - bae - b^2 g \\ dce + d^2 g - c^2 f - cdh & acf + adh - bce - cdg \end{pmatrix}.$$

We can see that

$$dae + dbg - caf - cbh = 1 \bmod \mathfrak{n},$$
$$a^2 f + abh - bae - b^2 g = 0 \bmod \mathfrak{n},$$
$$dce + d^2 g - c^2 f - cdh = 0 \bmod \mathfrak{n},$$
$$acf + adh - bce - cdg = 1 \bmod \mathfrak{n}.$$

Hence, $\Gamma_d(\mathfrak{n}) \trianglelefteq \mathrm{PSL}_2(\mathcal{O}_K)$. □

Using Lemma 4.14 and the Fourth Isomorphism Theorem for Groups, we can investigate the congruent subgroups Γ as finite subgroups $\Gamma/\Gamma_K(\mathfrak{n})$.

For an integer $n \in \mathbb{N}$, we write $\Gamma_K(n)$ for $\Gamma_K((n))$, where $(n) = n(\mathcal{O}_K)$ is the principal ideal generated by n.

Proposition 4.15 ([Fre90, Remark 3.8, Corollary 3.9])**.** *If n is a rational integer greater than 2, the principal congruence subgroup $\Gamma_K(n)$ contains no trivial element of finite order.*

Proof. Let $E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Every nontrivial finite group Γ contains an element of prime order. Suppose, to the contrary, that there exist a prime $p \in \mathbb{N}$ and a matrix

$$M \in \Gamma_K(n) \text{ such that } M \neq E \text{ and } M^p = E.$$

Consider the matrix $B := M - E$ and let $\mathfrak{b}$ be the ideal generated by the coefficients of B. Since $M \in \Gamma_K(n)$, $\mathfrak{b}$ is contained in (n). Using the binomial theorem,

$$M^p = (B+E)^p = \sum_{k=0}^{p} \binom{p}{k} B^k E^{p-k} = E,$$

which gives us

$$\sum_{k=1}^{p} \binom{p}{k} B^k = 0_{2,2} \tag{4.1}$$

where $0_{2,2}$ is the zero matrix. Consider Equation (4.1) modulo $\mathfrak{b}^2$, we obtain

$$pB \equiv 0_{2,2} \bmod \mathfrak{b}^2.$$

Hence $p\mathfrak{b} \in \mathfrak{b}^2$ and, therefore,

$$p \in \mathfrak{b} \subset (n). \tag{4.2}$$

We know that for a prime p the binomial coefficients $\binom{p}{k}$, $1 \leq k \leq p-1$ are divisible by p. Therefore, for $k \geq 2$, $pB^k \equiv 0_{2,2} \bmod \mathfrak{b}^3$ and $pB^k \subseteq \mathfrak{b}^3$. Since $p \geq 3$ due to the number of terms in the binomial expansion, we know that the coefficients of B^p are in $\mathfrak{b}^3$ and therefore, by Equations (4.1) and (4.2), $pB \equiv 0_{2,2} \bmod \mathfrak{b}^3$, which implies that $p \in \mathfrak{b}^2 \subset (n^2)$. However, this is impossible since this would mean that n^2 divides the prime p, a contradiction. Therefore, $\Gamma_K(n)$ contains no element of finite order other than E. □

For now, we will restrict our work on congruence subgroups to the quadratic case. Let $\Gamma_d = \mathrm{PSL}_2(\mathcal{O}_d)$ and $n \in \mathbb{Z}$ with $n \geq 3$. For calculations on the congruence

subgroups of level n, we plan to use a permutation representation of the congruence subgroups of level $\mathfrak{n}$ in Γ_d.

The action of Γ_d on $\mathfrak{H}^2$ induces a permutation on the vectors $\mathcal{O}_d/(n)\times\mathcal{O}_d/(n)$. This permutation group is a subgroup of the symmetric group S_{m^2} where $m = |\mathcal{O}_d/(n)|$. To create this permutation representation, we use the action of the image of each generator of Γ_d in $\Gamma_d/\Gamma_d(n)$ on $\mathcal{O}_d/(n)\times\mathcal{O}_d/(n)$ as the generators of the permutation group.

4.4 Cusps of the Surface $\mathfrak{H}^n/\mathrm{PSL}_2(\mathcal{O}_K)$

To begin, we extend the action of $\mathrm{PSL}_2(\mathbb{R})^n$ to $\overline{\mathfrak{H}}^n$ where

$$\overline{\mathfrak{H}} = \mathfrak{H} \cup \mathbb{R} \cup \{\infty\}.$$

The action is the same Möbius transformation as before with the usual behavior with ∞: For any $a \in \mathbb{R}$,

(1) $\infty + a = \infty$,

(2) $\frac{\infty}{a} = \infty$, and

(3) $\frac{a}{\infty} = 0$.

Definition 4.16. The projective line of K, denoted $\mathbb{P}^1(K)$, is the extension of the usual line of K by a point at infinity.

Definition 4.17. The orbits of $\mathbb{P}^1(K)$ under a subgroup $\Gamma \subset \mathrm{PSL}_2(K)$ are called the *cusps* (or cusp class) of Γ respectively. We denote a representative of a cusp, σ, as

$$\sigma := (\alpha : \beta)$$

(where $(1 : 0)$ is called the cusp at infinity) which we will describe in the next proposition. We give this notation for a cusp, $(\alpha : \beta)$, with respect to its associiated ideal class (α, β) which we discuss next. A cusp (α, β), is an element of $\mathbb{P}^1(K)$ and we say $(\alpha, \beta) = (\gamma, \delta)$ if there exists and element $a \in K$ such that $a\alpha = \gamma$ and $a\beta = \delta$. For ease of understanding, we will refer to the cusps as defined as a *cusp class*, the equivalance class of cusps defined by the action of $\mathrm{PSL}_2(\mathcal{O}_K)$, and a representative of that class as a cusp from here on.

Definition 4.18. A matrix is said to be *unimodular* if it is a square integer matrix that is invertible over the integers.

Proposition 4.19 ([VDG88])**.** *The association*

$$(\alpha : \beta) \mapsto \ \textit{class of } (\alpha, \beta)$$

creates a bijective correspondence between the set of cusp classes of Γ_K *and the ideal class group* Cl_K *of* K*. In particular, the number of cusp classes of* Γ_K *is equal to the class number of* K*.*

Proof. Let σ and τ be cusps such that (where $\sim$ denotes equivalence of two elements of the same class)

$$\tau = \frac{a\sigma + b}{c\sigma + d} \sim \sigma.$$

Then the ideal class of τ can be represented by $(a\alpha+b\beta, c\alpha+d\beta) \sim (\alpha, \beta)$ since $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is unimodular.

Suppose that $\sigma = (\alpha : \beta)$ and $\tau = (\gamma : \delta)$ are two cusps associated with the same ideal class. With the multiplication by a suitable element of K, we assume that $(\alpha, \beta) = (\gamma, \delta) = \mathfrak{a}$. Then we know that there exist $\alpha^*, \beta^* \in \mathfrak{a}^{-1}$ such that $\alpha\beta^* + \beta\alpha^* = 1$ and, similarly, there exists $\gamma^*, \delta^* \in \mathfrak{a}^{-1}$ such that $\gamma\delta^* + \delta\gamma^* = 1$. Define the matrices

$$M_\sigma = \begin{pmatrix} \alpha & \alpha^* \\ \beta & \beta^* \end{pmatrix}, \quad M_\tau = \begin{pmatrix} \gamma & \gamma^* \\ \delta & \delta^* \end{pmatrix}.$$

Notice that these matrices have determinant 1 and transforms the cusp $\infty = (1 : 0)$ to their respective cusps:

$$M_\sigma(1:0) = (\alpha : \beta) \text{ and } M_\tau(1:0) = (\gamma : \delta).$$

We have

$$M_\sigma M_\tau^{-1} = \begin{pmatrix} \alpha & \alpha^* \\ \beta & \beta^* \end{pmatrix} \begin{pmatrix} \delta^* & -\gamma^* \\ -\delta & \gamma \end{pmatrix} = \begin{pmatrix} \alpha\delta^* - \alpha^*\delta & \alpha^*\gamma - \alpha\gamma^* \\ \beta\delta^* - \beta^*\delta & \beta^*\gamma - \beta\gamma^* \end{pmatrix}.$$

Hence, the matrix $M_\sigma M_\tau^{-1} \in \mathrm{PSL}_2(\mathcal{O}_K)$ and

$$M_\sigma M_\tau^{-1}\tau = M_\sigma(1:0) = \sigma.$$

Hence, $M_\sigma M_\tau^{-1}$ transforms τ to σ. Therefore, every ideal class is associated to a cusp class. □

Definition 4.20. The *set of multipliers* of $\mathcal{O}_K$, denoted by Λ, is the set of squares of units of $\mathcal{O}_K$:

$$\Lambda = \{a^2 : \ a \in \mathcal{O}_K^\times\}.$$

Definition 4.21. The *translation module* of a subgroup Γ of $\mathrm{PSL}_2(\mathbb{R})^n$ is the set of all $a \in \mathbb{R}^n$ such that there exist a matrix $M \in \Gamma$ where $Mz = z + a$ for all $z \in \mathfrak{H}^n$.

Definition 4.22. A subgroup of $\mathrm{PSL}_2(\mathbb{R})^n$ is said to *have a cusp* ∞ if its translation module is isomorphic to $\mathbb{Z}^n$ and its set of multipliers of $\mathcal{O}_K$, is isomorphic to $\mathbb{Z}^{n-1}$.

Corollary 4.23. $\mathrm{PSL}_2(\mathcal{O}_K)$ *has cusp* ∞.

Proof. We have that the translation module of $\mathrm{PSL}_2(\mathcal{O}_K)$ is $\mathcal{O}_K \cong \mathbb{Z}^n$. Also, by Theorem 3.9 and Theorem 3.8, we have

$$\mathcal{O}_K^\times \cong \mu(\mathcal{O}_K) \times \mathbb{Z} = \{+1, -1\} \times \mathbb{Z}^{n-1}.$$

Therefore, $\Lambda \cong \mathbb{Z}^{n-1}$, where Λ is the set of multipliers of $\mathcal{O}_K$. □

Proposition 4.24. *The set of all cusps of* Γ_K *is*

$$K \cup \{\infty\}.$$

Proof. We know that Γ_K has cusp ∞ by the previous proposition. We say that $\mathrm{PSL}_2(\mathcal{O}_K)$ has cusp $c = (\alpha : \beta)$ $(c \neq \infty)$ if there exist a matrix

$$A_c := \begin{pmatrix} \alpha & \alpha^* \\ \beta & \beta^* \end{pmatrix}$$

where $\alpha^*, \beta^* \in \mathfrak{c}^{-1}$, $\mathfrak{c} = (\alpha, \beta)$, such that the group

$$A_c^{-1}\Gamma_K A_c$$

has cusp ∞.

Now, let $c \in K$, then we can take the matrix

$$A_c = \begin{pmatrix} 0 & 1 \\ -1 & c \end{pmatrix}$$

which transforms c to ∞. Thus,

$$A_c^{-1}\Gamma_K A_c = \mathrm{PSL}_2(\mathcal{O}_K \oplus \mathfrak{c}^2),$$

where

$$\mathrm{PSL}_2(\mathcal{O}_K \oplus \mathfrak{a}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : \ a, d \in \mathcal{O}_K, b \in \mathfrak{a}^{-1}, c \in \mathfrak{a} \right\},$$

has cusp ∞. Thus Γ_K has cusp c. Therefore $K \cup \{\infty\}$ are cusps of Γ_K.

□

Remark. Every cusp of Γ_K is a fixed point of a parabolic element of Γ_K. From this we can see that there can exist no cusps outside of $K \cup \{\infty\}$ since, for a cusp k, there must exist

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

such that $a+d=2$ and $Mk=k$, which is only true for $k=\frac{a-d}{2c}\in K$.

Proposition 4.25. *Let $\mathfrak{m}$ be an ideal of K. The number of cusp classes of $\Gamma_K(\mathfrak{m})$ is the ray class number $h_\mathfrak{m}=\#Cl_\mathfrak{m}$.*

Proof. A cusp $\kappa\in K$ corresponds (Proposition 4.19) to the ideal $(\kappa,1)$.

We first show that equivalent cusps correspond to the same ideal class in $Cl_\mathfrak{m}$. Let $M=\begin{pmatrix}a & b\\ c & d\end{pmatrix}\in\Gamma_K(\mathfrak{m})$. We have

$$(\kappa,1)=((\kappa,1)\cdot M^t)=(a\kappa+b,c\kappa+d)$$

Set $\kappa'=M\kappa=\frac{a\kappa+b}{c\kappa+d}$. Since $M\in\Gamma_K(\mathfrak{m})$ we have $c\in\mathfrak{m}$ and $d\equiv 1 \bmod \mathfrak{m}$. Thus $(ck+d)\in H_\mathfrak{m}$ and therefore for the ideal classes we have

$$(\kappa,1)H_\mathfrak{m}=\left(\frac{a\kappa+b}{c\kappa+d},1\right)H_\mathfrak{m}.$$

If $(\kappa',1)$ and $(\kappa,1)$ are in the same ideal class in $Cl_\mathfrak{m}$ then there is $\alpha\in K$ such that

$$(\kappa',1)=\alpha(\kappa,1)=(\alpha\kappa,\alpha).$$

There are $a,b\in(\alpha\kappa,\alpha)^{-1}$ with $b\in\mathfrak{m}$ such that $a\alpha-\alpha\kappa b=1$. Let

$$
\begin{aligned}
M &= \begin{pmatrix} 1 & 0 \\ \kappa' & 1 \end{pmatrix}^{-1} \begin{pmatrix} a & b \\ \alpha\kappa & \alpha \end{pmatrix} \\
&= \begin{pmatrix} 1 & 0 \\ -\kappa' & 1 \end{pmatrix}^{-1} \begin{pmatrix} a & b \\ \alpha\kappa & \alpha \end{pmatrix} \\
&= \begin{pmatrix} a & b \\ -a\kappa' + \alpha\kappa & -b\kappa' + \alpha \end{pmatrix}.
\end{aligned}
$$

By construction, we have that $\det M = 1$. Also, by Lemma 3.21, we have $M \in \mathrm{SL}_2(\mathcal{O}_K)$. Thus $a = \frac{1}{\alpha} + b\kappa \in \mathcal{O}_K$. Since $\alpha \equiv 1 \bmod \mathfrak{m}$ and $b \in \mathfrak{m}$, we have $a \equiv 1 \bmod \mathfrak{m}$ and thus $M \in \Gamma_K(\mathfrak{m})$.

□

CHAPTER V

FUNDAMENTAL DOMAIN AND GENERATORS

5.1 Fundamental Domain and Known Generators

We begin by defining the common matrices for simplicity throughout this chapter. Our first two methods of finding generators require that K to be a real quadratic field. For $K = \mathbb{Q}(\sqrt{d})$, we define the matrices

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad \text{and} \quad U_\epsilon = \begin{pmatrix} \epsilon & 0 \\ 0 & \epsilon^{-1} \end{pmatrix},$$

where ϵ is the fundamental unit of $\mathcal{O}_d$. Also, for each $a \in K$, we define the matrix

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

Remark. These are natural relations that hold for these matrices:

$$S^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -E,$$

$$S^3 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = -S,$$

$$SU_\epsilon = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \epsilon & 0 \\ 0 & \epsilon^{-1} \end{pmatrix} = \begin{pmatrix} 0 & -\epsilon^{-1} \\ \epsilon & 0 \end{pmatrix},$$

$$S^3U_\epsilon = \begin{pmatrix} 0 & \epsilon^{-1} \\ -\epsilon & 0 \end{pmatrix},$$

$$SU_\epsilon S^3U_\epsilon = (SU_\epsilon)^4 = SU_\epsilon SU_\epsilon = E.$$

In [Deu86], Jesse Ira Deutsch states the next theorem for the generators of Euclidean $\mathcal{O}_d$. Instead of a proof, he gives aa example and says that it can be generalized. Thus, we have given our own proof for this below.

Theorem 5.1 ([Deu86])**.** *If $\mathcal{O}_d$ is Euclidean, then $\mathrm{PSL}_2(\mathcal{O}_d)$ is generated by S, T_1, T_ω, and U_ϵ.*

Proof. For a matrix of the form

$$\begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix} \in \mathrm{PSL}_2(\mathcal{O}_d),$$

where $\alpha \in \mathcal{O}_d$, let $\alpha = \alpha_1 + \alpha_2\omega$, $\alpha_1,\ \alpha_2 \in \mathbb{Z}$, then we have

$$T_\alpha = T_1^{\alpha_1} T_\omega^{\alpha_2} \tag{1.1}$$

Consider the basic case,

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \mathrm{PSL}_2(\mathcal{O}_d),$$

Then we have that $ad = 1$. So $a = \pm\epsilon^n$ and $d = a^{-1} = \pm\epsilon^{-n}$. Thus, where $b\epsilon^{-n} = z_1 + z_2\omega$, $z_1,\ z_2 \in \mathbb{Z}$, using (1.1),

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} \epsilon^n & \epsilon^n(z_1 + z_2\omega) \\ 0 & \epsilon^{-n} \end{pmatrix} = \begin{pmatrix} \epsilon^n & 0 \\ 0 & \epsilon^{-n} \end{pmatrix} \begin{pmatrix} 1 & z_1 + z_2\omega \\ 0 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} \epsilon & 0 \\ 0 & \epsilon^{-1} \end{pmatrix}^n \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{z_1} \begin{pmatrix} 1 & \omega \\ 0 & 1 \end{pmatrix}^{z_2} = U_\epsilon^n T_1^{z_1} T_\omega^{z_2}.$$

Now, for the general case, let $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be an arbitrary element of $\mathrm{PSL}_2(\mathcal{O}_d)$. Since $\mathcal{O}_d$ is a Euclidean domain, there exists a Euclidean algorithm for entries c and d:

$$\begin{aligned} c &= q_0 d + r_0 \\ d &= q_1 r_0 + r_1 \\ r_0 &= q_2 r_1 + r_2 \\ &\vdots \\ r_{n-2} &= q_n r_{n-1} + r_n \\ r_{n-1} &= q_{n+1} r_n, \end{aligned} \quad .$$

where $q_0, \ldots, q_{n+1},\ r_0, \ldots,\ r_n \in \mathcal{O}_d$

We can see that, multiplying by $-E$ as needed,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ q_0 d + r_0 & d \end{pmatrix} = \begin{pmatrix} b & bq_0 - a \\ d & -r_0 \end{pmatrix} \begin{pmatrix} 1 & -q_0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Also,

$$\begin{pmatrix} b & bq_0 - a \\ d & -r_0 \end{pmatrix} = \begin{pmatrix} -bq_0 + a & (bq_0 - a)q_1 + b \\ r_0 & r_1 \end{pmatrix} \begin{pmatrix} 1 & q_1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Thus, by application of this method by induction up to index $n+1$, as given in the Euclidean algorithm, we can see

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} -bq_0 + a & (bq_0 - a)q_1 + b \\ r_0 & r_1 \end{pmatrix} \begin{pmatrix} 1 & q_1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & -q_0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

$$= \ldots = \begin{pmatrix} \alpha & \beta \\ 0 & \pm r_n \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} 1 & q_1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & -q_0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Thus, we can apply the basic case to the matrix

$$\begin{pmatrix} \alpha & \beta \\ 0 & \pm r_n \end{pmatrix},$$

and we apply (1.1) to the matrices

$$\begin{pmatrix} 1 & \pm q_i \\ 0 & 1 \end{pmatrix}.$$

Therefore, $\mathrm{PSL}_2(\mathcal{O}_d)$ is generated by $S,\ T_1,\ T_\omega$, and U_ϵ.

□

In [Vas72], Vaserstein proves that, for any Dedekind domain of arithmetic type R with infinitely many invertible elements, $\mathrm{SL}_2(R)$ is generated by elementary matrices (in an algerbraic sense). In [May07], Sebastian Mayer gives the following lemma which is a special case of Vaserstein's Theorem.

Lemma 5.2 ([May07], Lemma 1.2.21, page 32)**.** *If* $d \equiv 1 \bmod 4$*, then* $\mathrm{PSL}_2(\mathcal{O}_d)$ *is generated by the set of matrices*

$$\left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} : \ a \in \mathcal{O}_d \right\} \cup \left\{ \begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix} : \ b \in \mathcal{O}_d \right\}.$$

Corollary 5.3. *If* $d \equiv 1 \bmod 4$*, then* $\mathrm{PSL}_2(\mathcal{O}_d)$ *is generated by the matrices* S*,* T_1 *and* T_ω*.*

Proof. It suffices to show that all upper and lower triangular matrices of Lemma 5.2 can be obtained with these matrices.

Let $a \in \mathcal{O}_d$, denote a as $a = a_1 + a_2\omega$ where $a_1,\ a_2 \in \mathbb{Z}$. Then

$$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} = T_1^{a_1} T_\omega^{a_2}.$$

Similarly, let $b \in \mathcal{O}_d$, write b as $b = b_1 + b_2\omega$ where $b_1,\ b_2 \in \mathbb{Z}$. Then

$$S^3 T_1^{-b_1} T_\omega^{-b_2} S = S^3 \begin{pmatrix} 1 & -b \\ 0 & 1 \end{pmatrix} S$$

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

□

5.2 Fundamental Domain and Generators of $\mathrm{PSL}(\mathcal{O}_K)$ in the General Case

In this section, we follow an arithmetical approach to computing the fundamental domain given by Tsueno Tamagawa. First we define some useful notations for $z = (z_1, \ldots, z_n) \in \mathbb{C}^n$:

The norm of z (Note that this particular definition does not behave the same as a typical norm):

$$Nz = z_1 \cdot \ldots \cdot z_n.$$

The trace of z:

$$Sz = z_1 + \ldots + z_n.$$

The absolute value of z:

$$|z| = (|z_1|, \ldots, |z_n|).$$

The real part of z:

$$\Re z = (\Re z_1, \ldots, \Re z_n).$$

The imaginary part of z:

$$\Im z = (\Im z_1, \ldots, \Im z_n).$$

Let V be a Euclidean vector space of dimension m, let (x, y) denote the inner product for $x, y \in V$, and let $\|x\| = (x, x)^{\frac{1}{2}}$ denote the magnitude of $x \in V$. A lattice Λ_V is a subgroup of V such that

$$\Lambda_V = \mathbb{Z}\alpha_1 + \mathbb{Z}\alpha_2 + \ldots + \mathbb{Z}\alpha_m$$

where $\alpha_1, \alpha_2, \ldots, \alpha_m$ is a set of linearly independent vectors. We use $\sqrt{|(\alpha_i, \alpha_j)|}$ to denote the determinant of Λ_V, which is the volume of a fundamental parallelotope of Λ_V.

Definition 5.4. We say that a vector $x \in V$ is Λ_V-*reduced* if $\|x + \alpha\| \geq \|x\|$ for all $\alpha \in \Lambda_V$. The set of all Λ_V-reduced vectors is denoted Π_{Λ_V}.

Lemma 5.5 ([Tam59], page 242)**.** *The set Π_{Λ_V} is a convex set defined by a finite number of inequalities of inner products*

$$\pm 2(x, \gamma_v) \leq (\gamma_v, \gamma_v) \qquad (v = 1, 2, \ldots, s)$$

where $\gamma_1, \gamma_2, \ldots, \gamma_s$ are suitable vectors in Λ_V, and Π_{Λ_V} is a fundamental domain of the translation group $\{x \mapsto x + \alpha : \alpha \in \Lambda_V, x \in V\}$. Furthermore, for a subspace $W \subset V$ with dimension equal to the rank of the subset $\{y \in \Lambda_V : \ Ny = 1\}$, the intersection $\Pi_{\Lambda_V} \cap W$ is compact and $x \in V$ is in Π_{Λ_V} if and only if $x = x_1 + x_2$ where $x_1 \in \Pi_{\Lambda_V} \cap W$, x_2 is an element of V, and x_2 is orthogonal to W.

Let

$$Y = \{y \in \mathbb{R}^n : \ y_1 > 0, \ldots, y_n > 0\}.$$

Let $Y_1 = \{y \in Y : \ Ny = 1\}$, and let $\log y = (\log y_1, \ldots, \log y_n)$ for $y = (y_1, \ldots, y_n)$.

Let $\Lambda_K = \{\log |u| : u \in K^\times\}$ where $K^\times$ is the group of units of K. Then Λ_K is a rank $n-1$ lattice in $\mathbb{R}^n$, and Λ_K spans the hyperplane $H = \{x : \ x \in K, Sx = 0\} \subset \mathbb{R}^n$.

Let $S_{\Lambda_K}(x, y)$ be a positive definite inner product on $\mathbb{R}^n$ for $x = (x_1, \ldots, x_n), \ y = (y_1, \ldots, y_n)$. Taking $\mathbb{R}^n$ as a Euclidean space with S_{Λ_K} as its inner product, a vector x is orthogonal to H if and only if x is a scalar multiple of $(1, \ldots, 1) \in \mathbb{R}^n$.

Definition 5.6. A vector $y \in Y$ is called *strongly reduced* if $\log y$ is Λ_K-reduced.

Let R be the set of all strongly reduced elements of Y, and let $R_1 = R \cap Y_1$. From the previous lemma, we have the following:

Lemma 5.7 ([Tam59], page 242)**.** *The set R is bounded by a finite number of analytic hypersurfaces in Y and R_1 is compact. For every $y \in Y$, there exist a unique $\varepsilon \in K^\times$ such that $|\varepsilon| y \in R$.*

Corollary 5.8 ([Tam59], page 243)**.** *If $(y_1, \ldots, y_n) \in R$, then there is a constant $c > 1$ that depends only on K such that for $1 \leq i \leq n$ we have*

$$c^{-1} N \sqrt[n]{y} \leq y_i \leq c N \sqrt[n]{y}.$$

Definition 5.9. We call $y \in Y$ *reduced* if $\sqrt{y} = \left(\sqrt{y_1}, \ldots, \sqrt{y_n}\right)$ is strongly reduced.

The set of all reduced $y \in \mathbb{R}^n$ is the set

$$R^2 = \{y^2 : \ y \in R\}.$$

By Lemma 5.7, for $y \in Y$, there is $\varepsilon \in K^\times$ such that $\varepsilon^2 y \in R^2$. Thus, if y is reduced, we have

$$\varepsilon^{-2} N \sqrt[n]{y} \leq y^{(1)}, \ldots, y^{(n)} \leq \varepsilon^2 N \sqrt[n]{y}.$$

Let $\mathfrak{a}$ be an ideal of $\mathcal{O}_K = \mathbb{Z} + \omega_1\mathbb{Z} + \ldots + \omega_{n-1}\mathbb{Z}$. Then $\mathfrak{a}$ is a rank n lattice of $\mathbb{R}^n$. Let

$$\Pi_\mathfrak{a} = \{x \in \mathbb{R}^n : \ S(x+\alpha)^2 \leq Sx^2 \text{ for all } \alpha \in \mathfrak{a}\}$$

be the set of all $\mathfrak{a}$-reduced vectors of $\mathbb{R}^n$ as defined in Definition 5.4. By Lemma 5.5, the set $\Pi_\mathfrak{a}$ is a compact and convex polyhedron that is symmetric with respect to 0, and for every $x \in \mathbb{R}^n$, there exist an element $\alpha \in \mathfrak{a}$ such that $x + \alpha \in \Pi_\mathfrak{a}$.

Let $A(\mathfrak{a})$ be the group of all affine transformations $z \to \varepsilon^2 z + \alpha$ with $\varepsilon \in \mathcal{O}_K^\times$ and $\alpha \in \mathfrak{a}$. The matrices that correspond to these transformations by the action of the Möbius transformation are of the form

$$\begin{pmatrix} \varepsilon & \beta \\ 0 & \varepsilon^{-1} \end{pmatrix}, \quad \beta = \varepsilon^{-1}\alpha.$$

We can see that if $\mathfrak{a} \subset \mathcal{O}_K$ then $A(\mathfrak{a})$ is a subgroup of Γ_K. For an element $z \in \mathfrak{H}^n$, we say that z is $\mathfrak{a}$-reduced if $\Im z = (\Im z_n, \ldots, \Im z_n)$ is reduced and $\Re z = (\Re z_1, \ldots, \Re z_n)$

is $\mathfrak{a}$-reduced. Take

$$G(\mathfrak{a}) = \{z \in \mathfrak{H}^n : \ z \text{ is } \mathfrak{a}\text{-reduced}\},$$

then we see that $G(\mathfrak{a})$ is a fundamental domain of $A(\mathfrak{a})$ and is bounded by finitely many analytic surfaces in $\mathfrak{H}^n$.

From here on we denote a pair of elements $\gamma, \delta \in K$ by $\langle \gamma, \delta \rangle$ to distinguish them from the embeddings defined in previous chapters.

Definition 5.10. Let $\langle \gamma, \delta \rangle$ be a non-zero pair of elements in K. We say that the pairs $\langle \gamma, \delta \rangle$ and $\langle \gamma^*, \delta^* \rangle$ are *associated* if there exists an element $\varepsilon \in \mathcal{O}_K^\times$ such that

$$\langle \varepsilon\gamma, \varepsilon\delta \rangle = \langle \gamma^*, \delta^* \rangle \quad (\varepsilon\gamma = \gamma^* \text{ and } \varepsilon\delta = \delta^*).$$

We say that two pairs of elements are *non-associated pairs* if no such $\varepsilon \in \mathcal{O}_K^\times$ exists.

Lemma 5.11 ([Tam59], page 243)**.** *Let $\mathfrak{a}$ and $\mathfrak{b}$ be ideals of $\mathcal{O}_K$ and let $z \in \mathfrak{H}^n$. For any constant $m > 0$, there exist only a finite number of non-associated pairs $\langle \gamma, \delta \rangle$ with $\gamma \in \mathfrak{a}$ and $\delta \in \mathfrak{b}$ such that*

$$N|\gamma z + \delta| < m,$$

where $\gamma z + \delta = (\gamma^{(1)} z_1 + \delta^{(1)}, \ldots, \gamma^{(n)} z_n + \delta^{(n)})$.

Proof. Let $\langle \gamma, \delta \rangle$ be a pair of elements where $\gamma \in \mathfrak{a}$ and $\delta \in \mathfrak{b}$. Choose $\varepsilon \in K^\times$ such that $|\varepsilon\gamma z + \varepsilon\delta|$ is strongly reduced. Let $\langle \varepsilon\gamma, \varepsilon\delta \rangle = \langle \gamma^*, \delta^* \rangle$. From Corollary 5.8, there

exists $c > 1$ where

$$|(\gamma^*)^{(1)} z_1 + (\delta^*)^{(1)}| < c\sqrt{m}, \ldots, |(\gamma^*)^{(n)} z_n + (\delta^*)^{(n)}| < c\sqrt{m}.$$

Since $z \in \mathfrak{H}^n$, $\Im z$ is positive ($\Im z_1, \ldots, \Im z_n > 0$, where $z = (z_1, \ldots, z_n) \in \mathfrak{H}^n$), then the set $\{\gamma z + \delta; \gamma \in \mathfrak{a}, \delta \in \mathfrak{b}\}$ is a lattice in $\mathbb{C}^n$ and the domain defined by

$$|z_1|, |z_2|, \ldots, |z_n| < c\sqrt{m}$$

is bounded. Thus there exist only finitely many pairs $\langle \gamma, \delta \rangle$ such that the inequality $N|\gamma z + \delta| < m$ is satisfied. □

Lemma 5.12 ([Tam59], page 243)**.** *Let $\mathfrak{a}$ be an ideal of $\mathcal{O}_K$. There exists a constant $c_1 > 0$, depending only on $\mathcal{O}_K$ such that for every $z \in \mathfrak{H}^n$ with $N(\Im z) < c_1$, there exists a pair $\langle \gamma, \delta \rangle$ where $\gamma \in \mathfrak{a}$ and $\delta \in \mathfrak{a}^{-1}$ such that*

$$N|\gamma z + \delta| < 1,$$

where $\gamma z + \delta = (\gamma^{(1)} z_1 + \delta^{(1)}, \ldots, \gamma^{(n)} z_n + \delta^{(n)})$.

Let $\mathfrak{a}_1, \ldots, \mathfrak{a}_h$ be a set or representatives of the ideal classes of K such that

(1) each $\mathfrak{a}_i$ is integral, and

(2) $\mathfrak{a}_i$ has minimum norm among integral ideals in its class.

We assume that $\mathfrak{a}_1$ represents the principle class, hence $\mathfrak{a}_1 = \mathcal{O}_K$.

Let F_i be the set of all $z \in \mathfrak{H}^n$ such that

(1) z is $\mathfrak{a}_i^{-2}$ reduced, and

(2) $N|\gamma z + \delta| \geq 1$ for all pairs $\langle \gamma, \delta \rangle$ with $\gamma \in \mathfrak{a}_i$ and $\delta \in \mathfrak{a}_i^{-1}$.

Lemma 5.13 ([Tam59], page 244)**.** *Let $\mathfrak{a}_i$ be the representative ideal of the i^{th} ideal class. There exist only a finite number of non-associated pairs $\langle \gamma, \delta \rangle$ with $\gamma \in \mathfrak{a}_i$ and $\delta \in \mathfrak{a}_i^{-1}$ such that $N|\gamma\tau + \delta| = 1$ for some $\tau \in F_i$*

From Lemma 5.13, we can see that the infinite number of inequalities defining F_i can be represented by a finite subset of inequalities among them. Thus, F_i is bounded by a finite number of analytic surfaces in $\mathfrak{H}^n$.

Let $\mathfrak{a}_i$ $(1 \leq i \leq h)$ be the representatives of the ideal classes of K. Let γ_i and δ_i be integers generating $\mathfrak{a}_i$. Then there exist $\alpha_i, \beta_i \in \mathfrak{a}_i^{-1}$ such that $\alpha_i\delta_i - \beta_i\gamma_i = 1$, which we show later in this chapter in Theorem 5.17. For $2 \leq i \leq h$ we denote by A_i the linear fractional transformation

$$z \to \frac{\alpha_i z + \beta_i z}{\gamma_i z + \delta_i}.$$

For $i = 1$ we set A_1 to the identity transformation I.

Theorem 5.14 ([Tam59], page 245)**.** *The set*

$$F_1 \cup A_2^{-1}F_2 \cup \ldots \cup A_h^{-1}F_h$$

is a fundamental domain of the group Γ_K.

Proof. Let $z \in \mathfrak{H}^n$. By Lemma 5.11 there exists a pair $\langle \gamma, \delta \rangle$, $\gamma, \delta \in \mathcal{O}_K$, such that $N|\gamma z + \delta| \leq N|\gamma^* z + \delta^*|$ for all $\gamma^* \in \mathcal{O}_K$ and $\delta^* \in \mathcal{O}_K$ such that $\langle \gamma^*, \delta^* \rangle \neq \langle 0, 0 \rangle$. We

have two cases for such pairs of integers:

Case 1: If $N|\gamma z+\delta| \geq 1$ we can find a unit $\varepsilon \in \mathcal{O}_K^{\times}$ and an integer $\alpha \in \mathcal{O}_K$ such that

$$\varepsilon^2 z + \alpha \in G(\mathcal{O}_K).$$

Then $z^* = \varepsilon^2 z + \alpha$ is equivalent to z with respect to Γ_K and z^* is a point of the set F_1.

Case 2: If $N|\gamma z + \delta| < 1$ let $\mathfrak{a}$ be the ideal generated by γ and δ and $\mathfrak{a}_i$ the representative of its class. Then there exists an element $\kappa \in \mathfrak{a}_i^{-1}$ such that $\mathfrak{a} = \kappa\mathfrak{a}_i$, so $\kappa^{-1}(\gamma, \delta) = \mathfrak{a}_i$. So we have that $\kappa^{-1}\gamma, \kappa^{-1}\delta \in \mathfrak{a}_i$ and

$$N|\kappa^{-1}\gamma z + \kappa^{-1}\delta| = N|\kappa|^{-1} N|\gamma z + \delta|.$$

With the assumption on γ and δ, we have that $N|\kappa| \leq 1$. On the other hand, from the assumption on $\mathfrak{a}_i$ we have that $N|\kappa| \geq 1$. Hence $N|\kappa| = 1$.

Let M be a matrix such that

$$\langle \gamma_i, \delta_i \rangle = \langle \gamma, \delta \rangle M = \langle \kappa^{-1}\gamma, \kappa^{-1}\delta \rangle,$$

where γ_i and δ_i are the generators of the representative class $\mathfrak{a}_i$. We have

$$N|\gamma_i M z + \delta_i| \leq N|\gamma^* M z + \delta^*|$$

for every pair $\langle \gamma^*, \delta^* \rangle$. For every $\langle \mu, \nu \rangle$ such that $\mu \in \mathfrak{a}_i$ and $\nu \in \mathfrak{a}_i^{-1}$, we have

$$\begin{aligned} \mu A_i Mz + \nu &= (\mu(\alpha_i Mz + \beta_i) + \nu(\gamma_i Mz + \delta_i))(\gamma_i Mz + \delta_i)^{-1} \\ &= (\mu^* Mz + \nu^*)(\gamma_i Mz + \delta_i)^{-1}, \end{aligned}$$

where $\mu^* = \alpha_i \mu + \gamma_i \nu \in \mathcal{O}_K$ and $\nu^* = \beta_i \mu + \delta_i \nu \in \mathcal{O}_K$. Thus, we have

$$N|\mu A_i Mz + \nu| \geq 1. \tag{5.1}$$

Let L be a transformation in $A(\mathfrak{a}_i^{-2})$ such that $LA_i Mz \in G(\mathfrak{a}_i^{-2})$. Then $LA_i Mz \in F_i$, hence $A_i^{-1} LA_i Mz \in A_i^{-1} F_i$. Since $A_i^{-1} A(\mathfrak{a}_i^{-2}) A_i \subset \Gamma_K$, we have

$$A_i^{-1} A(\mathfrak{a}_i^{-2}) A_i M \in \Gamma_K.$$

□

Remark. For this previous proof of Tamagawa's theorem, we excluded the part that shows uniqueness up to the boundaries of $A_i^{-1} F_i$. The complete proof is given in Tamagawa's work.

We now use Tamagawa's proof of Theorem 5.14 to construct a set of generators for a generic group Γ_K.

Theorem 5.15. *Let h be the class number of K and $n = [K : \mathbb{Q}]$. Let $\{\gamma_i, \delta_i\}$ be a set of generators for the ideal $\mathfrak{a}_i$, and let $\{\hat{\gamma}_i, \hat{\delta}_i\}$ be the set of generators for $\mathfrak{a}_i^{-2}$ where $1 \leq i \leq h$. Let $\epsilon_1, \epsilon_2, \ldots \epsilon_n$ be the generators of the unit group of $\mathcal{O}_K$ and let*

$1, \omega_1, \ldots, \omega_{n-1}$ *be the basis of* $\mathcal{O}_K$*. Let* $\mathcal{L}$ *be the subset of* $\mathcal{O}_K$ *defined as*

$$\mathcal{L} = \bigcup_{1 \le i \le h} \left\{ A_i^{-1} U_{\epsilon_1} A_i, \ldots, A_i^{-1} U_{\epsilon_n} A_i,\ A_i^{-1} T_{\hat{\gamma}_i} A_i,\ A_i^{-1} T_{\hat{\delta}_i} A_i \right\}.$$

Then the subset of Γ_K*,*

$$\mathcal{L} \cup \{S, T_1, T_{\omega_1}, \ldots, T_{\omega_{n-1}}, U_{\epsilon_1}, \ldots, U_{\epsilon_n}\},$$

generates Γ_K*.*

Proof. As we have seen in Theorem 5.14, for any element $z \in \mathfrak{H}$, we can be transformed to an element of $F_1 \cup A_2^{-1} F_2 \cup \ldots \cup A_h^{-1} F_h$. For any $z \in \mathfrak{H}$, we take the pair $\langle \gamma, \delta \rangle \in \mathcal{O}_K \times \mathcal{O}_K$ such that $|z\gamma + \delta|$ has the smallest norm. If $N|z\gamma + \delta| \ge 1$ as in case 1, then we can construct the transformation $z \mapsto \varepsilon^2 z + \alpha$ given in Tamigawa's proof using the set

$$\{T_1, T_{\omega_1}, \ldots, T_{\omega_{n-1}}, U_{\epsilon_1}, \ldots, U_{\epsilon_n}\} \subset \mathrm{PSL}_2(\mathcal{O}_K).$$

For this, we set $b = \varepsilon^{-2}\alpha$. Using $\{T_1, T_{\omega_1}, \ldots, T_{\omega_{n-1}}\}$ we construct $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$, and using $\{U_{\epsilon_1}, \ldots, U_{\epsilon_n}\}$ we construct $\begin{pmatrix} \varepsilon & 0 \\ 0 & \varepsilon \end{pmatrix}$. Then we have the transformation

$$\begin{pmatrix} \varepsilon & 0 \\ 0 & \varepsilon \end{pmatrix} \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} z = \begin{pmatrix} \varepsilon & 0 \\ 0 & \varepsilon \end{pmatrix} (z + b) = \varepsilon^2 z + \varepsilon^2 b = \varepsilon^2 z + \alpha$$

For the case where $N|z\gamma + \delta| < 1$, the matrix M from Tamagawa's proof is equal to $E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ unless z lies on the boundary of the fundamental domain, otherwise it gives a unit k such that

$$\langle \gamma, \delta \rangle M = \langle k^{-1}\gamma, k^{-1}\delta \rangle.$$

Thus M can be constructed using the set $\{U_{\epsilon_1}, \ldots, U_{\epsilon_n}, S\}$. We use the defined set $\mathcal{L}$ in our theorem to construct the transformation $A_i^{-1} L A_i \in \mathrm{PSL}_2(\mathcal{O}_K)$ where $LA_i \in A(\mathfrak{a}^{-2})$ and $\mathfrak{a}_i$ is the representative if the ideal class of (γ, δ). This gives us the transformation $A_i^{-1} L A_i M z \in A_i^{-1} F_i$. □

5.3 Computation

Currently for this section, we focus only on the quadratic case. We plan to extend this application to higher degree number fields in the future. To compute the matrices A_i, we will use an algorithm comparable to that of Algorithm 1.3.2 in [Coh00].

Algorithm 5.16 ([Coh00], §1.3 page 17)**.** *Let R be a Dedekind domain.*

Input: *Two coprime ideals $\mathfrak{a}$ and $\mathfrak{b}$ given by their HNF matrices A and B on the integral basis of R.*

Output: *$a \in \mathfrak{a}$ and $b \in \mathfrak{b}$ such that $a + b = 1$.*

1. *Let C be the $2n \times n$ matrix obtained by concatenating A and B, denoted $(A|B)$. Using HNF reduction, Compute an HNF matrix H and $2n \times 2n$ matrix L such that $LC = (H|0)$.*

2. *Set X be the n-component column vector formed by the first n entries of the first row of of the resulting matrix LC.*

3. Let a be the element of K whose coordinate vector on the integral basis is X^tA, and set b to the value $1-a$. Output a and b.

Theorem 5.17 ([Coh00], §1.3 page 18)**.** *Let $\mathfrak{a}$ and $\mathfrak{b}$ be two (fractional) ideals in R, an integer ring of a Dedekind domain K. Let a and b be two elements of K and set $\mathfrak{o} = a\mathfrak{a} + b\mathfrak{b}$. There exist $u \in \mathfrak{a}\mathfrak{o}^{-1}$ and $v \in \mathfrak{b}\mathfrak{o}^{-1}$ such that $au + bv = 1$ and these elements are found in polynomial time.*

Proof. If a is equal to zero, we can take $u = 0$ and $v = 1/b$, since we have

$$1/b \in \mathfrak{b}\mathfrak{o}^{-1} = R/b.$$

Similarly, we can find u and v where a is zero.

Assuming that both a and b are non-zero, set $I = a\mathfrak{a}\mathfrak{o}^{-1}$ and $J = b\mathfrak{b}\mathfrak{o}^{-1}$. By the definition of $\mathfrak{o}^{-1}$, I and J are integral ideals and we have $I + J = R$. Thus by our previous algorithm, we can find in polynomial time $e \in I$ and $f \in J$ such that $e + f = 1$, and $u = e/a$ and $v = f/b$ satisfy the desired conditions. □

Algorithm 5.18 (Computation of A_i)**.** *Let $\mathcal{O}_d$ be the integer ring of the quadratic field K and $\mathfrak{a}$ a representative of an ideal class of K.*

Input: γ *and* δ*, the integers that generate* $\mathfrak{a}$*.*

Output: $\alpha \in \mathfrak{a}^{-1}$ *and* $\beta \in \mathfrak{a}^{-1}$ *such that* $\alpha\delta - \beta\gamma = 1$*.*

1. If $\delta = 0$, then set $(\alpha, \beta) \leftarrow (0, 1/\gamma)$.

2. If $\gamma = 0$, then set $(\alpha, \beta) \leftarrow (1/\delta, 0)$.

3. *If γ and δ are both nonzero, as in Theorem* 5.17*:*

   a. $\mathfrak{a} \leftarrow \langle \delta \rangle$ *and* $\mathfrak{b} \leftarrow \langle \gamma \rangle$.

   b. $\mathfrak{o} \leftarrow \delta\mathfrak{a} + \gamma\mathfrak{b}$.

   c. $I \leftarrow \delta\mathfrak{a}\mathfrak{o}^{-1}$ *and* $J \leftarrow \gamma\mathfrak{b}\mathfrak{o}^{-1}$.

   d. *Pass I and J as input to Algorithm* 5.16 *with output $e \in I$ and $f \in J$.*

   e. $(\alpha, \beta) \leftarrow (e/\delta, f/\gamma)$.

4. *Return α, β.*

Now we have everything that we need to calculate the set of generators for all cases of $\mathrm{PSL}_2(\mathcal{O}_d)$. Thus we have the following algorithm:

Algorithm 5.19 (Computation of the Generators of $\mathrm{PSL}_2(\mathcal{O}_d)$)**.**

Input: $\mathcal{O}_d$*, the integer ring of the quadratic field K.*

Output: L*, the list of generators of* $\mathrm{PSL}_2(\mathcal{O}_d)$.

1. *Set ϵ to the fundamental unit of $\mathcal{O}_d$.*

2. *Let $(\gamma_1,\ \delta_1), \ldots, (\gamma_h,\ \delta_h)$ be representatives of the lowest norm of the classes of $Cl(\mathcal{O}_d)$.*

3. *Set $L \leftarrow [S, T, T_\omega, U_\epsilon]$.*

4. *For $2 \leq i \leq h$:*

   a. *Get $\alpha_i,\ \beta_i$ from Algorithm* 5.18 *with γ_i and δ_i as input.*

   b. *Set* $A_i \leftarrow \begin{pmatrix} \alpha_i & \beta_i \\ \gamma_i & \delta_i \end{pmatrix}$.

c. *Set* $\hat{\gamma}_i$ *and* $\hat{\delta}_i$ *to the generators of* $(\gamma_i,\ \delta_i)^{-2}$.

d. *Add the matrices* $A_i^{-1}U_\epsilon A_i$, $A_i^{-1}\begin{pmatrix}1 & \hat{\gamma}_i\\ 0 & 1\end{pmatrix}A_i$ *and* $A_i^{-1}\begin{pmatrix}1 & \hat{\delta}_i\\ 0 & 1\end{pmatrix}A_i$ *to the list* L.

5. Return L.

5.4 Examples

From Corollary 5.3 we see that the generators given in Theorem 5.1 and Theorem 5.15 are not necessarily a minimal set of generators for $\mathrm{PSL}_2(\mathcal{O}_d)$, but a working one nonetheless.

Using Theorem 5.15, Theorem 5.1, and Corollary 5.3 we give data of Γ_d up to $d = 59$ in Tables 1, 2, and 3. Table 1 contains the ideal class representatives of lowest norm and the fundamental unit of these quadratic fields. In Table 2, we list the set of generators for Γ_d and the methos used to aquire them. Also, for fields with class number 2 or higher, we give the values of the special matrices A_i, $T_{\hat{\gamma}_i}$, and $T_{\hat{\delta}_i}$ for $2 \leq i \leq h$ where needed. Note that for some sets provided, like that of $\mathcal{O}_{10}$, the ring of integers has a class number of two and there seems to be one generator missing according to Theorem 5.15 in Table 2. This is due to the fact that, for the ideal $\mathfrak{a}_2$, $\mathfrak{a}_2^{-2}$ is generated by a single element.

Table 1. Examples of Generators of PSL($\mathcal{O}_d$) (Part one).

Field	Ideal Class Representatives	Fundamental Unit
$\mathbb{Q}(\sqrt{2})$	(1)	$\epsilon = 1 - \omega$
$\mathbb{Q}(\sqrt{3})$	(1)	$\epsilon = 2 + \omega$
$\mathbb{Q}(\sqrt{5})$	(1)	$\epsilon = \omega$
$\mathbb{Q}(\sqrt{6})$	(1)	$\epsilon = -5 - 2\omega$
$\mathbb{Q}(\sqrt{7})$	(1)	$\epsilon = -8 + 3\omega$
$\mathbb{Q}(\sqrt{10})$	$(1), (2, \omega)$	$\epsilon = 3 - \omega$
$\mathbb{Q}(\sqrt{11})$	(1)	$\epsilon = 10 - 3\omega$
$\mathbb{Q}(\sqrt{13})$	(1)	$\epsilon = 1 + \omega$
$\mathbb{Q}(\sqrt{14})$	(1)	$\epsilon = 15 - 4\omega$
$\mathbb{Q}(\sqrt{15})$	$(1), (2, 1 - \omega)$	$\epsilon = 4 - \omega$
$\mathbb{Q}(\sqrt{17})$	(1)	$\epsilon = 5 - 2\omega$
$\mathbb{Q}(\sqrt{19})$	(1)	$\epsilon = 170 - 39\omega$
$\mathbb{Q}(\sqrt{21})$	(1)	$\epsilon = 2 + \omega$
$\mathbb{Q}(\sqrt{22})$	(1)	$\epsilon = -197 - 42\omega$
$\mathbb{Q}(\sqrt{23})$	(1)	$\epsilon = -24 + 5\omega$
$\mathbb{Q}(\sqrt{26})$	$(1), (2, \omega)$	$\epsilon = 5 - \omega$
$\mathbb{Q}(\sqrt{29})$	(1)	$\epsilon = 2 + \omega$
$\mathbb{Q}(\sqrt{30})$	$(1), (2, \omega)$	$\epsilon = -11 + 2\omega$
$\mathbb{Q}(\sqrt{31})$	(1)	$\epsilon = -1520 + 273\omega$
$\mathbb{Q}(\sqrt{33})$	(1)	$\epsilon = -19 - 8\omega$
$\mathbb{Q}(\sqrt{34})$	$(1), (3, 1 + \omega)$	$\epsilon = -35 - 6\omega$
$\mathbb{Q}(\sqrt{35})$	$(1), (2, 1 + \omega)$	$\epsilon = 6 + \omega$
$\mathbb{Q}(\sqrt{37})$	(1)	$\epsilon = 7 - 2\omega$
$\mathbb{Q}(\sqrt{38})$	(1)	$\epsilon = 37 - 6\omega$
$\mathbb{Q}(\sqrt{39})$	$(1), (2, 1 + \omega)$	$\epsilon = -25 + 4\omega$
$\mathbb{Q}(\sqrt{41})$	(1)	$\epsilon = -27 - 10\omega$
$\mathbb{Q}(\sqrt{42})$	$(1), (2, \omega)$	$\epsilon = 13 + 2\omega$
$\mathbb{Q}(\sqrt{43})$	(1)	$\epsilon = 3482 + 531\omega$
$\mathbb{Q}(\sqrt{46})$	(1)	$\epsilon = 24335 - 3588\omega$
$\mathbb{Q}(\sqrt{47})$	(1)	$\epsilon = 48 + 7\omega$
$\mathbb{Q}(\sqrt{51})$	$(1), (3, \omega)$	$\epsilon = -50 - 7\omega$
$\mathbb{Q}(\sqrt{53})$	(1)	$\epsilon = 3 + \omega$
$\mathbb{Q}(\sqrt{55})$	$(1), (2, 1 + \omega)$	$\epsilon = -89 + 12\omega$
$\mathbb{Q}(\sqrt{57})$	(1)	$\epsilon = 131 + 40\omega$
$\mathbb{Q}(\sqrt{58})$	$(1), (2, \omega)$	$\epsilon = -99 + 13\omega$
$\mathbb{Q}(\sqrt{59})$	(1)	$\epsilon = 530 - 69\omega$

Table 2. Examples of Generators of PSL($\mathcal{O}_d$) (Part two).

Field	Method	Generators of Γ_d
$\mathbb{Q}(\sqrt{2})$	5.1	$S, T_1, T_\omega, U_\epsilon$
$\mathbb{Q}(\sqrt{3})$	5.1	$S, T_1, T_\omega, U_\epsilon$
$\mathbb{Q}(\sqrt{5})$	5.3	S, T_1, T_ω
$\mathbb{Q}(\sqrt{6})$	5.1	$S, T_1, T_\omega, U_\epsilon$
$\mathbb{Q}(\sqrt{7})$	5.1	$S, T_1, T_\omega, U_\epsilon$
$\mathbb{Q}(\sqrt{10})$	5.15	$S, T_1, T_\omega, U_\epsilon, A_2^{-1}U_\epsilon A_2, A_2^{-1}T_{\hat{\gamma}_2}A_2$
$\mathbb{Q}(\sqrt{11})$	5.1	$S, T_1, T_\omega, U_\epsilon$
$\mathbb{Q}(\sqrt{13})$	5.3	S, T_1, T_ω
$\mathbb{Q}(\sqrt{14})$	5.15	$S, T_1, T_\omega, U_\epsilon$
$\mathbb{Q}(\sqrt{15})$	5.15	$S, T_1, T_\omega, U_\epsilon, A_2^{-1}U_\epsilon A_2, A_2^{-1}T_{\hat{\gamma}_2}A_2$
$\mathbb{Q}(\sqrt{17})$	5.3	S, T_1, T_ω
$\mathbb{Q}(\sqrt{19})$	5.1	$S, T_1, T_\omega, U_\epsilon$
$\mathbb{Q}(\sqrt{21})$	5.3	S, T_1, T_ω
$\mathbb{Q}(\sqrt{22})$	5.15	$S, T_1, T_\omega, U_\epsilon$
$\mathbb{Q}(\sqrt{23})$	5.15	$S, T_1, T_\omega, U_\epsilon$
$\mathbb{Q}(\sqrt{26})$	5.15	$S, T_1, T_\omega, U_\epsilon, A_2^{-1}U_\epsilon A_2, A_2^{-1}T_{\hat{\gamma}_2}A_2$
$\mathbb{Q}(\sqrt{29})$	5.3	S, T_1, T_ω
$\mathbb{Q}(\sqrt{30})$	5.15	$S, T_1, T_\omega, U_\epsilon, A_2^{-1}U_\epsilon A_2, A_2^{-1}T_{\hat{\gamma}_2}A_2$
$\mathbb{Q}(\sqrt{31})$	5.15	$S, T_1, T_\omega, U_\epsilon$
$\mathbb{Q}(\sqrt{33})$	5.3	S, T_1, T_ω
$\mathbb{Q}(\sqrt{34})$	5.15	$S, T_1, T_\omega, U_\epsilon, A_2^{-1}U_\epsilon A_2, A_2^{-1}T_{\hat{\gamma}_2}A_2, A_2^{-1}T_{\hat{\delta}_2}A_2$
$\mathbb{Q}(\sqrt{35})$	5.15	$S, T_1, T_\omega, U_\epsilon, A_2^{-1}U_\epsilon A_2, A_2^{-1}T_{\hat{\gamma}_2}A_2$
$\mathbb{Q}(\sqrt{37})$	5.3	S, T_1, T_ω
$\mathbb{Q}(\sqrt{38})$	5.15	$S, T_1, T_\omega, U_\epsilon$
$\mathbb{Q}(\sqrt{39})$	5.15	$S, T_1, T_\omega, U_\epsilon, A_2^{-1}U_\epsilon A_2, A_2^{-1}T_{\hat{\gamma}_2}A_2$
$\mathbb{Q}(\sqrt{41})$	5.3	S, T_1, T_ω
$\mathbb{Q}(\sqrt{42})$	5.15	$S, T_1, T_\omega, U_\epsilon, A_2^{-1}U_\epsilon A_2, A_2^{-1}T_{\hat{\gamma}_2}A_2$
$\mathbb{Q}(\sqrt{43})$	5.15	$S, T_1, T_\omega, U_\epsilon$
$\mathbb{Q}(\sqrt{46})$	5.15	$S, T_1, T_\omega, U_\epsilon$
$\mathbb{Q}(\sqrt{47})$	5.15	$S, T_1, T_\omega, U_\epsilon$
$\mathbb{Q}(\sqrt{51})$	5.15	$S, T_1, T_\omega, U_\epsilon, A_2^{-1}U_\epsilon A_2, A_2^{-1}T_{\hat{\gamma}_2}A_2$
$\mathbb{Q}(\sqrt{53})$	5.3	S, T_1, T_ω
$\mathbb{Q}(\sqrt{55})$	5.15	$S, T_1, T_\omega, U_\epsilon, A_2^{-1}U_\epsilon A_2, A_2^{-1}T_{\hat{\gamma}_2}A_2$
$\mathbb{Q}(\sqrt{57})$	5.3	S, T_1, T_ω
$\mathbb{Q}(\sqrt{58})$	5.15	$S, T_1, T_\omega, U_\epsilon, A_2^{-1}U_\epsilon A_2, A_2^{-1}T_{\hat{\gamma}_2}A_2$
$\mathbb{Q}(\sqrt{59})$	5.15	$S, T_1, T_\omega, U_\epsilon$

Table 3. Special Matrix Values Generators of $\mathrm{PSL}(\mathcal{O}_d)$.

Field	A_2	$T_{\hat{\gamma_2}}$	$T_{\hat{\delta_2}}$
$\mathbb{Q}(\sqrt{10})$	$\begin{pmatrix} -2 & -\frac{1}{2}\omega \\ \omega & 2 \end{pmatrix}$	$\begin{pmatrix} 1 & \frac{1}{2} \\ 0 & 1 \end{pmatrix}$	–
$\mathbb{Q}(\sqrt{15})$	$\begin{pmatrix} 3\omega & \frac{13}{2} - \frac{1}{2}\omega \\ 1+\omega & 2 \end{pmatrix}$	$\begin{pmatrix} 1 & \frac{1}{2} \\ 0 & 1 \end{pmatrix}$	–
$\mathbb{Q}(\sqrt{26})$	$\begin{pmatrix} -6 & -\frac{1}{2}\omega \\ \omega & 2 \end{pmatrix}$	$\begin{pmatrix} 1 & \frac{1}{2} \\ 0 & 1 \end{pmatrix}$	–
$\mathbb{Q}(\sqrt{30})$	$\begin{pmatrix} -7 & -\frac{1}{2}\omega \\ \omega & 2 \end{pmatrix}$	$\begin{pmatrix} 1 & \frac{1}{2} \\ 0 & 1 \end{pmatrix}$	–
$\mathbb{Q}(\sqrt{34})$	$\begin{pmatrix} -\frac{77}{3} - \frac{1}{3}\omega & \frac{4}{3} - \frac{7}{3}\omega \\ 1+\omega & 3 \end{pmatrix}$	$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & \frac{59}{9} + \frac{55}{9}\omega \\ 0 & 1 \end{pmatrix}$
$\mathbb{Q}(\sqrt{35})$	$\begin{pmatrix} 8\omega & \frac{33}{2} - \frac{1}{2}\omega \\ 1+\omega & 2 \end{pmatrix}$	$\begin{pmatrix} 1 & \frac{1}{2} \\ 0 & 1 \end{pmatrix}$	–
$\mathbb{Q}(\sqrt{39})$	$\begin{pmatrix} 9\omega & \frac{37}{2} - \frac{1}{2}\omega \\ 1+\omega & 2 \end{pmatrix}$	$\begin{pmatrix} 1 & \frac{1}{2} \\ 0 & 1 \end{pmatrix}$	–
$\mathbb{Q}(\sqrt{42})$	$\begin{pmatrix} -10 & -\frac{1}{2}\omega \\ \omega & 2 \end{pmatrix}$	$\begin{pmatrix} 1 & \frac{1}{2} \\ 0 & 1 \end{pmatrix}$	–
$\mathbb{Q}(\sqrt{51})$	$\begin{pmatrix} 5 & \frac{1}{3}\omega \\ \omega & 3 \end{pmatrix}$	$\begin{pmatrix} 1 & \frac{1}{3} \\ 0 & 1 \end{pmatrix}$	–
$\mathbb{Q}(\sqrt{55})$	$\begin{pmatrix} 13\omega & \frac{53}{2} - \frac{1}{2}\omega \\ 1+\omega & 2 \end{pmatrix}$	$\begin{pmatrix} 1 & \frac{1}{2} \\ 0 & 1 \end{pmatrix}$	–
$\mathbb{Q}(\sqrt{58})$	$\begin{pmatrix} -14 & -\frac{1}{2}\omega \\ \omega & 2 \end{pmatrix}$	$\begin{pmatrix} 1 & \frac{1}{2} \\ 0 & 1 \end{pmatrix}$	–

REFERENCES

[Blu03] Otto Blumenthal, *Über Modulfunktionen von Mehreren Veränderlichen*, vol. 56, 1903. MR 1511187

[Coh00] Henri Cohen, *Advanced Topics in Computational Number Theory*, Graduate Texts in Mathematics, vol. 193, Springer-Verlag, New York, 2000. MR 1728313

[Deu86] Jesse Ira Deutsch, *Identities on Modular Forms in Several Variables Derivable from Hecke Transformations*, Ph.D. thesis, 1986, Thesis (Ph.D.)–Brown University, p. 63. MR 2634902

[Fre90] Eberhard Freitag, *Hilbert Modular Forms*, Springer-Verlag, Berlin, 1990. MR 1050763

[Hir73] *Hilbert Modular Surfaces*, Secrétariat de l'Enseignement Mathématique, Université de Genève, Geneva, 1973, Série des Conférences de l'Union Mathématique Internationale, No. 4, Monographie No. 21 de l'Enseignement Mathématique. MR 0389921

[Maa] H. Maaß, *Über Gruppen von Hyperabelschen Transformationen*, vol. 1940 (German).

[May07] Sebastian Mayer, *Hilbert Modular Forms for the Fields* $\mathbb{Q}(\sqrt{5})$, $\mathbb{Q}(\sqrt{13})$ *and* $\mathbb{Q}(\sqrt{17})$, PhD dissertation, RWTH Aachen, 2007.

[Ser73] J.-P. Serre, *A Course in Arithmetic*, Springer-Verlag, New York-Heidelberg, 1973, Translated from the French, Graduate Texts in Mathematics, No. 7. MR 0344216

[Tam59] Tsuneo Tamagawa, *On Hilbert's Modular Group*, J. Math. Soc. Japan **11** (1959), 241–246. MR 0121356

[Vas72] L. N. Vaserštein, *The Group* SL_2 *Over Dedekind Rings of Arithmetic Type*, Mat. Sb. (N.S.) **89(131)** (1972), 313–322, 351. MR 0435293

[VDG88] Gerard Van Der Geer, *Hilbert modular surfaces*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], vol. 16, Springer-Verlag, Berlin, 1988. MR 930101

APPENDIX A

INDEX OF NOTATION

α'	the conjugate of $\alpha \in K$
ϵ	the fundamental unit of $\mathcal{O}_d$
ϵ_i	the i^{th} fundamental unit of $\mathcal{O}_K$
$\mathfrak{H}$	the upper half plane
D	the discriminant
d	a positive, square-free integer
h	the class number of $\mathcal{O}_d$
K	the real quadratic field $\mathbb{Q}(\sqrt{d})$
$N_K(\alpha)$	the norm of $\alpha \in K$
Sz	the trace of the vector z
$S_\Lambda(x, y)$	the inner product of vectors x and y in Λ
$\mathrm{SL}_2(R)$	the special linear group of degree 2 of R
$tr_K(\alpha)$	the trace of $\alpha \in K$