HAMBY, PAULA J., M.A. Enumeration of Quadratic Forms Over Totally Real Fields. (2012)
Directed by Dr. Dan Yasaki. 49 pp.

Let $\mathbb{F}$ be a real quadratic field with $\mathcal{O}_{\mathbb{F}}$ its ring of integers. Let f be a quadratic form over $\mathbb{F}$ with discriminant D. Using Koecher Theory and the generalized Voronoï Algorithm, we show that there are finitely many quadratic forms with discriminant D over $\mathbb{F}$. As there are finitely many quadratic forms, we can enumerate the forms up to a factor of the determinant of the norm of the form.

As an application, we can use these results to show a correspondence between the class of quadratic forms over $\mathbb{F}$ and the ideal class of a relative extension of $\mathbb{F}$ generated by the field discriminant.

ENUMERATION OF QUADRATIC FORMS OVER TOTALLY REAL FIELDS

by

Paula J. Hamby

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
2012

Approved by

_____
Committee Chair

APPROVAL PAGE

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

Committee Chair _____
Dan Yasaki

Committee Members _____
Sebastian Pauli

_____
Brett Tangedal

_____
Date of Acceptance by Committee

_____
Date of Final Oral Examination

ACKNOWLEDGMENTS

My experience at the University of North Carolina at Greensboro, which has culminated in this thesis, would not have been possible, nor nearly as pleasant, without the guidance and help of my committee members, encouragement and support from an excellent faculty and staff, and the camaraderie of my fellow students.

Foremost, I would like to express my deepest gratitude to my advisor, Dr. Dan Yasaki, who has gone above and beyond to insure my success and whose Number Theory class set the course for my graduate career. Dr. Yasaki also deserves credit for the exemplary LaTeX template used in this thesis! I would like to thank Dr. Tangedal for my first and thorough introduction to quadratic forms and number fields, Dr. Rychtar for an introduction to LaTeX, and Dr. Pauli for an introduction to the computational tools such as Sage used in this thesis. I especially want to thank Dr. Chhetri for her encouragement and interest in me early in my career. It made a big impact. Thanks to Dr. Duvall and Dr. Bell for running interference for me with the graduate office.

This has been a splendid experience.

TABLE OF CONTENTS

Page

LIST OF TABLES

Page

CHAPTER I

INTRODUCTION

1.1 Basics of Number Fields and Quadratic Forms

While the foundations of integral binary forms is generally attributed to Fermat, Euler, Lagrange, Legendre and Gauss [Wei07], Lagrange made the first general investigations of binary quadratic forms.

Definition I.1. A *number field* $\mathbb{F}$ is a finite degree field extension of the field of rational numbers $\mathbb{Q}$.

Definition I.2. The elements $\mathbb{F}$ which satisfy a monic polynomial with integer coefficients are called algebraic integers. The algebraic integers of $\mathbb{F}$ form a ring called the *ring of integers* of $\mathbb{F}$, denoted $\mathcal{O}_{\mathbb{F}}$.

Definition I.3. Let $\mathbb{F}$ be a number field with ring of integers $\mathcal{O}_{\mathbb{F}}$. An $\mathbb{F}$-*integral binary quadratic form* is a homogeneous degree 2 polynomial in 2 variables with coefficients in the ring of integers $\mathcal{O}_{\mathbb{F}}$. The form can be written as $ax_1^2 + bx_1x_2 + cx_2^2$.

For example, let $\mathbb{F} = \mathbb{Q}$, $\mathcal{O}_{\mathbb{F}} = \mathbb{Z}$. Then $x_1^2 + 3x_1x_2 + 6x_2^2$ is a $\mathbb{Q}$-integral binary quadratic form.

A binary quadratic form, $f = ax_1^2 + bx_1x_2 + cx_2^2$, can be represented as a 2×2 square symmetric matrix

$$A_f = \begin{bmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{bmatrix} \quad \text{such that} \quad f = \begin{bmatrix} x_1 & x_2 \end{bmatrix} \begin{bmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix},$$

where $x_1, x_2 \in \mathcal{O}_{\mathbb{F}}$.

Definition I.4. The *discriminant* D of a binary quadratic form, $f(x_1, x_2) = ax_1^2 + bx_1x_2 + cx_2^2$ is

$$D = b^2 - 4ac.$$

Equivalently, $D = -4\det(A_f)$.

The following theorem is attributed to Lagrange.

Theorem I.5 ([SO85])**.** *Let r be a divisor of an integer that can be represented by the form $ax_1^2 + bx_1x_2 + cx_2^2$ with x_1, x_2, relatively prime. Then r can be represented by a form $AX_1^2 + BX_1X_2 + CX_2^2$ with $X_1, X-2$ relatively prime and $B^2 - 4AC = b^2 - 4ac$.*

In other words, if a number r can be represented by $fax_1^2 + bx_1x_2 + cx_2^2$ with discriminant D, then through a suitable change of basis, r can be represented by the form $AX_1^2 + BX_1X_2 + CX_2^2$ with discriminant equal to D.

Definition I.6. The general linear group of degree 2 over a field, $\mathrm{GL}_2(\mathbb{F})$, or ring, $\mathrm{GL}_2(R)$ is the set of 2×2 invertible matrices with coefficients in $\mathbb{F}$ or R respectively with matrix multiplication as the group operator.

Recall that an element $u \in \mathcal{O}_{\mathbb{F}}$ is a unit in $\mathcal{O}_{\mathbb{F}}$ if there exists an element $v \in \mathcal{O}_{\mathbb{F}}$ such that $uv = 1$.

Definition I.7. Two $\mathbb{F}$-integral binary quadratic forms f and g are *equivalent*, denoted $f \sim g$, if there exists a matrix $M \in \mathrm{GL}_2(\mathcal{O}_{\mathbb{F}})$ such that

$$M^t A_f M = A_g.$$

Theorem I.8. *Equivalent forms have the same discriminant up to a square of a unit in $\mathcal{O}_{\mathbb{F}}$.*

Proof. Let f and g be equivalent quadratic forms. Then there exist a matrix $M \in \mathrm{GL}_2(\mathcal{O}_{\mathbb{F}})$ such that $M^t A_f M = A_g$. Let D_f and D_g be the discriminants of f and g respectively. Note that as $M \in \mathrm{GL}_2(\mathcal{O}_{\mathbb{F}})$, then $\det(M)$ is a unit in $\mathcal{O}_{\mathbb{F}}$. Then we have

$$\begin{aligned} D_g &= -4 \det(A_g) \\ &= -4 \det(M^t A_f M) \\ &= -4 \det(M^t)\det(A_f)\det(M) \\ &= -4 \det(M)^2 \det(A_f) \\ &= -4 \, u^2 \det(A_f) \\ &= u^2 D_f \quad \text{where } u \text{ is a unit in } \mathcal{O}_{\mathbb{F}}. \end{aligned}$$

□

Theorem I.9. *Equivalence of $\mathbb{F}$-integral binary quadratic forms is an equivalence relation.*

Proof. Let f, g, and h be $\mathbb{F}$-integral binary quadratic forms.

- The form $f \sim f$, because $I^t A_f I = A_f$, where I is the identity matrix.
- Suppose $f \sim g$. Then there exist a matrix M such that $M^t A_f M = A_g$, but as $M \in \mathrm{GL}_2(\mathcal{O}_{\mathbb{F}})$, M is invertible and its inverse $M^{-1} \in \mathrm{GL}_2(\mathcal{O}_{\mathbb{F}})$. Thus $A_f = (M^{-1})^t A_g M^{-1}$. Thus $g \sim f$.
- Let $f \sim g$ and $g \sim h$. Then there exist matrices M and $N \in \mathrm{GL}_2(\mathcal{O}_{\mathbb{F}})$ such that $M^t A_f M = A_g$ and $N^t A_g N = A_h$. Then by substitution for A_g by $M^t A_f M$

in the second equation, we get $N^t M^t A_f MN = A_h$. Note that $(MN)^t = N^t M^t$. As $\mathrm{GL}_2(\mathcal{O}_\mathbb{F})$ is a group, then $MN \in \mathrm{GL}_2(\mathcal{O}_\mathbb{F})$. Thus, by definition I.7, $f \sim h$.

□

Definition I.10. A *positive definite $\mathbb{Q}$-integral binary quadratic form* is an $\mathbb{F}$-integral binary quadratic form $f(x_1, x_2) = ax_1^2 + bx_1x_2 + cx_2^2$ with coefficients in $\mathbb{Q}$ such that for every $(x, y) \in \mathbb{Q}$ with $(x_1, x_2) \neq (0, 0)$, $f(x_2, x_2) > 0$. If $f(x_1, x_2)$ is positive definite then $a > 0$ and $c > 0$.

Definition I.11. The *special linear group* $\mathrm{SL}_2(\mathbb{Z}) \subset \mathrm{GL}_2(\mathbb{Q})$ is the group of 2×2 invertible matrices with coefficients in $\mathbb{Z}$ and determinant 1.

Definition I.12. Two forms, f and g, are *properly equivalent* if there exists $M \in \mathrm{SL}_2(\mathbb{Z})$ such that $A_f = M^t A_g M$.

The following theorem is attributed to Lagrange.

Theorem I.13 ([SO85])**.** *There are only finitely many proper equivalence classes of $\mathbb{Q}$-integral positive binary quadratic forms with a given discriminant D.*

Theorems I.5 and I.13, while based only over $\mathbb{Q}$, form the basis of a reduction theory of binary quadratic forms, by providing a definition of equivalence (Definition I.7) and showing that finitely many classes of forms exist per discriminant (Theorem I.13). Gauss, Dirichlet, and Minkowski [SO85] extended these theories to quadratic forms in n variables. Koecher Theory [Koe60] and Voronoï's reduction theory [Vor08] have been used to extend reduction theory to n-ary forms over totally real number fields.

1.2 Reduction Theory of Binary Quadratic Forms over $\mathbb{Q}$

With a definition of equivalence classes, reduction theory for $\mathbb{F}$-integral binary quadratic forms can be defined. Essentially, given a reduction algorithm, a reduction theory allows us to determine if two elements of a set are equivalent. Given two elements of a set, we apply the reduction algorithm to the elements. If they are both reduced to the same reduced element, the two elements are equivalent.

For example, there is an equivalence relation on $\mathbb{Q}$ defined as

$$\frac{a}{b} \sim \frac{c}{d} \text{ if and only if } ad = bc, \quad \text{where } \frac{a}{b}, \frac{c}{d} \in \mathbb{Q}.$$

Thus, if $\frac{a}{b} \sim \frac{c}{d}$, then $\left[\frac{a}{b}\right]$ and $\left[\frac{c}{d}\right]$ are the same equivalence class. A number $\frac{a}{b} \in \mathbb{Q}$ is reduced if $(a, b) = 1$ with $b \neq 0$. Given a number $\frac{x}{y} \in \mathbb{Q}$, if $(x, y) = 1$, then $\frac{x}{y}$ is reduced. If $(x, y) \neq 1$ then x and y have a greatest common factor z greater than 1, which means $x = za, y = zb$ for some $a, b \in \mathbb{Z}$ such that $(a, b) = 1$. Thus divide numerator and denominator by the greatest common factor to get the representative $\frac{a}{b} \in \left[\frac{x}{y}\right]$. The representative $\frac{a}{b}$ such that $(a, b) = 1$ is a reduced form of $\frac{x}{y}$.

Definition I.14. A $\mathbb{Q}$-integral positive definite binary quadratic form, $f(x_1, x_2) = ax_1^2 + bx_1x_2 + cx_2^2$, is reduced over $\mathbb{Q}$ if either

$$c > a \quad \text{and } -a < b \leq a,$$

or

$$c = a \quad \text{and } 0 \leq b \leq a.$$

We need to prove existence of such a form in every equivalence class and that there is exactly one such form in each class. See Theorem I.15.

Theorem I.15. *Each equivalence class of $\mathbb{Q}$-integral positive definite binary quadratic forms over $\mathbb{Q}$ contains a unique reduced form.*

Proof. To prove existence, let C be an equivalence class of positive definite quadratic forms of discriminant D. Let $f(x_1, x_2) = ax_1^2 + bx_1x_2 + cx_2^2$, represented by $A_f = \begin{bmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{bmatrix}$, be an element of C such that a is the smallest among elements in C. In such a case, we necessarily have $c \geq a$, or else $\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \begin{bmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{bmatrix} \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} c & \frac{-b}{2} \\ \frac{-b}{2} & a \end{bmatrix}$ gives the form $g(x_1, x_2) = cx_1^2 - bx_1x_2 + ax_2^2$ which is an equivalent form with c minimal. Then we just relabel c and a so that a is minimal.
Now letting $\begin{bmatrix} 1 & h \\ 0 & 1 \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ act on f for $h = \lfloor (a-b)/2a \rfloor$ gives an equivalent form $j(x_1, x_2) = a'x_1^2 + b'x_1x_2 + c'x_2^2$, where $a = a'$ and $b' \in (-a', a']$. Since $a' = a$ is minimal, similarly as above, we have $a' \leq c'$. If $a' < c'$ or $a' = c'$ and $b' > 0$, the form is reduced by Definition I.14. However, if $a' = c'$ and $b' < 0$, we see that $j \sim k(x_1, x_2) = c'x_1^2 + -b'x_1x_2 + a'x_2^2$ is an equivalent form that results in a reduced form. So every equivalence class of positive definite quadratic forms of discriminant D has a reduced form.

To prove uniqueness, let $f(x_1, x_2) = ax_1^2 + bx_1x_2 + cx_2^2$ and $g(x_1, x_2) = a'x_1^2 + b'x_1x_2 + c'x_2^2$ be reduced forms of C. Since $f \sim g$ there exist $M = \begin{bmatrix} p & q \\ r & s \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z})$

such that $MA_fM^t = A_g$. Computing

$$MA_fM^t = \begin{bmatrix} p^2a + prb + r^2c & pqa + (pqrs)\frac{b}{2} + rsc \\ pqa + (pqrs)\frac{b}{2} + rsc & q^2a + qsb + s^2c \end{bmatrix} = \begin{bmatrix} a' & \frac{b'}{2} \\ \frac{b'}{2} & c' \end{bmatrix},$$

we have $a' = ap^2 + bpr + cr^2$. As f is reduced, a is minimal among the equivalent forms in C and $|b| \leq a \leq c$.

If $\frac{r}{p} < 1$, we have that $0 \leq 1 + \frac{b}{a}\frac{r}{p} \leq 2$ and

$$a' = ap^2 + bpr + cr^2 = ap^2\left(1 + \frac{br}{ap}\right) + cr^2.$$

Thus $a' \geq ap^2\left(1 + \frac{br}{ap}\right) + ar^2 \geq a(p^2 + r^2) \geq a$.

Similarly, if $\frac{p}{r} < 0$ we have that $0 \leq 1 + \frac{b}{c}\frac{p}{r} \leq 2$ and

$$a' \geq ap^2 + ar^2\left(1 + \frac{bp}{cr}\right) \geq a(p^2 + r^2) \geq a.$$

This means that a' is minimal if and only if $a' = a$. Then $a' = a$ and M is of the form $\begin{bmatrix} 1 & h \\ 0 & 1 \end{bmatrix}$, which means that $b' = b + 2ah$ for some h. As f and g are both reduced, then $b, b' \in (-a, a]$, which means that $h = 0$. With $h = 0$, M is the identity matrix, and $A_f = A_g$. □

Over $\mathbb{Q}$ every equivalent form has the same discriminant up to the square of a unit in $\mathbb{Z}$. Since 1 and -1 are the only units in $\mathbb{Z}$, every form in a given equivalence class has the same discriminant. We show that there are finitely many equivalence classes per discriminant and therefore have finitely many reduced forms per discriminant.

Theorem I.16. *For $D < 0$, there are finitely many equivalence classes of $\mathbb{Q}$-integral positive definite binary quadratic forms per discriminant D. Denote this number by $c(D)$.*

Proof. Let $f(x_1, x_2) = ax_1^2 + bx_1x_2 + cx_2^2$ be a reduced $\mathbb{Q}$-integral positive definite binary quadratic form. Because $|b| \leq a \leq c$ then

$$4a^2 \leq 4ac = b^2 - D \leq a^2 - D,$$

and so

$$-a < b \leq a \leq \sqrt{\frac{-D}{3}}.$$

Thus, the values for a and b have an upper limit. As c is a function of D, a, and b, c also has a limited number of values. □

Example I.17. Assume that $D = -4$. By Theorem I.16, a reduced form with discriminant D can only have the values $a = 1$ and $b \in \{0, 1\}$. However, b cannot be an odd integer, because $D \equiv 0 \pmod 4$ and $4ac \equiv 0 \pmod 4$, thus $b \equiv 0 \pmod 4$. Therefore $b \neq 1$. Thus there can only be one reduced form in the equivalence class of $\mathbb{Q}$-integral positive definite binary forms for discriminant -4. Namely, $f(x_1, x_2) = x_1^2 + x_2^2$ is positive definite and the reduced $\mathbb{Q}$-integral positive definite binary quadratic form with $D = -4$.

Example I.18. Assume that $D = -15 \equiv 3 \pmod 4$. By Theorem I.16, a reduced form with discriminant D can only have the values $a \in \{1, 2\}$. As b must be odd, then $b \in \{-1, 1\}$ depending on the value of a. Recall that c is determined by D, a and b. Thus we see in Table 1 that there are only two reduced forms with $D = -15$.

Table 1. Reduced $\mathbb{Q}$-integral binary quadratic forms with $D = -15$.

a	b	c	positive definite?	reduced?
1	1	4	True	Yes
2	-1	2	True	No, because $c = a$ so $0 \leq b$.
2	1	2	True	Yes

Table 2. Reduced $\mathbb{Q}$-integral binary quadratic forms with $D = -47$.

a	b	c	positive definite?	reduced?
1	1	12	True	Yes
2	-1	6	True	Yes
2	1	6	True	Yes
3	-1	4	True	Yes
3	1	4	True	Yes
3	3	$\frac{14}{3}$	True	No, because c is not an integer.

Example I.19. Assume that $D = -47 \equiv 3 \pmod 4$. By Theorem I.16, a reduced form with discriminant D can only have the values $a \in \{1, 2, 3\}$. As b must be odd, then $b \in \{-1, 1, 3\}$ depending on the value of a. Recall that c is determined by D, a and b. Thus we see in Table 2 that there are five reduced forms with $D = -47$.

In the next chapter, we will discuss Koecher Theory from which we can describe a reduction theory of positive definite forms over totally real number fields. We will then use a generalization of Voronoï's algorithm to find a domain for these forms and then prove that there are finitely many equivalence classes of positive definite forms of a given discriminant. Those conditions allow us to count the number of classes of positive definite forms.

CHAPTER II

KOECHER THEORY

Let V be the 3-dimensional vector space of 2×2 symmetric matrices with coefficients in $\mathbb{R}$, $\mathrm{Sym}_2(\mathbb{R})$. A binary quadratic form can be represented by a matrix in $\mathrm{Sym}_2(\mathbb{Q}) \subset \mathrm{Sym}_2(\mathbb{R})$. Let $C \subset V$ be the set of positive definite matrices. Then for $c \in C, \lambda c \in C$ for $\lambda > 0$. So we see that C is a cone. Voronoï [Vor08] proved that C could be decomposed into a union of cells parameterized by perfect binary quadratic forms over $\mathbb{Q}$. He showed that there are finitely many rational perfect n-ary quadratic forms up to $\mathrm{GL}_n(\mathbb{Z})$ equivalence and that the cones defined by nonequivalent perfect forms form a domain, containing representatives from each equivalence class of quadratic forms. A fundamental domain is a subset of the space containing exactly one representative from each orbit of the action of $\mathrm{GL}_n(\mathbb{Z})$ on the space. The domain Voronoï produced is not a fundamental domain, as there are more than one representative from most equivalence classes. However if we consider the action of the stabilizer of the cone, we can choose unique representatives. Thus up to an action of the stabilizer of the cone, Voronoï created a reduction theory.

Koecher [Koe60] generalized Voronoï's reduction theory to positivity domains over arbitrary number fields using perfect points. For a description of Koecher's reduction theory of positivity domains, we'll closely follow Gunnells and Yasaki's explanation in [GY12].

Let V be a finite dimensional vector space over $\mathbb{R}$. Let $\langle\ ,\ \rangle : V \times V \to \mathbb{R}$ be a positive definite symmetric bilinear form. For a subset $C \subset V$, let $\overline{C}$ represent the

closure of C. Let C° represent the relative interior of C and $\partial C = \overline{C} \setminus C^\circ$ represent the boundary of C.

Definition II.1. A subset $C \subset V$ is called a *positivity domain* if the following conditions hold:

- C is open and nonempty.
- $\langle x, y \rangle > 0$ for all $x, y \in C$.
- For each $x \in V \setminus C$ there is a nonzero $y \in \overline{C}$ such that $\langle x, y \rangle \leq 0$.

Let $D \subset \overline{C} \setminus \{0\}$ be a nonempty discrete subset. Then for $x \in C$, let

$$\mu(x) = \inf_{d \in D} \{\langle d, x \rangle\}.$$

Koecher [Koe60] proved that $\mu(x) > 0$ and that there are finitely many $d \in D$ for which the infimum is achieved. This finite set, denoted $M(x)$, is referred to as the set of *minimal vectors* for x and defined by:

$$M(x) = \{d \in D \mid \langle d, x \rangle = \mu(x)\}.$$

Definition II.2. A point $x \in C$ is called perfect if the span $M(x) = V$.

Note that if $x \in C$ is perfect, then λx for $\lambda > 0$ is also perfect, because $M(\lambda x) = M(x)$ still spans V. Let $\Phi(D)$ denote the set of all perfect points x with $\mu(x) = 1$.

Definition II.3. A nonempty discrete subset $D \subset \overline{C} \setminus \{0\}$ is said to be *admissible* if for any sequence $\{x_i\}$, converging to a point in ∂C, we have $\lim \mu(x_i) = 0$.

The definition of an admissible set D is important because Koecher [Koe60] proved that if D is admissible, then $\Phi(D)$ is a discrete subset of C and provides a polyhedral decomposition of C. That decomposition is what makes Koecher's reduction theory work.

Definition II.4. A *polyhedral cone* in a real vector space V is a subset σ such that

$$\sigma = \sigma(v_1, \ldots, v_p) = \left\{ \sum_{i=1}^{p} \lambda_i v_i \mid \lambda_i \geq 0 \right\},$$

where $v_1, \ldots, v_p$ is a fixed set of vectors. We say that $v_1, \ldots, v_p$ *span* σ and the dimension of σ is the dimension of its linear span. If the dimension of σ is n, call σ an *n-cone*.

Recall that if $x \in \Phi(D)$, then x is perfect and the linear span of its minimal vectors $M(x) = V$, so we can talk about the cone defined by $M(x)$. Let $\sigma(x)$ denote the cone

$$\sigma(x) = \left\{ \sum \lambda_d d \mid \lambda_d \geq 0, d \in M(x) \right\},$$

which Koecher calls the *perfect pyramid of x.*

Let Σ be the set of all perfect pyramids with all their proper faces as x ranges over all points in $\Phi(D)$, the set of all perfect points. Koecher [Koe60, § 5.1] proved that for admissible D, the perfect pyramids have the following properties:

(a) Any compact subset of C meets finitely many perfect pyramids.

(b) Two different perfect pyramids have no interior point in common.

(c) Given any perfect pyramid σ, there are only finitely many perfect pyramids σ' such that $\sigma \cap \sigma'$ contains a point of C. Such σ' is referred to as a *neighbor* of σ.

(d) The intersection of any two perfect pyramids is a common face of each.

(e) Let F be a codimension one face of a perfect pyramid $\sigma(x)$. If F meets C, then there exists another perfect pyramid $\sigma(x')$ such that $\sigma(x) \cap \sigma(x') = F$. Note that if $F \in \partial C$, F is referred to as a *dead end*, because $\sigma(x')$ does not exist outside C.

(f) Then $C = \bigcup_{\sigma \in \Sigma} \sigma \cap C$.

Definition II.5. A *fan* Δ is a collection of cones that satisfy the following conditions.

(1) If F is a face of σ and $\sigma \in \Delta$, then $F \in \Delta$.

(2) if $\sigma, \sigma' \in \Delta$, then $\sigma \cap \sigma' = F$ is a face of both σ and σ'.

Condition d implies that Σ is a fan. We refer to Σ as the *Koecher fan*, and $\sigma \in \Sigma$ as the *Koecher cones.*

Theorem II.6. *Let $G \subset \mathrm{GL}(V)$ be the group of automorphisms of C. Let $\Gamma \subset G$ be a discrete subset such that $\Gamma D = D$. Koecher [Koe60, § 5.4] proved that if D is admissible, then Γ acts properly discontinuously on C. Thus we have a reduction theory for Γ in that*

(RT1) There are finitely many Γ-orbits in Σ.

(RT2) Every $x \in C$ is contained in a unique cone in Σ.

(RT3) Given any cone $\sigma \in \Sigma$ with $\sigma \cap C \neq \emptyset$, the group $\{\gamma \in \Gamma \mid \gamma\sigma = \sigma\}$ is finite.

If we choose representatives $\sigma_1, \ldots, \sigma_n$ of the orbits of Γ in Σ and let $\Omega = \bigcap(\sigma_i \cap C)$, then every form of C is represented in Ω, but not uniquely. Each of the σ_i have a finite stabilizer subgroup Γ_i of Γ. So, to construct a fundamental domain, we take a form from the set $\{\gamma_j^t x \gamma_j \mid \gamma_j \in \Gamma_i, x \in \sigma_i\}$.

Definition II.7. A *totally real number field* is a number field $\mathbb{F}$ in which all the embeddings into the complex numbers, $\mathbb{C}$, are real numbers.

Example II.8. The number field $\mathbb{Q}(\sqrt{2})$ is a totally real number field. It has two embeddings into $\mathbb{C}$,

(1) $\varphi_1 : \mathbb{Q}(\sqrt{2}) \hookrightarrow \mathbb{C}$ defined by $\varphi_1(a + b\sqrt{2}) = a + b\sqrt{2}$, and

(2) $\varphi_2 : \mathbb{Q}(\sqrt{2}) \hookrightarrow \mathbb{C}$ defined by $\varphi_2(a + b\sqrt{2}) = a - b\sqrt{2}$

with $a, b \in \mathbb{Q}$. Because a, b, and $\sqrt{2}$ are real numbers, then all the embeddings of elements in $\mathbb{Q}(\sqrt{2})$ are real numbers.
However, $\mathbb{Q}(\sqrt{-2})$ is not a totally real number field because the embedding

$$\varphi : \mathbb{Q}(\sqrt{-2}) \hookrightarrow \mathbb{C} \text{ defined by } \varphi(a + b\sqrt{-2}) = a + b\sqrt{-2}$$

is not a real number.

Let $\mathbb{F}$ be a totally real number field with d embeddings in $\mathbb{R}$ and ring of integers $\mathcal{O}_{\mathbb{F}}$. Define $\sigma : \mathbb{F} \to \mathbb{R}$ as

$$\sigma(\alpha) = \sum_{1=i}^{d} \sigma_i(\alpha)$$

where $\alpha \in \mathbb{F}$ and $\sigma_i(\alpha)$ is the ith embedding of α in $\mathbb{R}$. We set $\alpha_i = \sigma_i(\alpha)$. Similarly, if $A \in \mathrm{Mat}_{n\times n}(\mathbb{F})$, then A_k refers to the matrix whose (ij)th entry is $\sigma_k(A_{ij})$.

Let $V = \mathrm{Sym}_2(\mathbb{R})^d$, where $\mathrm{Sym}_2(\mathbb{R}) = \left\{ \begin{bmatrix} a & b \\ b & c \end{bmatrix} \mid a, b, c \in \mathbb{R} \right\}$. Let $\mathrm{Sym}_2^+(\mathbb{R})$ represent the set of positive definite symmetric matrices with entries in $\mathbb{R}$. For $A \in V$, $A = (A_1, A_2, \ldots, A_d)$.

Definition II.9. The inner product $\langle\ ,\ \rangle : V \times V \to \mathbb{R}$ is defined as

$$\langle A, B\rangle = \sum \mathrm{Tr}(A_i B_i) \text{ for } 1 \leq i \leq d.$$

There exists a natural embedding $\phi : \mathrm{Sym}_2(\mathbb{F}) \to V$ given by

$$\phi(A) = (A_1, \ldots, A_d),$$

which defines a rational structure on V.

Define the map $q : \mathcal{O}_{\mathbb{F}}^2 \to \mathrm{Sym}_2(\mathbb{F})$ by

$$q(v) = vv^t.$$

Let $C \subseteq V = \prod \mathrm{Sym}_2^+(\mathbb{R})$. Then C is a positivity domain [Koe60, §9].

Let $D = \{q(v) \mid v \in \mathcal{O}_{\mathbb{F}}^2 \setminus \{0\}\} \subset C \setminus \{0\}$. Then D is an admissible set [Koe60, Lemma 11]. Thus $\Phi(D)$ is finite, and we have a Koecher fan.

The group $\mathrm{GL}_2(\mathbb{R})^d$ acts on V by

$$(g \cdot A) = gAg^t.$$

This action preserves C and is the automorphism group of C.

If we then find the stabilizers of the individual cones, $\Gamma_{\sigma(x)}$, in our Koecher Fan, we have a reduction theory for C. For each $x \in \Phi(D)$, fix $d \in M(x)$. Then a form $A \in \sigma(x)$ is reduced if

$$\langle A, q(d)\rangle = \min\{\langle \gamma A, q(d)\rangle \mid \gamma \in \Gamma_{\sigma(x)}\}.$$

Note that C can be viewed as the space of real-valued positive definite quadratic forms in n variables. If $A \in C$, then define Q_A on F^n by

$$Q_A(x) = \sum x^t A_i x.$$

Thus we have a reduction theory on the set of positive definite quadratic forms over $\mathbb{F}$.

We also have a reduction algorithm for forms in C.

Algorithm II.10.

Input: $y \in C, \Sigma$

Output: $y' \sim y$ such that $y' \in \Sigma$

Let $\nu = \min\{\langle y, \sigma \rangle | \sigma \in \Sigma\}$ and $F = \sigma$ associated with ν.

- For each neighbor σ' of F, compute $\langle y, \sigma' \rangle$.
- If there exists a neighbor σ' with $\langle y, \sigma' \rangle < \nu$, replace F with σ', ν with $\langle y, \sigma' \rangle$, and return to step one.
- Otherwise, terminate the procedure: y lines in the cone F.
- For each $\sigma \in \Sigma$ and each neighbor σ' of σ there is $\gamma \in G$ the automorphism group of C such that $\gamma\sigma' \in \Sigma$. So $\gamma y \in \Sigma$.

CHAPTER III

VORONOÏ ALGORITHM

Theorem II.6 gives a reduction theory on the set of positive definite quadratic forms over a totally real number field, but such a theory isn't particular helpful in finding the Koecher fan and cones over $\mathbb{F}$. Fortunately Voronoï [Vor08] created an algorithm for finding these cones, defined by perfect forms (see Definition II.2), over $\mathbb{Q}$, which can be generalized to cones over $\mathbb{F}$ (see Algorithm III.3). Ong [Ong77] used this algorithm to find cells associated with perfect binary quadratic forms over $\mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{3})$ and $\mathbb{Q}(\sqrt{5})$ and Leibak [Lei05] used it to find cells associated with perfect binary quadratic forms over $\mathbb{Q}(\sqrt{6})$.

To find the representatives of the perfect pyramids in the Koecher fan, $\sigma \in \Sigma$, we begin with a perfect form x_1 and its cone $\sigma(x_1)$. We then find the neighboring cones $\sigma(x_2), \ldots, \sigma(x_n)$, which we already know to be finite by Theorem II.6. Retain neighboring cones $\sigma(x_i), i \in \{2, \ldots, n\}$, which are mutually non-equivalent and not equivalent to $\sigma(x_1)$. Then the procedure is repeated for each new non-equivalent perfect form. As the classes of perfect forms are finite, so are the cones representing them. We eventually come to a point such that we find no new non-equivalent perfect forms and thus obtain Σ.

3.1 Over $\mathbb{Q}$

Following Schürmann [Sch09] we illustrate the Voronoï algorithm for the space of positive definite binary quadratic forms over $\mathbb{Q}$.

Example III.1. Let $x_1 = 2a^2 + 2ab + 2b^2$ represented as $A_{x_1} = \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}$. Then, the minimum value of x_1 is $\mu(x_1) = 2$, and the set of minimum vectors for x_1 is

$$M(x_1) = \left\{ \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ -1 \end{bmatrix} \right\}.$$

Finding the minimal vectors is nontrivial. For this, we can use the *Algorithm of Fincke and Pohst* [FP85]. Given a perfect form x and a constant $C > 0$, this algorithm will find all $d \in \mathbb{Z}^n$ such that $x(d) < C$. Then $M(x)$ consist of those $d \in \mathbb{Z}^n$ for which $x(d) = \mu(d)$. To find the neighbors of $\sigma(x_1)$, we now need the extreme rays that define the faces of our $\sigma_1(x_1)$. Let $\mathcal{R}$ be the set of rays, r_i such that r_i is perpendicular to a face of $\sigma(x)$, defined by a subset of $M(x)$, and $\langle dd^t, r_i \rangle > 0$ for all other $d \in M(x)$. The neighboring forms of $\sigma_1(x_1)$ are of the form $x_1 + \rho r_i$ for $r_i \in \mathcal{R}, i \in \{1, 2, 3\}$ and ρ is the smallest positive number such that $\mu(x_1) = \mu(x_1 + \rho r_i)$ and $M(x_1 + \rho r_i) \not\subseteq M(x_1)$. To find ρ use the following algorithm.

Algorithm III.2 (Determination of ρ.)**.**

Input: Initial upper and lower bound.

Output: ρ.

(1) Initialize upper and lower bounds for ρ. Say $u = 1$ and $l = 0$.

(2) If $x_1 + ur_i$ is not positive definite, then u is too large. If $\mu(x_1 + ur_i) = \mu(x_1)$, then u is too small. So do the following until $x_1 + ur_i$ is positive definite and $\mu(x_1 + ur_i) \neq \mu(x_1)$.

(a) If $x_1 + ur_i$ is not positive definite, set $u = (l+u)/2$, else set $l = u$ and $u = 2u$.

This provides an upper and lower bound of ρ.

(3) If $M(x_1 + lr_i) \subseteq M(x_i)$, then $l \neq \rho$ and we have to reduce the range of our bounds. Begin by setting $a = (u+l)/2$.

(a) If $\mu(x_1 + ar_i) \geq \mu(x_i)$, then ρ is in the upper half of the range, so set $l = a$. Otherwise $\mu(x_1 + ar_i) < \mu(x_i)$, then ρ is in the lower half of the range, so set

$$u = \min\{(\mu(x_i) - x_i(v))/r_i(v) \mid v \in M(x_i + ar_i), r_i(v) < 0\} \cup \{a\}.$$

(b) If $\mu(x_1 + ur_i) = \mu(x_i)$, just set $l = u$.

Then repeat until $M(x_1 + lr_i) \not\subseteq M(x_i)$.

(4) Now we have that $l = \rho$.

Following Voronöi's algorithm, as described by Schümann, we get the neighbors of x_1 to be $N_{x_1} = \left\{ \begin{bmatrix} 2 & -1 \\ -1 & 2 \end{bmatrix}, \begin{bmatrix} 6 & 3 \\ 3 & 2 \end{bmatrix}, \begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix} \right\}$. Then, when we check for equivalence, we find that these neighbors are equivalent to our perfect form x_1 via matrices $\begin{bmatrix} -1 & 1 \\ 1 & 0 \end{bmatrix}$, $\begin{bmatrix} -1 & -1 \\ 0 & -1 \end{bmatrix}$ and $\begin{bmatrix} -1 & 0 \\ -1 & -1 \end{bmatrix}$, respectively. Thus, $\Sigma = \{\sigma(x_1)\}$ for positive definite binary quadratic forms over $\mathbb{Q}$.

3.2 Over A Totally Real Number Field

Let $\mathbb{F}$ be a totally real number field with d embeddings in $\mathbb{R}$ and ring of integers $\mathcal{O}_{\mathbb{F}}$. Let $V = \mathrm{Sym}_2(\mathbb{R})^d$ and $\langle , \rangle : V \times V \to \mathbb{R}$ be the inner product defined in II.9. Recall from the previous chapter that $C \subseteq V = \prod \mathrm{Sym}_2^+(\mathbb{R})$ is a positivity domain and $D = \{q(v) \mid v \in \mathcal{O}_{\mathbb{F}} \setminus \{0\}\}$ is an admissible set. Recall that $M(x) = \{d \in D \mid x(d) = \mu(x)\}$. We can still use Fincke and Pohst to find $M(x)$ by utilizing the map φ in equation IV.1 that takes forms from $\mathrm{Sym}_2(\mathbb{F}) \to \mathrm{Sym}_4(\mathbb{Q})$. The extreme rays, $r_i \in \mathcal{R}$, can be found using linear inequalities such that $\langle r_i, d_i d_i^t \rangle = 0$ for all $d \in M(x)$ that define the face F_i and $\langle r_i, dd^t \rangle > 0$ for the remaining $d \in M(x)$.

Algorithm III.3 (Generalized Voronoï Algorithm)**.**

Input: Number of variables, n, in the n-ary form and $\mathbb{F}$.

Output: A complete list of nonequivalent perfect forms in $\mathrm{Sym}_n^+\mathbb{F}$.

Begin with a perfect form x.

(1) Compute $M(x)$ and $\mathcal{R}$.

(2) Enumerate $r \in \mathcal{R}$ such that $\mathcal{R} = \{r_1, \ldots, r_k\}$.

(3) Determine contiguous perfect forms $x_i = x + \rho r_i, i \in \{1, ..., k\}$.

Algorithm III.4 (Find Contiguous Perfect Forms)**.**

Input: Perfect form x and r_i.

Output: $\rho > 0$ with $\mu(x + \rho r_i) = \mu(x)$ and $M(x + \rho r_i) \not\subseteq M(x)$.

$(l, u) \leftarrow (0, 1)$

while $x + \rho r_i$ is not positive definite or $\mu(x + \rho r_i) = \mu(x)$ do

if $\mu(x + \rho r_i) \neq \mu(x)$ then

$u \leftarrow (l + u)/2$

else

$(l, u) \leftarrow (u, 2u)$

endif

while $M(x + \rho r_i) \not\subseteq M(x)$ do

$a \leftarrow (u + l)/2$

if $\mu(x + \rho r_i) \geq \mu(x)$ then

$l \leftarrow a$

else

$u \leftarrow \min \mu(x) - \langle x, vv^t \rangle / \langle r_i, vv^t \rangle \mid v \in M(x + \rho r_i) \cup \{a\}$

endif

if $\mu(x + \rho r_i) = \mu(x)$ then

$l \leftarrow u$

endif

end while

return l

(4) Test if x_i is equivalent to known perfect forms.

Repeat steps $1-4$ for new perfect forms.

Definition III.5. A collection of n elements of $\mathcal{O}_{\mathbb{F}}$, $s_1, s_2, \ldots, s_n$, such that every element of $\mathcal{O}_{\mathbb{F}}$ can be written as a $\mathbb{Z}$ linear combination of these elements is called an *integral basis* for $\mathcal{O}_{\mathbb{F}}$. We say that $\mathcal{O}_{\mathbb{F}} = [s_1, s_2, \ldots, s_n]$.

Theorem III.6. *Let $\mathbb{F} = \mathbb{Q}(\sqrt{d})$ where $d \in \mathbb{Z}, d \geq 2$ and d is square free. Then $[1, \omega] = \{a1 + b\omega \mid a, b \in \mathbb{Z}\}$ is an integral basis for $\mathcal{O}_{\mathbb{F}}$, where*

$$\omega = \begin{cases} \sqrt{d} & \text{if } d \equiv 2, 3 \pmod 4 \\ \frac{1+\sqrt{d}}{2} & \text{if } d \equiv 1 \pmod 4. \end{cases}$$

Theorem III.7. *There are exactly two perfect positive definite quadratic forms over $\mathbb{Q}(\sqrt{2})$.*

Proof. Apply Algorithm III.3 to the space of positive definite forms over $\mathbb{Q}(\sqrt{2})$. We have that $x_1 = (\frac{1}{2} + \frac{1}{4}\omega)a^2 + (\frac{1}{2} + \frac{1}{2}\omega)ab + (\frac{1}{2} + \frac{1}{4}\omega)b^2$, is a perfect form represented by $A_{x_1} = \begin{bmatrix} \frac{1}{4}(\omega+2) & \frac{1}{8}(2\omega+2) \\ \frac{1}{8}(2\omega+2) & \frac{1}{4}(\omega+2) \end{bmatrix}$. Then $\mu(x_1) = 1$ and

$$M(x_1) = \left\{ \begin{bmatrix} -\omega+1 \\ \omega-1 \end{bmatrix}, \begin{bmatrix} 1 \\ -1 \end{bmatrix}, \begin{bmatrix} -\omega+1 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ -\omega+1 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix} \right\}.$$

Using the generalized algorithm above, we find that $\sigma(x_1)$ has six neighbors:

$$N_{x_1} = \{n_1, n_2, n_3, n_4, n_5, n_6\}$$

where

$$n_1 = \begin{bmatrix} \frac{1}{4}(\omega+2) & \frac{1}{4}(2\omega+3) \\ \frac{1}{4}(2\omega+3) & \frac{1}{2}(2\omega+3) \end{bmatrix}, n_2 = \begin{bmatrix} \frac{1}{2}(2\omega+3) & \frac{1}{4}(2\omega+3) \\ \frac{1}{4}(2\omega+3) & \frac{1}{4}(\omega+2) \end{bmatrix},$$

$$n_3 = \begin{bmatrix} \frac{1}{2} & \frac{1}{4} \\ \frac{1}{4} & \frac{1}{4}(\omega+2) \end{bmatrix}, n_4 = \begin{bmatrix} \frac{1}{4}(\omega+2) & \frac{1}{4} \\ \frac{1}{4} & \frac{1}{2} \end{bmatrix},$$

$$n_5 = \begin{bmatrix} \frac{1}{4}(\omega+2) & \frac{1}{4}(-\omega-1) \\ \frac{1}{4}(-\omega-1) & \frac{1}{4}(\omega+2) \end{bmatrix}, \text{ and } n_6 = \begin{bmatrix} \frac{1}{4}(\omega+2) & \frac{1}{4}(\omega+1) \\ \frac{1}{4}(\omega+1) & \frac{1}{4}(\omega+2) \end{bmatrix}.$$

When we check for equivalence, we find that n_1 is not equivalent to x_1, so we place it in our list of nonequivalent perfect forms as x_2. Then n_i for $i \in \{2,3,4,5,6\}$ are either equivalent to x_1 or x_2.

We repeat the process for x_2, finding that $\mu(x_2) = 1$ and

$$M(x_2) = \left\{ \begin{bmatrix} 1 \\ \omega-2 \end{bmatrix}, \begin{bmatrix} -\omega+1 \\ \omega-1 \end{bmatrix}, \begin{bmatrix} 1 \\ -1 \end{bmatrix}, \begin{bmatrix} \omega+1 \\ -1 \end{bmatrix}, \begin{bmatrix} -\omega+1 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \right.$$
$$\left. \begin{bmatrix} \omega+1 \\ -\omega \end{bmatrix}, \begin{bmatrix} 1 \\ -\omega+1 \end{bmatrix}, \begin{bmatrix} 2 \\ -1 \end{bmatrix}, \begin{bmatrix} -\omega \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ -\omega+1 \end{bmatrix}, \begin{bmatrix} \omega \\ -\omega+1 \end{bmatrix} \right\}.$$

We find that $\sigma(x_2)$ has 24 neighbors. When tested for equivalence, all 24 neighbors are equivalent to either x_1 or x_2. Thus $\Sigma = \{\sigma(x_1), \sigma(x_2)\}$ for positive definite binary quadratic forms over $\mathbb{Q}(\sqrt{2})$. □

CHAPTER IV

FINITENESS OF EQUIVALENCE CLASSES

To show that there are finitely many equivalence classes per discriminant of a positive definite integral binary form over a real quadratic field, we will utilize a theorem of Eisenstein and Hermite. This theorem says that there are finitely many isomorphism classes of positive definite bilinear spaces over $\mathbb{Z}$ of given discriminant and dimension. We provide a map from $\mathrm{Sym}_2(\mathbb{F}) \to \mathrm{Sym}_4(\mathbb{Q})$ and invoke Theorem IV.5. But as equivalent forms have the same determinant up to a square of an element in $\mathrm{Sym}_2(\mathcal{O}_\mathbb{F})$, Theorem I.8, we must resolve an issue of discriminants of the form in $\mathrm{Sym}_4(\mathbb{Q})$. But we show in Theorem IV.3 that the determinant of a form in $\mathrm{Sym}_4(\mathbb{Q})$ mapped from $\mathrm{Sym}_2(\mathbb{F})$ has determinant equal to the norm of the determinant of the form in $\mathrm{Sym}_2(\mathbb{F})$ times the square of an element in $\mathrm{Sym}_2(\mathcal{O}_\mathbb{F})$.

Definition IV.1. [SO85] A *bilinear space* over $\mathbb{Z}$ is a pair (N, b) where N is a finitely generated free $\mathbb{Z}$-module and $b\colon N \times N \to \mathbb{R}$ a $\mathbb{Z}$-bilinear symmetric mapping.

Definition IV.2. Two bilinear spaces (N, b) and (N', b') are *isomorphic* if there is a $\mathbb{Z}$-linear isomorphism $\alpha : N \to N'$ with

$$b'(\alpha x, \alpha y) = b(x, y) \quad \text{for all } x, y \in N.$$

$$\text{Let } A \in \mathrm{Sym}_2(\mathbb{F}) = \begin{bmatrix} a + a'\omega & \frac{b+b'\omega}{2} \\ \frac{b+b'\omega}{2} & c + c'\omega \end{bmatrix} \text{ and define a map } \varphi\colon \mathrm{Sym}_2(\mathbb{F}) \to \mathrm{Sym}_4(\mathbb{Q})$$

by

$$\varphi(A) = \begin{bmatrix} T(A) & T(\omega A) \\ T(\omega A) & T(\omega^2 A) \end{bmatrix}, \tag{IV.1}$$

where $T(C) = \begin{bmatrix} \mathrm{Tr}(c_{1,1}) & \mathrm{Tr}(c_{1,2}) \\ \mathrm{Tr}(c_{2,1}) & \mathrm{Tr}(c_{2,2}) \end{bmatrix}$.

For example, if $A \in \mathrm{Sym}_2(\mathbb{Q}(\sqrt{2})) = \begin{bmatrix} 1+2\omega & \frac{4+6\omega}{2} \\ \frac{4+6\omega}{2} & 2+1\omega \end{bmatrix}$, then

$$\varphi(A) = \begin{bmatrix} T(A) & T(\omega A) \\ T(\omega A) & T(\omega^2 A) \end{bmatrix} \tag{IV.2}$$

$$= \begin{bmatrix} \mathrm{Tr}(1+2\omega) & \mathrm{Tr}(\frac{4+6\omega}{2}) & \mathrm{Tr}(1\omega+4) & \mathrm{Tr}(2\omega+6) \\ \mathrm{Tr}(\frac{4+6\omega}{2}) & \mathrm{Tr}(2+1\omega) & \mathrm{Tr}(2\omega+6) & \mathrm{Tr}(2\omega+2) \\ \mathrm{Tr}(1\omega+4) & \mathrm{Tr}(2\omega+6) & \mathrm{Tr}(2+4\omega) & \mathrm{Tr}(4+6\omega) \\ \mathrm{Tr}(2\omega+6) & \mathrm{Tr}(2\omega+2) & Tr(4+6\omega) & \mathrm{Tr}(4+2\omega) \end{bmatrix}$$

$$= \begin{bmatrix} 2 & 4 & 8 & 12 \\ 4 & 4 & 12 & 4 \\ 8 & 12 & 4 & 8 \\ 12 & 4 & 8 & 8 \end{bmatrix}. \tag{IV.3}$$

Theorem IV.3. *For $\varphi(A)$,*

$$\det(\varphi(A)) = \begin{cases} (4d)^2 N(\det(A)) & \text{for } \omega = \sqrt{d} \\ d^2 N(\det(A)) & \text{for } \omega = \frac{1+\sqrt{d}}{2} \end{cases}.$$

Proof. Assume A and $\varphi(A)$ as in equation IV.1.

If $\omega = \sqrt{d}$, the determinant of $\varphi(A)$ is

$$\begin{aligned}\det(\varphi(A)) =& 16a^2c^2d^2 - 16a^2c'^2d^3 - 8ab^2cd^2 + 16abb'c'd^3 \\ &- 8ab'^2cd^3 - 16a'^2c^2d^3 + 16a'^2c'^2d^4 - 8a'b^2c'd^3 \\ &+ 16a'bb'cd^3 - 8a'b'^2c'd^4 + b^4d^2 - 2b^2b'^2d^3 + b'^4d^4 \end{aligned} \tag{IV.4}$$

and the norm of $\det(A)$, $N(\det(A))$, is

$$\begin{aligned}N(A) =& a^2c^2 - a^2c'^2d - \frac{1}{2}ab^2c + abb'cd \\ &- \frac{1}{2}ab'^2cd - a'^2c^2d + a'^2c'^2d^2 - \frac{1}{2}a'b^2cd \\ &+ a'bb'cd - \frac{1}{2}a'b'^2c'd^2 + \frac{1}{16}b^4 - \frac{1}{8}b^2b'^2d + \frac{1}{16}b'^4d^2. \end{aligned} \tag{IV.5}$$

If $\omega = \frac{1+\sqrt{d}}{2}$. The determinant of $\varphi(A)$ is

$$\begin{aligned}
\det(\varphi(A)) =& a^2c^2d^2 + a^2cc'd^2 - \frac{1}{4}a^2c'^2d^3 + \frac{1}{4}a^2c'^2d^2 \\
&+ aa'c^2d^2 + aa'cc'd^2 - \frac{1}{4}aa'c'^2d^3 + \frac{1}{4}aa'c'^2d^2 \\
&- \frac{1}{2}ab^2cd^2 - \frac{1}{4}ab^2c'd^2 - \frac{1}{2}abb'cd^2 + \frac{1}{4}abb'c'd^3 \\
&- \frac{1}{4}abb'c'd^2 - \frac{1}{8}ab'^2cd^3 - \frac{1}{8}ab'^2cd^2 + \frac{1}{16}ab'^2c'd^3 \\
&- \frac{1}{16}ab'^2c'd^2 - \frac{1}{4}a'^2c^2d^3 + \frac{1}{4}a'^2c^2d^2 - \frac{1}{4}a'^2cc'd^3 \\
&+ \frac{1}{4}a'^2cc'd^2 + \frac{1}{16}a'^2c'^2d^4 - \frac{1}{8}a'^2c'^2d^3 + \frac{1}{16}a'^2c'^2d^2 \\
&- \frac{1}{4}a'b^2cd^2 - \frac{1}{8}a'b^2c'd^3 - \frac{1}{8}a'b^2c'd^2 + \frac{1}{4}a'bb'cd^3 \\
&- \frac{1}{4}a'bb'cd^2 + \frac{1}{8}a'bb'c'd^3 - \frac{1}{8}a'bb'c'd^2 + \frac{1}{16}a'b'^2cd^3 \\
&- \frac{1}{16}a'b'^2cd^2 - \frac{1}{32}a'b'^2c'd^4 + \frac{1}{16}a'b'^2c'd^3 - \frac{1}{32}a'b'^2c'd^2 \\
&+ \frac{1}{16}b^4d^2 + \frac{1}{8}b^3b'd^2 - \frac{1}{32}b^2b'^2d^3 + \frac{3}{32}b^2b'^2d^2 \\
&- \frac{1}{32}bb'^3d^3 + \frac{1}{32}bb'^3d^2 + \frac{1}{256}b'^4d^4 - \frac{1}{128}b'^4d^3 \\
&+ \frac{1}{256}b'^4d^2
\end{aligned} \tag{IV.6}$$

and $N(\det(A))$ is

$$\begin{aligned}
N(A) =& a^2c^2 + a^2cc' - \frac{1}{4}a^2c'^2d + \frac{1}{4}a^2c'^2 \\
&+ aa'c^2 + aa'cc' - \frac{1}{4}aa'c'^2d + \frac{1}{4}aa'c'^2 \\
&- \frac{1}{2}ab^2c - \frac{1}{4}ab^2c' - \frac{1}{2}abb'c + \frac{1}{4}abb'c'd \\
&- \frac{1}{4}abb'c' - \frac{1}{8}ab'^2cd - \frac{1}{8}ab'^2c + \frac{1}{16}ab'^2c'd \\
&- \frac{1}{16}ab'^2c' - \frac{1}{4}a'^2c^2d + \frac{1}{4}a'^2c^2 - \frac{1}{4}a'^2cc'd \\
&+ \frac{1}{4}a'^2cc' + \frac{1}{16}a'^2c'^2d2 - \frac{1}{8}a'^2c'^2d + \frac{1}{16}a'^2c'^2 \\
&- \frac{1}{4}a'b^2c - \frac{1}{8}a'b^2c'd - \frac{1}{8}a'b^2c' + \frac{1}{4}a'bb'cd \\
&- \frac{1}{4}a'bb'c + \frac{1}{8}a'bb'c'd - \frac{1}{8}a'bb'c' + \frac{1}{16}a'b'^2cd \\
&- \frac{1}{16}a'b'^2c - \frac{1}{32}a'b'^2c'd^2 + \frac{1}{16}a'b'^2c'd - \frac{1}{32}a'b'^2c' \\
&+ \frac{1}{16}b^4 + \frac{1}{8}b^3b' - \frac{1}{32}b^2b'^2d + \frac{3}{32}b^2b'^2 - \frac{1}{32}bb'^3d \\
&+ \frac{1}{32}bb'^3 + \frac{1}{256}b'^4d^2 - \frac{1}{128}b'^4d + \frac{1}{256}b'^4. \qquad \text{(IV.7)}
\end{aligned}$$

So, for $\varphi(A)$ where $\omega = \sqrt{d}$, we have $\det(\varphi(A)) = (4d)^2N(\det(A))$. Similarly for $\omega = \frac{1+\sqrt{d}}{2}$, we have $\det(\varphi(A)) = d^2N(\det(A))$. □

Since $\{1, \omega\}$ is a $\mathbb{Z}$-basis for $\mathcal{O}_{\mathbb{F}}$, we have $\hat{B} = \{[1,0]^t, [0,1]^t, [\omega,0]^t, [0,\omega]^t\}$ is a $\mathbb{Z}$-basis for $\mathcal{O}_{\mathbb{F}}^2$. Then $\begin{bmatrix} x_1 + x_2\omega \\ x_3 + x_4\omega \end{bmatrix}$ is $\begin{bmatrix} x_1 \\ x_3 \\ x_2 \\ x_4 \end{bmatrix}$ in basis $\hat{B}$, denoted $x_{\hat{B}}$. A straight-forward computation yields the following result.

Theorem IV.4. *Given* A_f *in* $\mathrm{Sym}_2(\mathcal{O}_\mathbb{F})$ *and* $x \in \mathcal{O}_\mathbb{F}^2$,

$$\mathrm{Tr}_\mathbb{F}(x^t A_f x) = x_{\hat{B}}^t \varphi(A) x_{\hat{B}}.$$

Theorem IV.5 ([SO85, Eisenstein, Hermite])**.** *There are only finitely many isomorphism classes of positive definite bilinear spaces over* $\mathbb{Z}$ *of given dimension* n *and given determinant* D.

Theorem IV.6. *If* $\varphi(A), \varphi(B) \in \mathrm{Sym}_4(\mathbb{Q})$ *are* $\mathrm{GL}_4(\mathbb{Z})$ *equivalent, then* $A, B \in \mathrm{Sym}_2(\mathbb{F})$ *are* $\mathrm{GL}_2(\mathcal{O}_\mathbb{F})$ *equivalent.*

Proof. Let $\varphi(A), \varphi(B) \in \mathrm{Sym}_4(\mathbb{Q})$ be $\mathrm{GL}_4(\mathbb{Z})$ equivalent and in the range of φ. Then there exists $\hat{M} \in \mathrm{GL}_4(\mathbb{Z})$ such that $\hat{M}^t \varphi(A) \hat{M} = \varphi(B)$. As $\varphi(A)$ and $\varphi(B)$ are in the image of φ then they are respectively of the form $\begin{bmatrix} \mathrm{Tr}(A_{ij}) & \mathrm{Tr}(\omega A_{ij}) \\ \mathrm{Tr}(\omega A_{ij}) & \mathrm{Tr}(\omega^2 A_{ij}) \end{bmatrix}$ and $\begin{bmatrix} \mathrm{Tr}(B_{ij}) & \mathrm{Tr}(\omega B_{ij}) \\ \mathrm{Tr}(\omega B_{ij}) & \mathrm{Tr}(\omega^2 B_{ij}) \end{bmatrix}$ for some $A, B \in \mathrm{Sym}_2(\mathbb{F})$. As $\varphi(A)$ and $\varphi(B)$ are $\mathrm{GL}_4(\mathbb{Z})$ equivalent, then $\hat{M}^t \varphi A \hat{M}$ must be $\begin{bmatrix} \mathrm{Tr}(B_{ij}) & \mathrm{Tr}(\omega B_{ij}) \\ \mathrm{Tr}(\omega B_{ij}) & \mathrm{Tr}(\omega^2 B_{ij}) \end{bmatrix}$. Let

$$\hat{M} = \begin{bmatrix} m & n & m'd & n'd \\ o & p & o'd & p'd \\ m' & n' & m & n \\ o' & p' & o & p \end{bmatrix}.$$

Then

$$\hat{M}^t\varphi(A)\hat{M} = \begin{bmatrix} \mathrm{Tr}(M^tAM_{ij}) & \mathrm{Tr}(\omega M^tAM_{ij}) \\ \mathrm{Tr}(\omega M^tAM_{ij}) & \mathrm{Tr}(\omega^2 M^tAM_{ij}) \end{bmatrix} = \begin{bmatrix} \mathrm{Tr}(B_{ij}) & \mathrm{Tr}(\omega B_{ij}) \\ \mathrm{Tr}(\omega B_{ij}) & \mathrm{Tr}(\omega^2 B_{ij}) \end{bmatrix}$$

where $M = \begin{bmatrix} m + m'\omega & n + n'\omega \\ o + o'\omega & p + p'\omega \end{bmatrix} \in \mathrm{Sym}_2(\mathbb{F})$. And so $A \sim B$. □

Then by Theorems IV.5 and IV.6 we can conclude the following result.

Theorem IV.7. *There are finitely many positive definite forms per discriminant over real quadratic fields.*

CHAPTER V

ENUMERATING FORMS

In the last chapter, we showed that there are finitely many equivalence classes per discriminant of positive definite integral binary forms over real quadratic fields. Then that means that if we fix a discriminant D and a totally real quadratic field $\mathbb{F}$, then there is an upper bound on the total number of positive definite integral binary forms over $\mathbb{F}$. We don't know how to calculate this bound, but we know it exist. Therefore we can compile data, looping over positive definite forms in a systematic way, and count nonequivalent forms per discriminant.

To begin, we need the Koecher fan, Σ, for positive definite forms over $\mathbb{F}$. To determine if a form belongs to the Koecher Fan, we also need the neighboring forms $\{n_1, n_2, \ldots, n_k\}$ of each perfect pyramid, $\sigma(x) \in \Sigma$. We can find these using the Generalized Voronoï Algorithm III.3. Recall that we are using the inner product II.9. Then for any positive definite binary forms, f, $f \in \sigma(x)$ if and only if

$$\langle \sigma(x), f \rangle \leq \langle n_i, f \rangle \text{ for } i \in \{1, \ldots, k\}. \tag{V.1}$$

To find our positive definite forms, recall that a form $f = ax_1^2 + bx_1x_2 + cx_2^2$ is positive definite only if a and c are totally positive. For $a \in \mathcal{O}_{\mathbb{F}}$ where $\mathbb{F}$ is a quadratic field, then it is of the form $a = a_1 + a_2\omega, a_1, a_2 \in \mathbb{Z}$. Then a has two embedding into $\mathbb{R}$, namely $a_1 + a_2\omega$ and it's conjugate $a_1 - a_2\omega$. For a to be totally positive, $a_1 + a_2\omega > 0$ and $a_1 - a_2\omega > 0$. Solving the system of linear inequalities, we find that a_1 must be positive. Then we see that $a_1 \pm a_2\omega > 0$ sets bounds of $\pm\lfloor \frac{a_1}{\omega} \rfloor$ for a_2. Similarly,

$c_1 > 0$ with $||\lfloor \frac{c_1}{\omega} \rfloor|| > c_2$. Now note that $D = b^2 - 4ac$ and that if f is positive definite, then $D < 0$. If we systematically loop over a to find our positive definite forms, we can substitute a for c and look at a maximum $D = b^2 - 4a^2$ per a. As b^2 is always positive, then $4a^2 > b^2$ if $D < 0$. As $b = b_1 + b_2\omega$ in $\mathcal{O}_{\mathbb{F}}$, if we assume that $b_2 = 0$, we can find limits on b_1. Recall that $||\lfloor \frac{a_1}{\omega} \rfloor|| > a_2$, thus

$$4(2a_1)^2 > 4(a_1 + a_2\omega) > b_1^2.$$

So $b_1 < |4a_1|$. And finally, c is a function of a, b and D.

With all of these relations, if we begin with a_1 a positive integer, then we can create a list of possible a_2. Then for each combination of a_1, a_2, we allow $c1$ to range over $\{1, 2, \ldots, a1\}$ and find a list of each c_2 acceptable for each c_1. Then to pair with each of these combinations, we find a list for $b_1 \in \{-4a_1, \ldots, 4a\}$, and for each b_1, the corresponding list of $b_2 \in \{-\lfloor \frac{4a_1 - b_1}{\omega} \rfloor \ldots \lfloor \frac{4a_1 - b_1}{\omega} \rfloor\}$. This system will find forms that are not positive definite, but once we check them against the system described in V.1, non-positive definite forms will be excluded anyway. For example, if we are working over $\mathbb{Q}(\sqrt{2})$ and we want to systematically work through positive definite binary quadratic forms, we begin with $a_1 = 1$. Then we have

$$a_2 \in \{-\left|\left\lfloor \frac{1}{\sqrt{2}} \right\rfloor\right|, \ldots - \left|\left\lfloor \frac{1}{\sqrt{2}} \right\rfloor\right|\} = \{0\},$$

$$c_1 \in \{1\} \text{ and } c_2 \in \{0\}.$$

Then we have that $b_1 \in \{-4, \ldots, 4\}$. Then we have to choose acceptable b_2 for each b_1. See Table "Example Loop for Positive Definite Forms over $\mathbb{Q}\sqrt{2}$". If the form is

Positive Definite, then we can determine if the form is in our Koecher Fan.

Table 3. Example Loop for Positive Definite Forms over $\mathbb{Q}(\sqrt{2})$.

a_1	a_2	c_1	c_2	b_1	b_2	Positive Definite?	In Σ?
1	0	1	0	-4	{-5,. . . ,5}	no	no
1	0	1	0	-3	{-4,. . . ,4}	no	no
1	0	1	0	-2	{-3,. . . ,3}	no	no
1	0	1	0	-1	{-3,. . . ,-1}	no	no
1	0	1	0	-1	0	yes	yes
1	0	1	0	-1	{1,. . . ,3}	no	no
1	0	1	0	0	-2	no	no
1	0	1	0	0	-1	yes	no
1	0	1	0	0	0	yes	yes
1	0	1	0	0	1	yes	no
1	0	1	0	0	2	no	no
1	0	1	0	1	{-2,. . . ,-1}	no	no
1	0	1	0	1	0	yes	no
1	0	1	0	1	{1,. . . ,2}	no	no
1	0	1	0	2	{-1,. . . ,1}	no	no
1	0	1	0	3	0	no	no
1	0	1	0	4	0	no	no
1	0	1	0	5	0	no	no

Once we have determined if a positive definite form belongs to Σ and then to which cone, $\sigma(x)$, the form belongs, we can use the stabilizer of the cone and the stabilizers of the faces of the cone to find nonequivalent forms of the same discriminant. We need the stabilizer of the faces, because the stabilizer of the cone will not permute the form to equivalent forms on the faces.

Algorithm V.1 (Finding Nonequivalent Forms of the Same Discriminant)**.**

Input: List of Distinct Forms with same Discriminant, List of Stabilizer Groups for $\sigma(x)$ and the faces of $\sigma(x)$

Output: List of Nonequivalent Forms with Same Discriminant

For f in List of Forms:

For γ in List of Stabilizer Groups

If $\gamma^t f \gamma \neq f$:

If $\pm\gamma^t f \gamma \in$ List of Forms:

Remove $\gamma^t f \gamma$ from List of Forms.

Return List of Forms.

Repeat for each $\sigma(x) \in \Sigma$.

CHAPTER VI

CLASS NUMBERS

In Chapter IV, we showed there were finitely many classes of positive definite quadratic forms per discriminant over a totally real field, or more briefly, the class number is finite. As an application, we can show a correspondence between the classes of quadratic forms over a totally real field $\mathbb{F}$ and the ideal classes of a relative quadratic extension $\mathbb{K}$ of $\mathbb{F}$ generated by the field discriminant.

6.1 Correspondence of Forms and Ideals over $\mathbb{Q}$

Let $\mathbb{E} = \mathbb{Q}(\sqrt{D})$ where $D < 0$ is the discriminant of $\mathbb{E}$ (see definition VI.3). Let $\overline{\alpha}$ represent the conjugate of $\alpha \in \mathbb{E}$. Equivalence classes of binary quadratic forms with determinant D have a finite abelian group structure. We show that there is a bijection between equivalence classes of quadratic forms and equivalence classes of ideals of quadratic fields.

Definition VI.1. An integral ideal, I, is a set of elements of $\mathcal{O}_{\mathbb{E}}$ such that

(1) if $\alpha, \beta \in I$, then $\alpha + \beta \in I$, and

(2) $\alpha I \subset I$ for all $\alpha \in \mathcal{O}_{\mathbb{E}}$.

Theorem VI.2. *Suppose $I \subset \mathcal{O}_{\mathbb{E}}$ is an ideal. Then there exists $\alpha, \beta \in \mathcal{O}_{\mathbb{E}}$ such that*

$$I = \{x_1\alpha + x_2\beta \mid x_1, x_2 \in \mathbb{Z}\}.$$

An integral basis for $\mathcal{O}_{\mathbb{E}}$ is not unique. Any other integral basis of I is of the form

$$\begin{bmatrix} \alpha' \\ \beta' \end{bmatrix} = A \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$$

where A is a 2×2 matrix with entries in $\mathbb{Z}$ such that $\det(A) = 1$.

Definition VI.3. The *field discriminant*, $D_{\mathbb{E}}$, is the determinant of the matrix, $M = \begin{bmatrix} \alpha & \beta \\ \overline{\alpha} & \overline{\beta} \end{bmatrix}$ where $[\alpha, \beta]$ is an integral basis for $\mathcal{O}_{\mathbb{E}}$.

Definition VI.4. A basis $[\alpha, \beta]$ for an ideal I is *correctly ordered* if

$$\frac{\alpha\overline{\beta} - \beta\overline{\alpha}}{\sqrt{D_{\mathcal{O}_{\mathbb{E}}}}} > 0$$

where $\overline{\alpha}$ is the conjugate of α, similarly for $\overline{\beta}$.

Theorem VI.5. *Any two correctly ordered bases of an ideal I are equivalent by an element in* $\mathrm{SL}_2(\mathbb{Z})$*, and conversely.*

Proof. Let $[\alpha, \beta] = [\delta, \gamma]$, both correctly ordered bases for an ideal I. Because δ, γ are a different basis for I , there are $a, b, c, d \in \mathbb{Z}$ such that

$$\begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} \delta \\ \gamma \end{bmatrix} = M \begin{bmatrix} \delta \\ \gamma \end{bmatrix},$$

with $\det(M) = \pm 1$. Since $a, b, c, d \in \mathbb{Z}$ and $\mathbb{Z}$ is fixed by conjugation, we have

$$\begin{bmatrix} \alpha & \overline{\alpha} \\ \beta & \overline{\beta} \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} \delta & \overline{\delta} \\ \gamma & \overline{\gamma} \end{bmatrix}.$$

Taking determinants, we have $\alpha\overline{\beta} - \beta\overline{\alpha} = \det(M)(\delta\overline{\gamma} - \gamma\overline{\delta})$. Since $[\alpha, \beta]$ and $[\delta, \gamma]$ are correctly oriented, then $\det(M) = 1$ and $M \in \mathrm{SL}_2(\mathbb{Z})$. Conversely, if $M \in \mathrm{SL}_2(\mathbb{Z})$ and $[\delta, \gamma]$ is correctly oriented then

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} \delta & \overline{\delta} \\ \gamma & \overline{\gamma} \end{bmatrix} = \begin{bmatrix} \alpha & \overline{\alpha} \\ \beta & \overline{\beta} \end{bmatrix}$$

and by taking discriminants again, we see that $[\alpha, \beta]$ is correctly oriented. □

Definition VI.6. Two ideals $I, J \subset \mathcal{O}_{\mathbb{E}}$ are *equivalent*, denoted $I \sim J$, if there exists $\alpha, \beta \in \mathcal{O}_{\mathbb{E}}$ such that

$$\alpha I = \beta J \quad \text{and} \quad N(\alpha\beta) > 0.$$

The set of equivalence classes generated by this definition of equivalence will be denoted $\mathrm{Cl}(\mathcal{O}_{\mathbb{E}})$.

Definition VI.7. Let I, J be ideals in $\mathcal{O}_{\mathbb{E}}$. Then the *product of I with J*, denoted IJ, is the set of all finite sums of elements of the form $\alpha\beta$ with $\alpha \in I$ and $\beta \in J$.

Definition VI.8. Let I be an nonzero ideal of $\mathcal{O}_{\mathbb{E}}$. Let $[\alpha, \beta]$ be an ordered basis for I. The norm of I, $N(I) = \frac{\alpha\overline{\beta} - \beta\overline{\alpha}}{\sqrt{D_{\mathbb{E}}}}$.

Theorem VI.9. *Multiplication of ideals gives* $\mathrm{Cl}(\mathcal{O}_{\mathbb{E}})$ *an abelian group structure in which the ideal class of* $\mathcal{O}_{\mathbb{E}} = (1)$ *is the identity element.*

Proof. If I, J are ideals in $\mathcal{O}_{\mathbb{E}}$, then their product is also an ideal in $\mathcal{O}_{\mathbb{E}}$. Multiplication of ideals is associative and commutative as multiplication of elements in $\mathcal{O}_{\mathbb{E}}$ is commutative and associative. Multiplication of ideals induces a well-defined multiplication of ideal classes. Let $I_1 \sim J_1$ and $I_2 \sim J_2$. Then there exists $\alpha_1, \beta_1, \alpha_2, \beta_2$ such that

$\alpha_i I_i = \beta_i J_i$ for $i = 1, 2$. Multiplying these two equalities, we get $\alpha_1\alpha_2 I_1 I_2 = \beta_1\beta_2 J_1 J_2$, thus $I_1 I_2 \sim J_1 J_2$. Finally, we need to show that every element of $\mathrm{Cl}(\mathcal{O}_\mathbb{E})$ has an inverse. Let $I = [\alpha, \beta]$ be an ideal of $\mathcal{O}_\mathbb{E}$. Then the ideal $\overline{I}$ generated by the conjugates of I is $[\overline{\alpha}, \overline{\beta}]$. The product $I\overline{I}$ is the principal ideal generated by the positive integer $N(I)$. Thus $I\overline{I} \sim (1)$, so I has an inverse. □

Theorem VI.10. *Let I be an ideal in $\mathcal{O}_\mathbb{E}$ and let $[\alpha, \beta]$ be a correctly ordered basis for I. Then the quadratic form*

$$f(x_1, x_2) = \frac{N(\alpha)x_1^2 + \mathrm{Tr}(\alpha\overline{\beta})x_1x_2 + N(\beta)x_2^2}{N(I)} = ax_1^2 + bx_1x_2 + cx_2^2$$

has integral coefficients and is a primitive form of discriminant D.

Proof. The numerators of $a, b, c \in \mathbb{Z}$ as they are norms and traces. Likewise, the denominator $N(I) \in \mathbb{Z}$. The numerators are also elements in $(N(I))$. So there exists elements, $j, k, l \in \mathcal{O}_\mathbb{E}$ such that

$$\begin{aligned} a &= \frac{\alpha\overline{\alpha}}{N(I)} = \frac{j(N(I))}{N(I)} = j, \\ b &= \frac{\alpha\overline{\beta} + \overline{\beta}\alpha}{N(I)} = \frac{k(N(I)}{N(I)} = k, \text{ and} \\ c &= \frac{\beta\overline{\beta}}{N(I)} = \frac{l(N(I))}{N(I)} = l. \end{aligned}$$

Since a and $N(I)$ are both in $\mathbb{Z}$ and $j \in \mathcal{O}_\mathbb{E}$, then $j \in \mathbb{Z}$. Similarly, $k, l \in \mathbb{Z}$. Now,

$[\alpha, \beta]$ is positively oriented, thus $\alpha\overline{\beta} - \overline{\alpha}\beta = \sqrt{D}N(I)$. The discriminant of $\mathbb{F}$ is

$$\begin{aligned} b^2 - 4ac &= \frac{(\alpha\overline{\beta} + \overline{\alpha}\beta)^2}{N(I)^2} - 4\frac{\alpha\overline{\alpha}\beta\overline{\beta}}{N(I)^2} \\ &= \frac{(\alpha\overline{\beta} - \overline{\alpha}\beta)}{N(I)^2} \\ &= \frac{DN(I)^2}{N(I)^2} \\ &= D. \end{aligned}$$

Now, we just need to show that $(a, b, c) = 1$. If m is a positive divisor of (a, b, c), then $m^2|(b^2 - 4ac)$. If $D \equiv 1 \pmod 4$ then D is squarefree, and $m = 1$. If $d \equiv 0 \pmod 4$, then $D' = \frac{D}{n4}$, where $n \in \mathbb{Z}$ is squarefree and $D' \not\equiv 1 \pmod 4$, so $m = 1$ or $m = 2$. If $m = 2$, write $a = 2a', b = 2b', c = 2c'$ for integers a', b', c' and b' odd. Then $b^2 - 4ac = 4b'^2 - 16a'c' = 4d'$. But this implies that

$$4b'^2 \equiv 4d' \pmod{16} \text{ implies } b'^2 \equiv d' \pmod 4.$$

With b' odd, $b'^2 \equiv 1 \pmod 4$, which contradicts that $d' \not\equiv 1 \pmod 4$. Therefore, $m = 1$ in all cases, and f is primitive. □

Theorem VI.11. *Let $f(x_1, x_2) = Ax_1^2 + Bx_1x_2 + Cx_2^2$ be a quadratic form of discriminant D. Write $f(x_1, x_2) = t(ax_1^2 + bx_1x_2 + cx_2^2)$ where $(a, b, c) = 1, a > 0$. Let*

$$I = [\alpha, \beta] = \left[a, \frac{b - \sqrt{D_{\mathbb{E}}}}{2}.\right]$$

Then I is an ideal of $\mathcal{O}_{\mathbb{E}}$ and $[\alpha, \beta]$ is a correctly ordered basis for I.

Proof. As $a \in \mathbb{Z}$ and $\mathbb{Z} \subset \mathcal{O}_{\mathbb{E}}$, then $a \in \mathcal{O}_{\mathbb{E}}$.

Case 1 Assume $D_{\mathbb{E}} \equiv 0 \pmod 4$. Then b is even and we have $\beta = \frac{2b' - 2\sqrt{D_{\mathbb{E}}}}{2} \in \mathcal{O}_{\mathbb{E}}$.

Case 2 Assume $D_{\mathbb{E}} \equiv 1 \pmod 4$. Then b is odd and we have $\beta = \frac{b+\sqrt{D_{\mathbb{E}}}}{2} = \frac{b-1}{2} + \frac{1+\sqrt{D_{\mathbb{E}}}}{2} \in \mathcal{O}_{\mathbb{E}}$.

□

Theorem VI.12 ([Bue89]Theorem 6.20)**.** *Theorems* VI.10 *and* VI.11 *create an isomorphism between the group of classes of binary quadratic forms of discriminant D and the narrow class group of $\mathcal{O}_{\mathbb{E}}$.*

6.2 Correspondence of Forms and Ideals over $\mathbb{Q}(\sqrt{d})$

For this section, we will follow [Mas00] closely. Let $\mathbb{F}$ be a real quadratic field and denote the conjugation of $\alpha \in \mathbb{F}$ as $\alpha*$.

Definition VI.13. Let $\alpha \in \mathbb{F}$, then α is *totally negative* if both the embeddings of α and $\alpha*$ into $\mathbb{R}$ are less than 0.

Let $\mathbb{K} = \mathbb{F}(\gamma)$ be a relative quadratic field extension of $\mathbb{F}$. We want $\mathbb{K}$ to be a totally complex number field (i.e. all embeddings of $\mathbb{K}$ into $\mathbb{C}$ are nonreal) and this may be achieved by choosing $\gamma \in \mathbb{F}$ such that $\gamma \in \mathcal{O}_{\mathbb{F}}$ and γ is totally negative. There are two embeddings of $\mathbb{K}$ into the complex numbers that fix $\mathbb{F}$. Denote the complex conjugation by $\overline{\alpha}$ for $\alpha \in \mathbb{K}$. For a given $\alpha \in \mathbb{K}$, define the relative trace, $\mathrm{Tr}_{\mathbb{K}/\mathbb{F}}(\alpha)$, as $\alpha + \overline{\alpha}$. The relative norm, $N_{\mathbb{K}/\mathbb{F}}$, is defined as $\alpha\overline{\alpha}$. From now on, we simply write $\mathrm{Tr}(\alpha)$ and $N(\alpha)$ in place of $\mathrm{Tr}_{\mathbb{K}/\mathbb{F}}(\alpha)$ and $N_{\mathbb{K}/\mathbb{F}}$, respectively. We can also define the norm of ideals in $\mathbb{K}$. Note that the norm of an ideal in $\mathbb{K}$ is an ideal in $\mathcal{O}_{\mathbb{F}}$. Let $[1, \Omega] = \{\alpha + \beta\Omega \mid \alpha, \beta \in \mathcal{O}_{\mathbb{F}}\}$ be a relative integral basis for $\mathcal{O}_{\mathbb{K}}$.

The relative field discriminant is

$$D_{\mathbb{K}/\mathbb{F}} = \det \begin{bmatrix} 1 & \Omega \\ 1 & \overline{\Omega} \end{bmatrix}^2 .$$

Theorem VI.14. *Any ideal $I_{\mathbb{K}}$ has a relative integral basis $I_{\mathbb{K}} = [\alpha, \beta]$. Any two correctly ordered bases of an ideal $I_{\mathbb{K}}$ are equivalent by an element in $\mathrm{SL}_2(\mathcal{O}_{\mathbb{F}})$ with determinant greater than 0.*

Theorem VI.15. *Let α, β be elements in $\mathbb{K}$ such that $[\alpha, \beta]$ is correctly ordered. If*

$$\begin{bmatrix} \alpha & \beta \\ \overline{\alpha} & \overline{\beta} \end{bmatrix} = \begin{bmatrix} 1 & \Omega \\ 1 & \overline{\Omega} \end{bmatrix} M$$

then for $I_{\mathbb{K}} = [\alpha, \beta], N(I_{\mathbb{K}})$ divides $(\det(M))$, and $N(I_{\mathbb{K}}) = (\det(M))$ if and only if $I_{\mathbb{K}} \in \mathcal{O}_{\mathbb{F}}$.

Let $f(x_1, x_2)_{\mathcal{O}_{\mathbb{F}}} = ax_1^2 + bx_1x_2 + cx_2^2$ be a quadratic form with coefficients in $\mathcal{O}_{\mathbb{F}}$, and $\overline{f(x_1, x_2)_{\mathcal{O}_{\mathbb{F}}}}$ be the conjugate form of $f(x_1, x_2)_{\mathcal{O}_{\mathbb{F}}}$. If the discriminant of $f(x_1, x_2)_{\mathcal{O}_{\mathbb{F}}} = D_{\mathbb{F}}$, then the discriminant of $\overline{f(x_1, x_2)_{\mathcal{O}_{\mathbb{F}}}} = \overline{D}_{\mathbb{F}}$. Let ϵ_0 be the fundamental unit of $\mathbb{F}$. Let $\epsilon_+ = \epsilon_0$ if $N(\epsilon_0) = 1$, and $\epsilon_+ = \epsilon_0^2$ if $N(\epsilon_0) = -1$. $f(x_1, x_2)_{\mathcal{O}_{\mathbb{F}}}$ is positive definite if $a > 0$. But $\overline{f(x_1, x_2)_{\mathcal{O}_{\mathbb{F}}}}$ may be either positive definite or negative definite depending on the value of $\overline{a}$. If $N(\epsilon_0) = -1$, we can consider only forms were a and $\overline{a}$ are positive.

Definition VI.16. Two quadratic forms $f(x_1, x_2)_{\mathcal{O}_{\mathbb{F}}}$ and $g(x_1, x_2)_{\mathcal{O}_{\mathbb{F}}}$ are equivalent if

$$A_f = (\epsilon_+)^n M^t A_g M$$

for some matrix $M \in \mathrm{GL}_2(\mathcal{O}_\mathbb{F})^{++}$, and $n \in \mathbb{Z}$, where

$$\mathrm{GL}_2(\mathcal{O}_\mathbb{F})^{++} = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a, b, c, d \in \mathcal{O}_\mathbb{F}, \text{ with } ad - bc \text{ a totally positive unit} \right\}.$$

Let $I_\mathbb{K} = [\alpha, \beta] = [1, \Omega]M$ be an ideal of $\mathbb{K}$. Then the quadratic form

$$\begin{aligned} f_{I_\mathbb{K}}(x_1, x_2)_{\mathcal{O}_\mathbb{F}} &= \frac{N(\alpha)x_1^2 + \mathrm{Tr}(\alpha\overline{\beta})x_1x_2 + N(\beta)x_2^2}{N(I_\mathbb{K})} \\ &= \frac{N(\alpha)x_1^2 + \mathrm{Tr}(\alpha\overline{\beta})x_1x_2 + N(\beta)x_2^2}{\det M} \\ &= ax_1^2 + bx_1x_2 + cx_2^2 \end{aligned} \tag{VI.1}$$

is a relative quadratic form with coefficients in $\mathcal{O}_\mathbb{F}$. Equation VI.10 can also be written

$$f_{I_\mathbb{K}}(x_1, x_2)_{\mathcal{O}_\mathbb{F}} = \frac{1}{N(I_\mathbb{K})} N(\alpha x_1 + \beta x_2) = \frac{1}{N(I_\mathbb{K})} N\left(\begin{bmatrix} x_2 & x_1 \end{bmatrix} \begin{bmatrix} \beta \\ \alpha \end{bmatrix} \right).$$

Theorem VI.17. *The form*

$$f_{I_\mathbb{K}}(x_1, x_2)_{\mathcal{O}_\mathbb{F}} = \frac{N(\alpha)x_1^2 + \mathrm{Tr}(\alpha\overline{\beta})x_1x_2 + N(\beta)x_2^2}{N(I_\mathbb{K})}$$

associated with the ideal $I_\mathbb{K}$ has discriminant $D_{\mathbb{K}/\mathbb{F}}$.

Proof. From equation 6.2, we get that

$$\begin{aligned} b^2 - 4ac &= \frac{(\alpha\overline{\beta} + \overline{\alpha}\beta)^2 - 4\alpha\overline{\alpha}\beta\overline{\beta}}{N(I_{\mathbb{K}})^2} \\ &= \frac{(\alpha\overline{\beta} - \overline{\alpha}\beta)^2}{N(I_{\mathbb{K}})^2} \\ &= \frac{\det \begin{bmatrix} 1 & \Omega \\ 1 & \overline{\Omega} \end{bmatrix}^2 \det(M)^2}{\det(M)^2} \\ &= D_{\mathbb{K}/\mathbb{F}}. \end{aligned} \tag{VI.2}$$

□

Theorem VI.18. *The equivalence class of $f_{I_{\mathbb{K}}}(x_1, x_2)_{\mathcal{O}_{\mathbb{F}}}$ is independent of choice of integral basis for $I_{\mathbb{K}}$.*

Proof. Let $[\alpha, \beta] = [1, \Omega]M$ and $[\delta, \gamma] = [1, \Omega]P$ be two integral bases for $I_{\mathbb{K}}$. Then we have

$$f_{I_{\mathbb{K}}}(y_1, y_2)_{\mathcal{O}_{\mathbb{F}}} = \frac{1}{\det P} N \left(\begin{bmatrix} y_2 & y_1 \end{bmatrix} \begin{bmatrix} \gamma \\ \delta \end{bmatrix} \right).$$

Then by Theorem VI.4,

$$\begin{bmatrix} \gamma \\ \delta \end{bmatrix} = A \begin{bmatrix} \beta \\ \alpha \end{bmatrix}$$

where $\det(A) = \epsilon$. Thus

$$f_{I_{\mathbb{K}}}(y_1, y_2)_{\mathcal{O}_{\mathbb{F}}} = \frac{1}{\det A \det M} N \left(\begin{bmatrix} y_2 & y_1 \end{bmatrix} A \begin{bmatrix} \beta \\ \alpha \end{bmatrix} \right).$$

By making the determinant ϵ, change of variables, we have

$$\begin{bmatrix} x_2 & x_1 \end{bmatrix} = \begin{bmatrix} y_2 & y_1 \end{bmatrix} A$$

giving us

$$\begin{aligned} f_{I_{\mathbb{K}}}(y_1, y_2)\mathcal{O}_{\mathbb{F}} &= \frac{1}{\det A \det M} N\left(\begin{bmatrix} x_2 & x_1 \end{bmatrix} \begin{bmatrix} \beta \\ \alpha \end{bmatrix} \right) \\ &= \frac{1}{\epsilon} f_{I_{\mathbb{K}}}(x_1, x_2)\mathcal{O}_{\mathbb{F}}. \end{aligned} \tag{VI.3}$$

Since equivalent forms allow for multiplication by a totally positive unit,

$$f_{I_{\mathbb{K}}}(y_1, y_2)\mathcal{O}_{\mathbb{F}} \sim f_{I_{\mathbb{K}}}(x_1, x_2)\mathcal{O}_{\mathbb{F}}.$$

□

Theorem VI.19. *Let $I_{\mathbb{K}}$ and $J_{\mathbb{K}}$ be two ideals in the same ideal class. Then*

$$f_{I_{\mathbb{K}}}(x_1, x_2)\mathcal{O}_{\mathbb{F}} \sim f_{J_{\mathbb{K}}}(x_1, x_2)\mathcal{O}_{\mathbb{F}}.$$

Proof. If $J_{\mathbb{K}} \sim I_{\mathbb{K}}$ then $J_{\mathbb{K}} = (\gamma)I_{\mathbb{K}}$ for some γ; so if $I_{\mathbb{K}} = [\alpha, \beta]$, then $J_{\mathbb{K}} = [\gamma\alpha, \gamma\beta]$

and

$$\begin{aligned} f_{J_{\mathbb{K}}}(x_1, x_2)_{\mathcal{O}_{\mathbb{F}}} &= \frac{1}{N(J_{\mathbb{K}})} N(\gamma\alpha x_1 + \gamma\beta x_2) \\ &= \frac{1}{N((\gamma)I_{\mathbb{K}})} N(\gamma) N(\alpha x_1 + \beta x_2) \\ &= \frac{1}{N(I_{\mathbb{K}})} N(\alpha x_1 + \beta x_2) \\ &= f_{I_{\mathbb{K}}}(x_1, x_2)_{\mathcal{O}_{\mathbb{F}}}. \end{aligned} \tag{VI.4}$$

□

Let $f(x_1, x_2) = ax_1^2 + bx_1x_2 + cx_2^2$ be a quadratic form of discriminant D. Define $\theta_f = \frac{b+\sqrt{D}}{2a}$. Then the ideal of $\mathbb{K}$ associated with this form is given by

$$f(x_1, x_2) = [a, a\theta_f]\,.$$

Consider the polynomial $x^2 + bx + \frac{b^2-D}{4}$. Then $\frac{b+\sqrt{D}}{a}$ is integral and satisfies this monic polynomial. Thus $\frac{b+\sqrt{D}}{a} \in \mathcal{O}_{\mathbb{K}}$.

Theorem VI.20. *Let $f(x_1, x_2) = ax_1^2 + bx_1x_2 + cx_2^2$ and $g(x_1, x_2) = dx_1^2 + ex_1x_2 + fx_2^2$ be equivalent forms with corresponding ideals $I_{\mathbb{K}} = [a, a\theta_f]$ and $J_{\mathbb{K}} = [d, d\theta_g]$. Then $I_{\mathbb{K}}$ and $J_{\mathbb{K}}$ are in the same ideal class.*

Proof. Let $M = \begin{bmatrix} r & s \\ t & u \end{bmatrix}$ be the matrix that takes g to f. Define ψ as

$$\psi_f = \frac{-b + \sqrt{D}}{2a}.$$

Then

$$\begin{aligned}\begin{bmatrix}\psi_f & 1\end{bmatrix} A_f \begin{bmatrix}\psi_f \\ 1\end{bmatrix} &= \begin{bmatrix}\psi_f & 1\end{bmatrix} M^t A_g M \begin{bmatrix}\psi_f \\ 1\end{bmatrix} \\ &= \begin{bmatrix}r\psi_f + s & t\psi_f + u\end{bmatrix} A_g \begin{bmatrix}r\psi_f + s \\ t\psi_f + u\end{bmatrix} \\ &= \begin{bmatrix}\frac{r\psi_f+s}{t\psi_f+u} & 1\end{bmatrix} A_g \begin{bmatrix}\frac{r\psi_f+s}{t\psi_f+u} \\ 1\end{bmatrix} = 0.\end{aligned}$$

Since $\psi_f \notin \mathbb{R}$, then $t\psi_f + u \neq 0$, and we can divide by this number. As ψ_g is the root of $g(x_1, 1)$, then $\psi_g = M\psi_f$. Also,

$$\theta_g = -\overline{\psi_g} = \frac{-(r\overline{\psi_f} + s)}{t\overline{\psi_f} + u} = \frac{r(-\overline{\psi_f}) - s}{-t(\overline{\psi_f}) + u} = \frac{r\left(\frac{b+\sqrt{D}}{2a}\right) - s}{-t\left(\frac{b+\sqrt{D}}{2a}\right) + u}.$$

So we see that $I_{\mathbb{K}} = [a, a\theta_f]$ and $J_{\mathbb{K}} = [d, d\theta_g]$ are in the same ideal class, because

$$\begin{bmatrix} r & -s \\ -t & u \end{bmatrix} \begin{bmatrix} a\frac{b+\sqrt{D}}{2a} \\ a \end{bmatrix} = C \begin{bmatrix} d\frac{e+\sqrt{D}}{2d} \\ d \end{bmatrix}, \text{ where } C = \frac{a(-t\frac{b+\sqrt{D}+u}{2a})}{d}.$$

so that $[a, a\theta] = C[d, d\theta]$ are the same ideal. □

Theorem VI.21. *Let* $f(x_1, x_2) = ax_1^2 + bx_1x_2 + cx_2^2 = (x_1 + \theta x_2)(x_1 + \overline{\theta}x_2)$ *and let* $I_{\mathbb{K}} = [a, a\theta]$. *Then* $f(x_1, x_2) = f_{I_{\mathbb{K}}}(x_1, x_2)$. *Thus,*

$$I_{\mathbb{K}} = [\alpha, \beta] \to \frac{1}{N(I_{\mathbb{K}})} N(\alpha x_1 + \beta x_2) \tag{VI.5}$$

and

$$ax_1^2 + bx_1x_2 + cx_2^2 \to \left[a, \frac{b + \sqrt{b^2 - 4ac}}{2}\right] \tag{VI.6}$$

are inverses.

Proof. From equation 6.2 we have

$$\begin{aligned} f_{I_{\mathbb{K}}}(x_1, x_2) &= \frac{1}{N(I_{\mathbb{K}})} N(ax_1 + a\theta x_2) \\ &= \frac{1}{a}(a^2x_1^2 + abx_1x_2 + acx_2^2) \\ &= f(x_1, x_2). \end{aligned} \tag{VI.7}$$

□

Theorem VI.22. *Let $\mathbb{F}$ be a real quadratic field, and let $\mathbb{K}$ be a totally complex quadratic extension of $\mathbb{F}$. Let $D_{\mathbb{K}/\mathbb{F}}$ be a generator of $\mathbb{K}/\mathbb{F}$. There exists a one to one correspondence between ideal classes in $\mathbb{K}$ and the equivalence classes of positive definite quadratic forms with coefficients in $\mathcal{O}_{\mathbb{F}}$ and discriminant $\epsilon^2 D_{\mathbb{K}/\mathbb{F}}$, where ϵ is a totally positive unit, and equivalence of quadratic forms is given in Definition* VI.16*. The correspondence is given by equations* VI.5 *and* VI.6*.*

REFERENCES

[Bue89] Duncan A. Buell, *Binary quadratic forms*, Springer-Verlag, New York, 1989, Classical theory and modern computations. MR 1012948 (92b:11021)

[FP85] U. Fincke and M. Pohst, *Improved methods for calculating vectors of short length in a lattice, including a complexity analysis*, Math. Comp. **44** (1985), no. 170, 463–471. MR 777278 (86e:11050)

[GY12] Paul E. Gunnells and Dan Yasaki, *Modular forms and elliptic curves over the complex cubic field of discriminant* -23, Int. J. Number Theory (2012), accepted.

[Koe60] Max Koecher, *Beiträge zu einer Reduktionstheorie in Positivitätsbereichen. I*, Math. Ann. **141** (1960), 384–432. MR 0124527 (23 #A1839)

[Lei05] Alar Leibak, *The complete enumeration of binary perfect forms over the algebraic number field* $\mathbb{Q}(\sqrt{6})$, Proc. Estonian Acad. Sci. Phys. Math. **54** (2005), no. 4, 212–234. MR 2190028 (2006i:11044)

[Mas00] Michael William Mastropietro, *Quadratic forms and relative quadratic extensions*, ProQuest LLC, Ann Arbor, MI, 2000, Thesis (Ph.D.)–University of California, San Diego. MR 2700674

[Ong77] Heidrun E. Ong, *Perfect quadratic forms over real quadratic number fields*, Math. Ann. **225** (1977), no. 1, 69–76. MR MR0427490 (55 #522)

[Sch09] Achill Schürmann, *Enumerating perfect forms*, Quadratic forms—algebra, arithmetic, and geometry, Contemp. Math., vol. 493, Amer. Math. Soc., Providence, RI, 2009, pp. 359–377. MR 2537111 (2010g:11110)

[SO85] Winfried Scharlau and Hans Opolka, *From Fermat to Minkowski*, Undergraduate Texts in Mathematics, Springer-Verlag, New York, 1985, Lectures on the theory of numbers and its historical development, Translated from the German by Walter K. Bühler and Gary Cornell. MR 770936 (85m:11003)

[Vor08] G. Voronoi, *Sur quelques proprietes des formes quadratiques positives parfaites.*, J. Reine Agnew. Math., **133** (1908), no. 1, 97–178. MR MR0427490 (55 #522)

[Wei07] André Weil, *Number theory*, Modern Birkhäuser Classics, Birkhäuser Boston Inc., Boston, MA, 2007, An approach through history from Hammurapi to Legendre, Reprint of the 1984 edition. MR 2303999 (2007k:01003)