UNIVERSITY OF CALIFORNIA, SAN DIEGO

Quadratic Forms and Relative Quadratic Extensions

A dissertation submitted in partial satisfaction of the
requirements for the degree
Doctor of Philosophy

in

Mathematics

by

Michael William Mastropietro

Committee in charge:

Professor Harold M. Stark, Chair
Professor Daniel Arovas
Professor Lawrence Carter
Professor Ronald Evans
Professor Audrey Terras

2000

The dissertation of Michael William Mastropietro is approved, and it is acceptable in quality and form for publication on microfilm:

Chair

University of California, San Diego

2000

To my Mother and Father

We could use up two Eternities in
learning all that is to be learned about our
own world and the thousands of nations
that have arisen and flourished and
vanished from it. Mathematics alone
would occupy me eight million years.
—Mark Twain.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

VITA

July 21, 1972	Born, Bristol, Pennsylvania
1993	B. S., *magna cum laude*, Duke University
1994–2000	Teaching assistant, Department of Mathematics, University of California San Diego
1996	M. A., University of California San Diego
2000	Department of Mathematics Distinguished Teaching Award for Teaching Assistants
2000	Ph. D., University of California San Diego

ABSTRACT OF THE DISSERTATION

Quadratic Forms and Relative Quadratic Extensions

by

Michael William Mastropietro
Doctor of Philosophy in Mathematics

University of California San Diego, 2000

Professor Harold M. Stark, Chair

Let k be a real quadratic field of class number one, and K be a totally complex extension of k. We investigate the correspondence between ideal classes of K and binary quadratic forms with $\mathcal{O}_k$ entries. We further demonstrate how to calculate the class number of K by identifying forms with points in the Hilbert upper half-plane, and using the geometry of the action of the Hilbert modular group $\mathrm{GL}_2(\mathcal{O}_k)^{++}$ to find a reduced form in each class. Finally, in the case where k has narrow class number one, we investigate how the class group of K can be decomposed into genera via quadratic characters.

Chapter 1

Preliminaries

1.1 Basic Number Field Concepts

In this first section we simply mention the basic concepts of algebraic number theory which we shall need throughout. For details the reader is referred to [12], [10].

An algebraic number field k is a finite degree field extension of the field of rational numbers $\mathbb{Q}$. If the degree of this extension is n, there are n embeddings of k into the complex numbers, $\mathbb{C}$. We refer to these embedding as the conjugates of k, and denote them by $k^{(1)}, k^{(2)}, \ldots, k^{(n)}$ (where $k^{(1)} = k$). Likewise, the conjugates of an element α of k are the images of α in $k^{(i)}$ and are denoted by $\alpha^{(i)}$. We define the norm and the trace of an element as the product and sum of its conjugates respectively.

Those elements of k which satisfy a monic irreducible polynomial with integer coefficients are called algebraic integers, or simply integers. Those integers which are in $\mathbb{Q}$ will be called rational integers if a distinction is needed. The integers of k form a ring (which contains $\mathbb{Z}$), denoted $\mathcal{O}_k$.

If k is a degree n extension of $\mathbb{Q}$ then $\mathcal{O}_k$ is an n-dimensional free $\mathbb{Z}$ module; that is, there is a collection of n elements of $\mathcal{O}_k$, $\omega_1, \omega_2, \ldots, \omega_n$, such that any element of $\mathcal{O}_k$ can be written as a $\mathbb{Z}$ linear combination of these elements. We say

$\mathcal{O}_k = [\omega_1, \omega_2, \ldots, \omega_n]$, and call this set an integral basis.

An integral basis for $\mathcal{O}_k$ is not unique, but two different integral bases differ by a determinant ± 1 change of variables. In this way we can define an important invariant of a field known as the discriminant.

Definition *Let $\mathcal{O}_k = [\omega_1, \omega_2, \ldots, \omega_n]$. We construct an $n \times n$ matrix M whose i, j entry is $\omega_j^{(i)}$. Then $d = d(k) = (\det(M))^2$ is called the field discriminant of k.*

Note by the above remarks, the discriminant is independent of choice of integral basis.

In number fields, one replaces the usual arithmetic of elements with arithmetic of ideals.

Definition *An integral ideal, $\mathfrak{a}$ is a set of elements of $\mathcal{O}_k$ which satisfy the following conditions.*

1. *If $\alpha, \beta \in \mathfrak{a}$, $\alpha + \beta \in \mathfrak{a}$.*
2. *$\gamma\mathfrak{a} \subset \mathfrak{a}$ for all $\gamma \in \mathcal{O}_k$.*

Although 0 satisfies these properties, it is not considered an ideal. In general, one writes $\mathfrak{a} = (\alpha_1, \alpha_2, \ldots, \alpha_t)$ to mean "the ideal generated by $\alpha_1, \alpha_2, \ldots, \alpha_t$". In other words, $\mathfrak{a}$ is all sets of $\mathcal{O}_k$ linear combinations of the α's. If $\mathfrak{a}$ is generated by one element, we say that $\mathfrak{a}$ is a principal ideal. It turns out that ideals are also n dimensional free $\mathbb{Z}$ modules, and thus have integral bases. In this case one writes $\mathfrak{a} = [\alpha_1, \alpha_2, \ldots, \alpha_n]$ to mean that all elements of $\mathfrak{a}$ can be expressed as a $\mathbb{Z}$ linear combination of the α's.

One can define the product of two ideals $\mathfrak{a}$ and $\mathfrak{b}$ by $\mathfrak{ab} = \{\alpha\beta \mid \alpha \in \mathfrak{a}, \beta \in \mathfrak{b}\}$, and it is an easy exercise to verify that this too is an ideal. Furthermore, one can define the inverse of an ideal $\mathfrak{a}$ as follows.

Definition *We define the inverse of an ideal $\mathfrak{a}$ as the set*

$$\mathfrak{a}^{-1} = \{\beta \in k \mid \forall \alpha \in \mathfrak{a}, \beta\alpha \in \mathcal{O}_k\}$$

We point out that $\mathfrak{a}^{-1}$ satisfies the definition of an ideal given above, except that its elements are not integers. In fact, if we take a finite product of ideals and inverses of ideals, this will also satisfy the above conditions. Such products are the so called *fractional ideals* of k. In the remainder of this paper, we use the word ideals to mean both ideals in the usual sense as well as fractional ideals, and when we refer to an ideal contained in $\mathcal{O}_k$ we call it an integral ideal.

In the same manner as we did for elements of k, we can define the conjugates of an ideal as its images in the conjugate fields of k. Also we can define the norm of ideals as the product of the conjugates. The norm of an ideal is an element of $\mathbb{Q}$, and is in $\mathbb{Z}$ if the ideal is integral.

The collection of ideals forms an abelian group under multiplication, where $\mathcal{O}_k$ is the identity element. The principal ideals form a subgroup of the group of ideals. The quotient group of ideals modulo principal ideals is called the ideal class group.

Definition *The cardinality of the class group of k is called the class number and is denoted by h, or $h(k)$ if clarification is needed.*

If $h = 1$ then every ideal in k is principal, and the arithmetic of k is as simple as possible. In general there is a degree $h(k)$ extension of k in which every ideal of k is principal. This field is called the Hilbert class field. Thus, the size of h gives an indication of how well behaved the arithmetic of the field is.

1.2 Quadratic Fields

Here we state specific results for degree 2 extensions of $\mathbb{Q}$. We let $k = \mathbb{Q}(\sqrt{D})$, where we can assume D is square free. If $D > 0$ we say that k is a real quadratic field, while if $D < 0$ we say k is a complex or imaginary quadratic field.

Proposition 1.1 *Let $k = \mathbb{Q}(\sqrt{D})$. $\mathcal{O}_k = [1, \omega]$, where*

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

We then immediately have the following.

Proposition 1.2 *Let $k = \mathbb{Q}(\sqrt{D})$. Then the discriminant*

$$d(k) \;=\; \begin{cases} 4D & \text{if } D \equiv 2 \text{ or } 3 \pmod 4 \\ D & \text{if } D \equiv 1 \pmod 4). \end{cases}$$

Proposition 1.3 *Let k be a real quadratic field, and let $\mathfrak{U}_k$ be the group of units of k. Then $\mathfrak{U}_k = \{\pm\epsilon_0^n\}$; that is, the units are generated by a single element. By convention, ϵ_0 is chosen to be positive and greater than one. We call ϵ_0 the fundamental unit.*

We now concentrate on complex quadratic fields k. Fix $k = \mathbb{Q}(\sqrt{d})$, where $d < 0$, is the discriminant of k. A $^-$ will denote conjugation in k. Lastly $\mathfrak{h} = \{x + iy \mid y > 0\}$, the so called complex upper half plane which we shall consider more fully in section 1.4.

Proposition 1.4 *Let k be a quadratic extension of $\mathbb{Q}$. Any ideal $\mathfrak{a} \in k$ has an integral basis, i.e. $\mathfrak{a} = [\alpha, \beta]_{\mathbb{Z}}$. Further any other integral basis of $\mathfrak{a}$ is of the form*

$$\begin{pmatrix} \hat\beta \\ \hat\alpha \end{pmatrix} = A \begin{pmatrix} \beta \\ \alpha \end{pmatrix} \tag{1.1}$$

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

Proposition 1.5 *Let α, β be elements of k such that $\frac{\beta}{\alpha} \notin \mathbb{Q}$. If*

$$\begin{pmatrix} \alpha & \beta \\ \bar\alpha & \bar\beta \end{pmatrix} = \begin{pmatrix} 1 & \omega \\ 1 & \bar\omega \end{pmatrix} M \tag{1.2}$$

where M is a 2×2 matrix with entries from $\mathbb{Q}$. For $\mathfrak{a} = (\alpha, \beta)$, $\mathcal{N}(\mathfrak{a})$ divides $\det(M)$, and $\mathcal{N}(\mathfrak{a}) = |\det(M)|$ if and only if $\mathfrak{a} = [\alpha, \beta]$. Furthermore, if α and β are chosen such that:

$$\frac{\beta}{\alpha} \in \mathfrak{h} \tag{1.3}$$

then $\det(M) > 0$, and the absolute value is unnecessary.

In fact, an integral basis exists for any field extension. If we insist on ordering α and β as in (1.3) then in Proposition 1.1 $\det(A) = 1$, and the absolute value may be dropped.

Proposition 1.6 *If $\mathfrak{a} = (\alpha, \beta)$ then $\mathcal{N}(\mathfrak{a})$ is the greatest common divisor of the coefficients of:*

$$\mathcal{N}(\alpha x + \beta y) = (\alpha x + \beta y)(\bar{\alpha} x + \bar{\beta} y) = \alpha\bar{\alpha}x^2 + (\alpha\bar{\beta} + \bar{\alpha}\beta)xy + \beta\bar{\beta}y^2. \tag{1.4}$$

The above is called the norm form.

This is actually only a special case of a more general theorem, the Kronecker Content Theorem, but all that we shall need. It will be useful also, to write the norm form:

$$\mathcal{N}(\alpha x + \beta y) = \mathcal{N}\left(\begin{pmatrix} y & x \end{pmatrix}\begin{pmatrix} \beta \\ \alpha \end{pmatrix}\right). \tag{1.5}$$

1.3 Relative Quadratic Extensions

Our main results will be based on quadratic extensions of quadratic fields of class number one. In many respects the theory is exactly the same, however, there are some differences. There is, of course, a more general theory of relative extensions which we will not mention.

If K is a degree 2 extension of k there are two embeddings (one of course trivial) of K into the complex numbers which fix k. We refer to these as the relative conjugate fields. The images of an element of K are of course called the relative conjugates. Throughout, we shall often use the adjective relative only when this needs to be made clear. We then define for all elements of K the relative trace and norm as the sum and product of the conjugates. Similarly we can define the relative trace and norm of an ideal of K. These quantities will be ideals of k, and will be contained in O_k if the ideal is integral.

If K is a degree 2 extension of k where $h(k) = 1$, then the integers of K are a 2 dimensional free $\mathcal{O}_k$ module. In other words, we have $\mathcal{O}_K = [1, \Omega]_{\mathcal{O}_k}$ and all elements of $\mathcal{O}_K$ are $\mathcal{O}_k$ linear combinations of 1 and Ω. We call $[1, \Omega]$ a relative integral basis, or simply an integral basis if it is understood that the base field is k. We further insist that Ω is chosen so that $\Omega \in \mathfrak{h}$. We now restate propositions 1.4 and 1.5.

Proposition 1.7 *Let k be a real quadratic field of class number 1, and K be a complex quadratic extension of k. Any ideal of $\mathfrak{a}$ of K has a relative integral basis $\mathfrak{a} = [\alpha, \beta]$. Any other integral basis for $\mathfrak{a}$ is of the form*

$$\begin{pmatrix} \hat{\beta} \\ \hat{\alpha} \end{pmatrix} = A \begin{pmatrix} \beta \\ \alpha \end{pmatrix} \tag{1.6}$$

where A is a 2×2 matrix with $\mathcal{O}_k$ entries and $\det(A) = \epsilon$, a unit. If we insist on the ordering of α and β such that

$$\frac{\beta}{\alpha} \in \mathfrak{h}, \tag{1.7}$$

then $\epsilon > 0$.

Proposition 1.8 *Let α, β be elements of K such that $\frac{\beta}{\alpha} \notin k$. If*

$$\begin{pmatrix} \alpha & \beta \\ \bar{\alpha} & \bar{\beta} \end{pmatrix} = \begin{pmatrix} 1 & \Omega \\ 1 & \bar{\Omega} \end{pmatrix} M \tag{1.8}$$

then for $\mathfrak{a} = (\alpha, \beta)$, $\mathcal{N}(\mathfrak{a})$ divides $(\det(M))$, and $\mathcal{N}(\mathfrak{a}) = (\det(M))$ if and only if $\mathfrak{a} = [\alpha, \beta]_{\mathcal{O}_k}$. Furthermore, if α and β are chosen as in (1.7) then $\det(M) > 0$.

1.4 The Modular Group

When one studies the equivalence of quadratic forms, it is helpful to have an understanding of the action of 2×2 matrices on complex numbers. For a more detailed treatment, see [11].

Let $\mathrm{GL}_2(\mathbb{R}) = \{2 \text{ x } 2\ \mathbb{R} \text{ matrices with } \det \neq 0\}$, and let $A = \begin{pmatrix} r & s \\ t & u \end{pmatrix} \in \mathrm{GL}_2(\mathbb{R})$. We define the action of A on a complex number $z = x + iy$ by

$$Az = \begin{pmatrix} r & s \\ t & u \end{pmatrix} z = \frac{rz+s}{tz+u} \tag{1.9}$$

We will use the following notation:

$$Az = z_A = x_A + iy_A$$

It is a straight forward calculation to show that for all matrices.

$$y_A = \frac{\det(A)\ y}{|tz+u|^2} \tag{1.10}$$

We see that y and y_A have the same sign when $\det A > 0$. Thus if we restrict to positive determinant matrices, the action preserves the complex upper-half plane.

Of fundamental interest to us is the action of a special subgroup of $GL_2(\mathbb{R})$ on $\mathfrak{h}$, the modular group $\mathrm{SL}_2(\mathbb{Z})$.

$$\mathrm{SL}_2(\mathbb{Z}) = \{A \in \mathrm{GL}_2(\mathbb{R}) \text{ with entries in } \mathbb{Z} \text{ and } \det(A) = 1\}.$$

Notice that I, the identity matrix, and $-I$ both preserve z, and it can be verified that these are the only $\mathrm{SL}_2(\mathbb{Z})$ matrices that do so; thus the action is actually one by $PSL_2(\mathbb{Z}) = SL_2(\mathbb{Z})/\{\pm I\}$. However, one always abuses notation and refers to the coset simply by the matrix itself. Because $\mathrm{SL}_2(\mathbb{Z})$ is a discrete group, it acts discontinuously on $\mathfrak{h}$. If we consider the orbits of points z in $\mathfrak{h}$, we can find a closed simply connected region such that every z has exactly one element in its orbit lying in this region. This region is called a fundamental domain. For $\mathrm{SL}_2(\mathbb{Z})$ one can describe a particular fundamental domain $\mathcal{F}$ in the following manner.

$$\mathcal{F} = \{z = x + iy \in \mathfrak{h} \mid -\frac{1}{2} < x \leq \frac{1}{2}, |z| \geq 1; \text{ if } |z| = 1, x \geq 0\} \tag{1.11}$$

One can represent $\mathcal{F}$ geometrically with the diagram below.

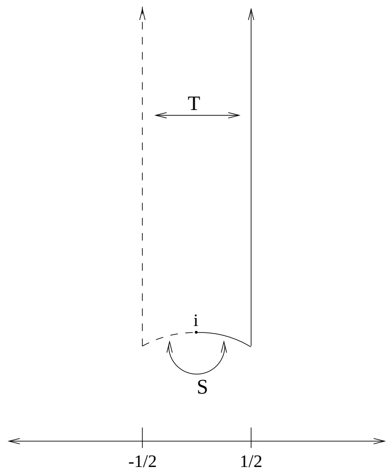

Figure 1.1: $\mathrm{SL}_2(\mathbb{Z})$ Fundamental Domain

Notice that the boundaries defined by $x = -\frac{1}{2}$ and $x = \frac{1}{2}$ can be identified through a translation by one. That is the matrix $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ identifies the point $z_1 = -\frac{1}{2} + iy$ with $z_2 = \frac{1}{2} + iy$. Also, one can show that if $|z| = 1$, for the matrix $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, $S(x+iy) = -x + iy$. Thus S identifies the left half of circle $|z| = 1$ with the right half. These are the only two boundary identifications.

There is a simple algorithm which one can use to find the image of any $z \in \mathfrak{h}$ in $\mathcal{F}$. In fact, this very algorithm can be used to construct $\mathcal{F}$ in the first place. The idea is what Stark calls the highest point method in [11].

1. If $\mathrm{Re}(z)$ is outside the range $-1/2 < \mathrm{Re}(z) \leq 1/2$ apply a series of $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ to translate $\mathrm{Re}(z)$ into this range.

2. If $|z| < 1$ apply $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ so that $|z| \geq 1$, this will happen by (1.10). If $|z| = 1$ make sure $\mathrm{Re}\, z \geq 0$ or else apply S one more time.

3. If $|\mathrm{Re}\, z| > 1/2$, repeat step 1.

This process will terminate, and when it does, we have found the image of z in $\mathcal{F}$. Notice that special care needs to be taken when the image of z lies on a boundary.

Chapter 2

Correspondence of forms and ideals

2.1 A Historical Note

Gauss first worked out the idea of equivalence classes of quadratic forms in his seminal *Disquitiones Arithmeticae*. It wasn't until Dedekind that the connection to ideals of quadratic fields was made. What is presented here is a modernized version of these classical ideas.

It should be noted also that there is a correspondence between ideal classes of real quadratic fields and quadratic forms, which we will not investigate. The reader is directed to Gauss' original treatment as well as more modern treatments in [1],[3],[10].

2.2 Binary Quadratic Forms

A binary quadratic form with integer coefficients is a homogeneous polynomial of degree two in two variables: $Q(x, y) = ax^2 + bxy + cy^2$, with $a, b, c \in \mathbb{Z}$. The discriminant of $Q(x, y)$, denoted $\mathrm{disc}(Q(x, y)) = b^2 - 4ac$. We shall be interested in the case where $\mathrm{disc}(Q(x, y)) < 0$. In this setting, we consider only those forms for which $a > 0$ which are called **positive definite**, as for all values of $(x, y) \neq (0, 0)$, $Q(x, y) > 0$.

One may think of these quadratic forms in terms of matrices since

$$Q(x,y) = \begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}. \tag{2.1}$$

We shall often refer to the form as a symmetric matrix.

By making a determinant one change of variables, one can create a form with different coefficients which still represents all the same values as the original form. This leads naturally to a notion of equivalence.

Definition *Two quadratic forms with rational integer coefficients, $Q(x, y) = ax^2 + bxy + cy^2$, $\widehat{Q}(x, y) = \widehat{a}x^2 + \widehat{b}xy + \widehat{c}y^2$, are equivalent, denoted, $Q(x, y) \sim \widehat{Q}(x, y)$, if*

$$\begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} = {}^tM \begin{pmatrix} \widehat{a} & \widehat{b}/2 \\ \widehat{b}/2 & \widehat{c} \end{pmatrix} M \tag{2.2}$$

for some matrix $M \in \mathrm{SL}_2(\mathbb{Z})$.

2.3 Correspondence of Forms and Ideals

In this section we present the connection between ideal classes and quadratic forms without proof. Our main results in the following chapter will mirror these facts, and the proofs given in the next chapter can be modified to work here.

Let $k = \mathbb{Q}(\sqrt{d})$, where $d < 0$ is the discriminant of k. We let $\mathfrak{a}$ be an ideal of k, and $\mathfrak{a} = [\alpha, \beta]$ as given by Proposition 1.4. We define a quadratic form associated with $\mathfrak{a}$ by using the norm form given in equation (1.4):

$$\begin{aligned} Q_{\mathfrak{a}}(x, y) &= \frac{1}{\mathcal{N}(\mathfrak{a})} \mathcal{N}(\alpha x + \beta y) \\ &= \frac{1}{\mathcal{N}(\mathfrak{a})} (\alpha x + \beta y)(\bar{\alpha} x + \bar{\beta} y) \\ &= ax^2 + bxy + cy^2. \end{aligned} \tag{2.3}$$

Theorem 1.6 gives us that $a, b, c \in \mathbb{Z}$.

The norm form is positive definite and its discriminant is d; in fact, it is the key to the correspondence. It can be seen that the equivalence class of $Q_{\mathfrak{a}}(x,y)$ is independent of the choice of integral basis for $\mathfrak{a}$. Furthermore, for any ideal $\mathfrak{b}$ in the same ideal class as $\mathfrak{a}$ we have $Q_{\mathfrak{a}}(x,y) \sim Q_{\mathfrak{b}}(x,y)$.

For the reverse correspondence, we start with a positive definite quadratic form with integer coefficients: $Q(x,y) = ax^2 + bxy + cy^2$, of discriminant $d < 0$. We wish to find a corresponding ideal class in $k = \mathbb{Q}(\sqrt{d})$. Let us factor $Q(x,y)$ as:

$$Q(x,y) = a(x + \theta y)(x + \bar{\theta} y), \tag{2.4}$$

where

$$\theta = \frac{b + \sqrt{d}}{2a} \tag{2.5}$$

is *minus* a root of $Q(x,1)$. Notice that $\theta \in \mathfrak{h}$. It is easily seen that $a\theta \in \mathcal{O}_k$ by noticing $b \equiv d \pmod 4$ along with Proposition 1.1. Therefore the ideal $(a, a\theta)$ is integral, and in fact has integral basis $[a, a\theta]$.

One can show that two equivalent forms lead to ideals that are in the same ideal class. Further, if we let $Q(x,y) = ax^2 + bxy + cy^2$, θ be as in (2.5), and $\mathfrak{a} = [a, a\theta]$, then the form $Q_{\mathfrak{a}}(x,y)$ as defined in (2.3) is equal to $Q(x,y)$. In this manner we have our correspondence. The theorem can be stated as follows:

Theorem 2.1 *Let k be an imaginary quadratic field of discriminant d. There exists a one to one correspondence between ideal classes of k and equivalence classes of positive definite binary quadratic forms of discriminant d, where equivalence of forms is given by equation (2.2).*

The correspondence is given by:

$$\mathfrak{a} = [\alpha, \beta] \longrightarrow \frac{1}{\mathcal{N}(\mathfrak{a})}\mathcal{N}(\alpha x + \beta y),$$

$$ax^2 + bxy + cy^2 \longrightarrow \left[a, \frac{b + \sqrt{b^2 - 4ac}}{2}\right].$$

2.4 Reduction Algorithm

We now demonstrate a method for systematically choosing representatives of each form class, and thus calculating the class number of the quadratic field of discriminant d. To do so, we take advantage of one last correspondence: we identify our forms with points in the complex upper half plane by identifying $Q(x,y)$ with

$$\psi = -\bar{\theta} = \frac{-b+\sqrt{b^2-4ac}}{2a}. \tag{2.6}$$

If we have two forms Q and $\widehat{Q}$, such that $Q = {}^t M \widehat{Q} M$, with $M = \begin{pmatrix} r & s \\ t & u \end{pmatrix}$

$$\begin{aligned}
\begin{pmatrix} \psi & 1 \end{pmatrix} Q \begin{pmatrix} \psi \\ 1 \end{pmatrix} &= 0, \\
\begin{pmatrix} \psi & 1 \end{pmatrix} {}^t M \widehat{Q} M \begin{pmatrix} \psi \\ 1 \end{pmatrix} &= 0, \\
\begin{pmatrix} r\psi + s & t\psi + u \end{pmatrix} \widehat{Q} \begin{pmatrix} r\psi + s \\ t\psi + u \end{pmatrix} &= 0, \\
\begin{pmatrix} \frac{r\psi+s}{t\psi+u} & 1 \end{pmatrix} \widehat{Q} \begin{pmatrix} \frac{r\psi+s}{t\psi+u} \\ 1 \end{pmatrix} &= 0.
\end{aligned}$$

Since ψ is not real, $t\psi + u \neq 0$, and we may divide by this quantity. Since by $\widehat{\psi}$ we mean the root of $\widehat{Q}(x,y)$ with $y = 1$, we see that $\widehat{\psi} = M\psi$. So moving from form to form is equivalent to acting on the roots by linear fractional transformation. Thus the representative form we choose for any class is the forms whose root lies inside $\mathcal{F}$.

Definition *Let $Q(x,y)$ be a positive definite quadratic form, and ψ be its root which lies in $\mathfrak{h}$. If $\psi \in \mathcal{F}$, then we say that $Q(x,y)$ is reduced.*

We should note that in most treatments of binary quadratic forms, the definition of a reduced form is given in terms of conditions on the coefficients, and the connections between reducing forms and linear fractional transformations is not mentioned. It was this connection, however, which was a motivation for this research.

To find a reduced form equivalent to a given form, we follow the procedure outlined in section 1.4. We re-present the algorithm in terms of the coefficients of the form.

1. If $|b| > a$ applying a series of $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ will translate b by a putting b in the range $-a < b \leq a$.
2. If $a > c$ apply $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ which interchanges a and c. If $a = c$ make sure $b \geq 0$ or else apply one more inversion.
3. If $|b| > a$, repeat step 1.

Reduced forms satisfy the following conditions:

$$-a < b \leq a \;;\; a \leq c \text{ ,if } a = c \text{ then } b \geq 0.$$

This is the usual definition of reduced forms, of course equivalent to the one presented above.

We can impose one more condition.

$$\begin{aligned} |d| &= 4ac - b^2 \\ &\geq 4a^2 - b^2 \\ &\geq 3a^2 \\ &\geq 3b^2 \end{aligned} \tag{2.7}$$

This leaves us with a finite number of triples (a, b, c) to check, and hence a way to count forms. We now give an example.

Example

Let us calculate the class number of $\mathbb{Q}(\sqrt{-71})$. By above considerations we need only consider $|b| \leq \sqrt{\frac{71}{3}} \leq 4$. However, since -71 is odd, $b = \pm 1, \pm 3$. The b's and the corresponding a's and c's are shown in the table below.

Table 2.1: Quadratic forms for $\mathbb{Q}(\sqrt{-71})$

$\mathbf{b}$	$\mathbf{ac} = \frac{\mathbf{71+b^2}}{\mathbf{4}}$	$(\mathbf{a}, \mathbf{b}, \mathbf{c})$
1	18	(1,1,18) (2,1,9) (3,1,6)
-1	18	(2,-1,9) (3,-1,6)
3	20	(4,3,5)
-3	20	(4,-3,5)

It follows that $h(\mathbb{Q}(\sqrt{-71}) = 7$. We can see which ideals these correspond to using the correspondence $Q(x, y) \to [a, a\theta]$. We know that a is the norm of the ideal, so we have ideals of norms 1, 2, 3 and 4. Since $-71 \equiv 1 \pmod 8$ and $-71 \equiv 1 \pmod 3$, we have the following factorizations

$$
\begin{aligned}
2 &= \mathfrak{p}_2 * \bar{\mathfrak{p}}_2 \\
3 &= \mathfrak{p}_3 * \bar{\mathfrak{p}}_3.
\end{aligned}
$$

It is easy to see that the forms $2x^2 \pm xy + 9y^2$, correspond to $\mathfrak{p}_2, \bar{\mathfrak{p}}_2$, and similarly $3x^2 \pm xy + 6y^2$ to $\mathfrak{p}_3, \bar{\mathfrak{p}}_3$. In fact the forms $Q_1(x, y) = ax^2 + bxy + cy^2$ and $Q_2(x, y) = ax^2 - bxy + cy^2$ always correspond to conjugate ideals. One can see this by noting that $\theta_2 = -\bar{\theta}_1$. Thus the ideal for $Q_2(x, y)$ is $[a, -a\bar{\theta}_1] = [a, a\bar{\theta}_1]$, which is the conjugate of the ideal for $Q_1(x, y)$. We are left now with only the ideals of norm 4, which, in light of the above remark, are also conjugates. There are only three ideals of norm 4, namely, $(2), \mathfrak{p}_2^2, \bar{\mathfrak{p}}_2^2$. Since (2) is principal, and the principal class must correspond to $x^2 + xy + 18y^2$, the last two forms must correspond to $\mathfrak{p}_2^2$ and $\bar{\mathfrak{p}_2}^2$. Our group is cyclic and generated, for example, by $\mathfrak{p}_2$.

Chapter 3

Correspondence of Forms and Ideals in Relative Quadratic Fields

Having sketched the classical theory, we turn our attention to the connection between ideal classes of a quartic field and quadratic forms with real quadratic integer entries. The motivation being, that once the correspondence is established, one can use the geometry of $\mathrm{GL}_2(\mathcal{O}_k)^{++}$ to reduce forms and calculate class numbers. Thus, our goal is to formulate a correspondence in the form of a theorem similar to Theorem 2.1.

We shall see that the basic nature of the correspondence from the last chapter will remain unchanged, but there will be some new obstacles to contend with along the way, some of which have interesting consequences.

Throughout the remainder of this chapter we shall make the following assumption. We let k be a real quadratic field of class number one, and $'$ denote conjugation in k. Further, denote by ϵ_0 the fundamental unit of k, and ϵ_+ the generator of the totally positive units, so that $\epsilon_+ = \epsilon_0$ if $\mathcal{N}(\epsilon_0) = 1$ and $\epsilon_+ = \epsilon_0^2$ if $\mathcal{N}(\epsilon_0) = -1$.

3.1 Quadratic Forms with $\mathcal{O}_k$ coefficients

Consider the binary form $Q(x,y) = ax^2 + bxy + cy^2$, with $a, b, c \in \mathcal{O}_k$. There is another form which is intimately related to $Q(x,y)$, namely, the conjugate form $Q'(x,y) = a'x^2 + b'xy + c'y^2$. If disc $Q(x,y) = \delta$, then disc $Q'(x,y) = \delta'$. We shall consider forms where both $\delta < 0$ and $\delta' < 0$. In this case, we say that δ is totally negative and denote this by $\delta \ll 0$.

Since our coefficients are real numbers, we can still give meaning to positive definite forms, and therefore we take $a > 0$. However, $Q'(x,y)$ will be either positive definite or negative definite, depending on whether $a' > 0$ or $a' < 0$. If $\mathcal{N}(\epsilon_0) = -1$, then we may consider only those forms where a and a' are positive. Without units of norm -1, we can only assume that $a > 0$. We therefore make the following definition.

Definition *Let $Q(x,y) = ax^2 + bxy + cy^2$, and $\mathrm{disc}(Q(x,y)) = \delta \ll 0$. If $\mathcal{N}(a) > 0$ we say $Q(x,y)$ is type +/+. If $\mathcal{N}(a) < 0$ then we say $Q(x,y)$ is type +/-.*

As before, it will be helpful to consider a form as a matrix, and we use the form and the matrix interchangeably. We give the following definition of equivalence in terms of a matrix equation.

Definition *Two quadratic forms, $Q(x,y)$, $\widehat{Q}(x,y)$, with $\mathcal{O}_k$ coefficients are equivalent, denoted, $Q(x,y) \sim \widehat{Q}(x,y)$, if*

$$Q = (\epsilon_+)^n * {}^tA\widehat{Q}A \tag{3.1}$$

for some matrix A, with $A \in \mathrm{GL}_2(\mathcal{O}_k)^{++}$, and some $n \in \mathbb{Z}$, where

$$\mathrm{GL}_2(\mathcal{O}_k)^{++} = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \; | a, b, c, d \in \mathcal{O}_k, \; ad - bc = \epsilon_+^m \right\}. \tag{3.2}$$

One might be curious as to why we allow multiplication by totally positive units. We include this condition because we would like the forms $Q(x,y)$ and $\epsilon_+Q(x,y)$ to be equivalent. Although these forms do not have the same discriminant, their discriminants generate the same ideal in $\mathcal{O}_k$, and furthermore, $k(\sqrt{\mathrm{disc}(Q)})$ and $k(\sqrt{\mathrm{disc}(\epsilon_+ Q)})$ are the same field.

When $\epsilon_+ = \epsilon_0^2$, the equivalence of Q and $\epsilon_+ Q$ can be accomplished without the use of this multiplication:

$$Q \sim \begin{pmatrix} \epsilon_0 & 0 \\ 0 & \epsilon_0 \end{pmatrix} Q \begin{pmatrix} \epsilon_0 & 0 \\ 0 & \epsilon_0 \end{pmatrix} = \epsilon_+ * Q.$$

However, when $\mathcal{N}(\epsilon_0) = 1$, there is no matrix in $\mathrm{GL}_2(\mathcal{O}_k)^{++}$ which acts like multiplication by $\epsilon_+ = \epsilon_0$ and so the multiplication is necessary.

3.2 Ideals in $k(\sqrt{\Delta})$

We now momentarily turn our attention to the ideal side of the correspondence. Let $K = k(\sqrt{\Delta})$ with $\Delta \ll 0$. We let $^{-}$ denote complex conjugation, that is, the nontrivial conjugation of K/k. Throughout, we are going to be faced with choosing a generator for principal ideals- specifically the relative norms of ideals of K. To deal with this problem, we shall fix a relative integral basis $[1, \Omega]_{\mathcal{O}_k}$ for $\mathcal{O}_K$, where we have chosen $\Omega \in \mathfrak{h}$, and further choose $\Omega' \in \mathfrak{h}$, where $[1, \Omega']$ is a relative integral basis for the conjugate field. All definitions will then depend on this choice of basis. We shall choose as the generator of the relative field discriminant

$$\delta(K/k) = \delta = \det \left| \begin{pmatrix} 1 & \Omega \\ 1 & \bar{\Omega} \end{pmatrix} \right|^2, \tag{3.3}$$

and will use δ in all calculations.

We have by Proposition 1.7 that ideals of K have relative integral bases. In addition, if $\mathfrak{a} = [\alpha, \beta]_{\mathcal{O}_k}$, then the conjugate ideal $\mathfrak{a}' = [\alpha', \beta']_{\mathcal{O}_k}$. In light of Proposition 1.8, we choose $\det(M)$ as the generator of $\mathcal{N}(\mathfrak{a})$, and $\det(M')$ as the generator for $\mathcal{N}(\mathfrak{a}')$ to be used in all calculations. We point out that for a principal ideal (γ), this method of choosing a generator gives $\mathcal{N}((\gamma)) = \mathcal{N}(\gamma)$. In other words, we use the norm of an element as the generator of the norm of the ideal generated by that element.

Finally, we will always order α and β such that $\frac{\beta}{\alpha} \in \mathfrak{h}$. If $\mathcal{N}(\epsilon_0) = -1$, then we can further require that $\frac{\beta'}{\alpha'} \in \mathfrak{h}$. If on the other hand, $\mathcal{N}(\epsilon_0) = 1$, there are two distinct cases, as with our forms.

Definition *When $\mathcal{N}(\epsilon_0) = -1$, let $\mathfrak{a}$ be an ideal of K, with $\mathfrak{a} = [\alpha, \beta]$ such that $\frac{\beta}{\alpha} \in \mathfrak{h}$. If $\frac{\beta'}{\alpha'} \in \mathfrak{h}$ we say that $\mathfrak{a}$ is a type +/+ ideal. If $\frac{\beta'}{\alpha'} \notin \mathfrak{h}$ we say $\mathfrak{a}$ is a type +/- ideal.*

3.3 From ideals to forms

We shall now begin to set up the correspondence between forms and ideals. We start by identifying an ideal of K with a quadratic form. This is accomplished by identifying $a = [\alpha, \beta] = [1, \Omega]M$ with $Q_{\mathfrak{a}}(x, y)$ where:

$$\begin{aligned} Q_{\mathfrak{a}}(x,y) &= \frac{1}{\mathcal{N}(\mathfrak{a})}\mathcal{N}(\alpha x + \beta y) \\ &= \frac{1}{\det M}\mathcal{N}(\alpha x + \beta y) \\ &= ax^2 + bxy + cy^2. \end{aligned} \tag{3.4}$$

The Kronecker Content Theorem assures us that $a, b, c \in \mathcal{O}_k$. We now prove a series of propositions which will help us prove the correspondence theorem.

Proposition 3.1 *$Q_{\mathfrak{a}}(x, y)$ has discriminant δ, where δ is given in (3.3).*

Proof.

$$\begin{aligned} b^2 - 4ac &= \frac{1}{\mathcal{N}(\mathfrak{a})^2}(\alpha\bar{\beta} + \bar{\alpha}\beta)^2 - 4\alpha\bar{\alpha}\beta\bar{\beta}) \\ &= \frac{1}{\mathcal{N}(\mathfrak{a})^2}(\alpha\bar{\beta} - \bar{\alpha}\beta)^2 \\ &= \delta. \end{aligned}$$

The last equality comes from taking determinants in (1.8) and the fact we are using $\det(M)$ as the value of $\mathcal{N}(\mathfrak{a})$. $\square$

Proposition 3.2 *The equivalence class of $Q_{\mathfrak{a}}(x, y)$ is independent of choice of integral basis for $\mathfrak{a}$.*

Proof.

Let $\mathfrak{a} = [\widehat{\alpha}, \widehat{\beta}]$, be a second integral basis for $\mathfrak{a}$, with $[\widehat{\alpha}, \widehat{\beta}] = [1, \Omega]\widehat{M}$.

$$\widehat{Q}(\widehat{x}, \widehat{y}) = \widehat{a}\widehat{x}^2 + \widehat{b}\widehat{x}\widehat{y} + \widehat{c}\widehat{y}^2 = \frac{1}{\det \widehat{M}} \mathcal{N}\left(\begin{pmatrix} \widehat{y} & \widehat{x} \end{pmatrix} \begin{pmatrix} \widehat{\beta} \\ \widehat{\alpha} \end{pmatrix}\right).$$

We have by Proposition 1.6,

$$\begin{pmatrix} \widehat{\beta} \\ \widehat{\alpha} \end{pmatrix} = A \begin{pmatrix} \beta \\ \alpha \end{pmatrix}$$

where $\det\, A = \epsilon$. Therefore

$$\widehat{Q}(\widehat{x}, \widehat{y}) = \frac{1}{\det A \ \det\, M} \mathcal{N}\left(\begin{pmatrix} \widehat{y} & \widehat{x} \end{pmatrix} A \begin{pmatrix} \beta \\ \alpha \end{pmatrix}\right).$$

By making the determinant ϵ change of variables

$$\begin{pmatrix} y & x \end{pmatrix} = \begin{pmatrix} \widehat{y} & \widehat{x} \end{pmatrix} A$$

we have

$$\begin{aligned} \widehat{Q}(\widehat{x}, \widehat{y}) &\sim \frac{1}{\det A \ \det M} \mathcal{N}\left(\begin{pmatrix} y & x \end{pmatrix} \begin{pmatrix} \beta \\ \alpha \end{pmatrix}\right) \\ &= \frac{1}{\epsilon} Q(x, y). \end{aligned}$$

Since equivalence of forms allows for multiplication by a totally positive unit,

$$\widehat{Q}(\widehat{x}, \widehat{y}) \sim Q(x, y).$$

$\square$

One can see that without allowing equivalent forms to differ by a totally positive unit, when $\epsilon_+ = \epsilon_0$, two different choice of basis for the same ideal would lead to two inequivalent forms.

Proposition 3.3 *Let* $\mathfrak{b}$ *and* $\mathfrak{a}$ *be two ideals of* K *in the same ideal class. Then* $Q_{\mathfrak{a}}(x, y) \sim Q_{\mathfrak{b}}(x, y)$.

Proof.

If $\mathfrak{b}$ is an ideal in the same class as $\mathfrak{a}$, $\mathfrak{b} = (\gamma)\mathfrak{a}$, for some γ; so if $\mathfrak{a} = [\alpha, \beta]$, $\mathfrak{b} = [\gamma\alpha, \gamma\beta]$, thus:

$$\begin{aligned} Q_{\mathfrak{b}}(x, y) &= \frac{1}{\mathcal{N}(\mathfrak{b})}\mathcal{N}(\gamma\alpha x + \gamma\beta y) \\ &= \frac{1}{\mathcal{N}((\gamma)\mathfrak{a})}\mathcal{N}(\gamma)\mathcal{N}(\alpha x + \beta y) \\ &= \frac{1}{\mathcal{N}(\mathfrak{a})}\mathcal{N}(\alpha x + \beta y) \\ &= Q_{\mathfrak{a}}(x, y). \end{aligned}$$

□

3.4 From forms to ideals

Given a quadratic form $Q(x, y) = ax^2 + bxy + cy^2$ of discriminant δ, we will identify it with an ideal of K by

$$Q(x, y) \to \mathfrak{a} = (a, a\theta), \tag{3.5}$$

where

$$\theta = \frac{b + \sqrt{\delta}}{2a}.$$

It can be shown that $a\theta$ is an element of $\mathcal{O}_K$. In fact it is an easy calculation to verify that $a\theta$ satisfies the polynomial $x^2 + bx + \frac{b^2-\delta}{4}$, and since $\delta = b^2 - 4ac$ implies $\frac{b^2-d}{4}$ is an integer, $a\theta$ satisfies a monic polynomial with integer coefficients.

Again, we shall prove a series of propositions concerning the relationship of forms to ideals which we need to prove Theorem 3.7.

Proposition 3.4 $(a, a\theta) = [a, a\theta]_{\mathcal{O}_k}$.

Proof.

Let $\mathfrak{a} = (a, a\theta)$. By Proposition 1.6, $\mathcal{N}(\mathfrak{a})$ is the greatest common divisor of the coefficients of $\mathcal{N}(ax + a\theta y) = aQ(x, y)$. Thus, $\mathcal{N}(\mathfrak{a}) = a * \gcd(a, b, c)$, and $a \mid \mathcal{N}(\mathfrak{a})$. Also, by Proposition 1.8 $\mathcal{N}(\mathfrak{a}) \mid \det(M)$ where:

$$\begin{pmatrix} a & a\theta \\ a & a\bar{\theta} \end{pmatrix} = \begin{pmatrix} 1 & \omega \\ 1 & \bar{\omega} \end{pmatrix} M.$$

Taking determinants and squaring we see

$$\begin{aligned} (a^2\bar{\theta} - a^2\theta)^2 &= \delta \det(M)^2, \\ a^2\delta &= \delta \det(M)^2, \\ a^2 &= \det(M)^2, \\ a &= \det(M). \end{aligned}$$

Thus we have $a \mid \mathcal{N}(\mathfrak{a}) \mid \det(M) = a$, so $\mathcal{N}(\mathfrak{a}) = \det(M)$, and by Proposition 1.8 $(a, a\theta) = [a, a\theta]$. $\square$

We now verify that the ideal class given by (3.5) is independent of the representative of the form class.

Proposition 3.5 *Let $Q(x, y)$ and $\widehat{Q}(x, y)$ be equivalent forms with $\mathcal{O}_k$ coefficients, with corresponding ideals $\mathfrak{a} = [a, a\theta]$, and $\widehat{\mathfrak{a}} = [\widehat{a}, \widehat{a}\widehat{\theta}]$. Then $\mathfrak{a}$ and $\widehat{\mathfrak{a}}$ are in the same ideal class.*

Proof.

We define ψ as in (2.6),

$$\psi = -\bar{\theta} = \frac{-b + \sqrt{\delta}}{2a}.$$

Noting that $Q(\psi, 1) = 0$, we have

$$\begin{pmatrix} \psi & 1 \end{pmatrix} \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} \begin{pmatrix} \psi \\ 1 \end{pmatrix} = 0. \tag{3.6}$$

Now if $M = \begin{pmatrix} r & s \\ t & u \end{pmatrix}$ is the matrix that takes $\widehat{Q}(x, y)$ to $Q(x, y)$, we saw in section 2.4 that $\widehat{\psi} = M\psi$.

Also,

$$\widehat{\theta} = -\overline{(\widehat{\psi})} = \frac{-(r\bar{\psi} + s)}{t\bar{\psi} + u} = \frac{r(-\bar{\psi}) - s}{-t(-\bar{\psi}) + u} = \frac{r\theta - s}{-t\theta + u}.$$

As a result, $\mathfrak{a} = [a, a\theta]$ and $\widehat{\mathfrak{a}} = [\widehat{a}, \widehat{a}\widehat{\theta}]$ are in the same ideal class, because

$$\begin{pmatrix} r & -s \\ -t & u \end{pmatrix} \begin{pmatrix} a\theta \\ a \end{pmatrix} = C * \begin{pmatrix} \widehat{a}\widehat{\theta} \\ \widehat{a} \end{pmatrix}, \text{ where } C = \frac{a\,(-t\theta + u)}{\widehat{a}},$$

so that $[a, a\theta]$ and $C * \widehat{\mathfrak{a}}$ are the same ideal. $\square$

Proposition 3.6 *Let $Q(x, y) = ax^2 + bxy + cy^2 = (x + \theta y)(x + \bar{\theta} y)$, and $\mathfrak{a} = [a, a\theta]$. Then $Q(x, y) = Q_{\mathfrak{a}}(x, y)$. Thus, equations (3.7) and (3.8) below are inverses.*

Proof.

From equation (3.4) we see:

$$\begin{aligned} Q_{\mathfrak{a}}(x, y) &= \frac{1}{\mathcal{N}(\mathfrak{a})} \mathcal{N}(ax + a\theta y) \\ &= \frac{1}{a}(a^2x^2 + abxy + acy^2) \\ &= ax^2 + bxy + cy^2 \\ &= Q(x, y). \end{aligned}$$

$\square$

We are now in a position to state and prove the theorem which which was the goal of the chapter.

Theorem 3.7 *Let k be a class number 1 real quadratic field, and let K be a totally complex quadratic extension of k. Let δ be a generator of the discriminant of K/k chosen as in (3.3). There exists a one to one correspondence between ideal classes in K and equivalence classes of positive definite quadratic forms with coefficients in $\mathcal{O}_k$ and discriminant $\epsilon^2\delta$, where ϵ is a totally positive unit, and equivalence of quadratic forms is given in (3.1). The correspondence is given by the following two maps,*

$$\mathfrak{a} = [\alpha, \beta] \longrightarrow \frac{1}{\mathcal{N}(\mathfrak{a})}\mathcal{N}(\alpha x + \beta y), \tag{3.7}$$

$$ax^2 + bxy + cy^2 \longrightarrow \left[a, \frac{b + \sqrt{b^2 - 4ac}}{2}\right]. \tag{3.8}$$

Proof.

Let us verify that the sequence of propositions from this chapter give us our result. First we have seen that equation (3.7) does in fact give a form of discriminant δ by Proposition 3.1, and (3.8) gives an ideal class in $k(\sqrt{\delta})$. Further, the equivalence class of the form in (3.7) is independent of the choice of representative of an ideal class by Proposition 3.3, and also independent of the choice of integral basis for that ideal from Proposition 3.2. Conversely, the ideal class of the ideal in (3.8) is independent of the choice of the form from an equivalence class by Proposition 3.5. Finally, Proposition 3.6 gives us that (3.7) and (3.8) are inverses, completing the theorem. $\square$

3.5 Examples

We will now give two examples explicitly giving the identification between quadratic forms and ideals. The first example has $\epsilon_+ = \epsilon_0^2$ where all ideals are $+/+$. The second example has $\epsilon_+ = \epsilon_0$, and an example of both a $+/-$ and a $+/+$

ideal are given. We will be using some facts about factoring ideals and finding integral bases for ideals which are useful only in constructing examples. For more insight one should consult [10] or [3].

Example 1

$k = \mathbb{Q}(\sqrt{5})$, $\mathcal{O}_k = \left[1, \frac{1+\sqrt{5}}{2}\right]_{\mathbb{Z}} = [1, \omega]$, $\epsilon_0 = \omega$, $\epsilon_+ = \epsilon_0^2$.
$K = k(\sqrt{-19})$, $\mathcal{O}_K = \left[1, \frac{1+\sqrt{-19}}{2}\right]_{\mathcal{O}_k} = [1, \Omega]$.

We factor the ideal (19) in k as $(19) = \mathfrak{p}_{19}\mathfrak{p}'_{19}$. Further in K, $\mathfrak{p}_{19} = \mathfrak{P}_{19}^2$ and we have

$$\mathfrak{P}_{19} = [4 + \omega, -63 - 18\omega + \Omega]_{\mathcal{O}_k}.$$

The corresponding norm form is

$$(4 + \omega)x^2 + (-125 - 36\omega)xy + (979 + 319\omega)y^2.$$

If we started with the form $7x^2 - 3xy + y^2$, we see that this corresponds to the ideal $\mathfrak{P}_7 = [7, \frac{3+\sqrt{-19}}{2}] = [7, 1 + \Omega]$, where (7) is prime in k and $(7) = \mathfrak{P}_7\bar{\mathfrak{P}}_7$ in K.

Example 2

$k = \mathbb{Q}(\sqrt{3})$, $\mathcal{O}_k = [1, 3]_{\mathbb{Z}} = [1, \omega]$, $\epsilon_0 = \epsilon_+ = 2 + \omega$.
$K = k(\sqrt{-23})$, $\mathcal{O}_K = \left[1, \frac{1+\sqrt{-23}}{2}\right]_{\mathcal{O}_k} = [1, \Omega]$.

In k, the ideal $(47) = \mathfrak{p}_{47}\mathfrak{p}'_{47}$; $\mathfrak{p}_{47} = \mathfrak{P}_{47}\bar{\mathfrak{P}}_{47}$, and $\mathfrak{p}'_{47} = \mathfrak{P}'_{47}\bar{\mathfrak{P}}'_{47}$, where we may take

$$\mathfrak{P}_{47} = [-1 + 4\omega, -161 - 23\omega + \Omega].$$

Notice that this is a $+/-$ ideal. The corresponding norm form is

$$(-1 + 4\omega)x^2 + (321 - 46\omega)xy + (2467 + 2485\omega)y^2.$$

Also in k, (29) is prime, and in K $(29) = \mathfrak{P}_{29}\bar{\mathfrak{P}}_{29}$.

$$\mathfrak{P}_{29} = [29, 387 + 87\omega + \Omega]$$

This is a $+/+$ ideal. The norm form is

$$29x^2 + (775 + 174\omega)xy + (5961 + 2325\omega)y^2.$$

Chapter 4

The Hilbert modular group

The notion of the action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathfrak{h}$ can be generalized to the case of the general number field. We shall be interested in the action of $\mathrm{GL}_2(\mathcal{O}_k)^{++}$ where k is a real quadratic field, and in particular how to use this action to reduce quadratic forms and compute class numbers. For a detailed treatment of the general number field case, see [11].

4.1 The action of $\mathrm{GL}_2(\mathcal{O}_k)^{++}$ on $\mathcal{H}$

For a real quadratic field k, the natural action of $\mathrm{GL}_2(\mathcal{O}_k)^{++}$ is on $\mathcal{H} = \mathfrak{h} \times \mathfrak{h}$. For $\mathbf{z} = (z_1, z_2) = (x_1 + iy_1, x_2 + iy_2)$, the action is given by:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mathbf{z} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} (z_1, z_2) = \left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} z_1, \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} z_2 \right), \tag{4.1}$$

where $'$ is used to denote conjugation in k, and the action is the usual $\mathrm{GL}_2(\mathbb{R})$ action on $\mathfrak{h}$ as defined in (1.9).

If k has fundamental unit of norm -1, then this action is the same as the action of determinant 1 matrices. For if $A \in \mathrm{GL}_2(\mathcal{O}_k)^{++}$, and $\det(A) = \epsilon_0^{2n}$, then

$A = \begin{pmatrix} \epsilon_0^n & 0 \\ 0 & \epsilon_0^n \end{pmatrix} A_0$, where $\det(A_0) = 1$. Therefore,

$$A\mathbf{z} = \begin{pmatrix} \epsilon_0^n & 0 \\ 0 & \epsilon_0^n \end{pmatrix} A_0\mathbf{z} = A_0\mathbf{z},$$

since it is clear from (4.1) that scalar matrices act trivially. Such a decomposition is not possible when $\mathcal{N}(\epsilon_0) = 1$.

It will be useful to treat z_1 and z_2 as conjugates in the formal sense. We define a formal norm for all $\alpha \in \mathcal{O}_k$ and $z \in \mathcal{H}$,

$$\mathcal{N}(\alpha\mathbf{z}) = (\alpha z_1)(\alpha' z_2).$$

We have that

$$|\mathcal{N}(\mathbf{z})|^2 = |z_1 z_2|^2 = (x_1^2 + y_1^2)(x_2^2 + y_2^2).$$

By the "height" of an element $\mathbf{z} \in H$ we shall mean

$$\mathcal{N}(\mathbf{y}) = |y_1 y_2|. \tag{4.2}$$

One may derive the following formula, similar to (1.10):

$$\mathcal{N}(A\mathbf{y}) = \frac{\mathcal{N}(ad - bc)\mathcal{N}(\mathbf{y})}{|\mathcal{N}(cz + d)|^2}. \tag{4.3}$$

4.2 The fundamental domain of $\mathrm{GL}_2(\mathcal{O}_k)^{++}$

Following the method demonstrated by Stark in [11], One can construct a fundamental domain for $\mathrm{GL}_2(\mathcal{O}_k)^{++}$ by the "highest point method." This essentially involves the following.

1. By use of $\begin{pmatrix} \epsilon_+ & 0 \\ 0 & 1 \end{pmatrix}$ one can fix the value of $\mathcal{N}(y)$, while altering the values of y_1, y_2 such that $\epsilon_+^{-1} \leq |\frac{y_1}{y_2}| \leq \epsilon_+$.

2. By applying $\begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}$ matrices one can put (x_1, x_2) inside a parallelogram (or other suitably chosen region) determined by 1 and ω.

3. By (4.3) we see that when $|\mathcal{N}(c\mathbf{z}+d)| < 1$ we raise the height of $\mathbf{z}$. This is equivalent to the condition that
$$\left|\mathcal{N}\left(\mathbf{z}+\frac{d}{c}\right)\right| < \left|\frac{1}{\mathcal{N}(c)}\right|.$$
We think of this collection of points as the "sphere" centered at $-\frac{d}{c}$ of "radius" $|\frac{1}{\mathcal{N}(c)}|$. There will be a collection of such spheres which will form the floor of the fundamental domain. According to Cohn in [5], $\mathbb{Q}(\sqrt{5})$ is the only field that has only spheres of radius 1. Because of this, the floor is a complicated structure, and not easily examined in general. This is a problem which will be confronted in what is to come.

4.3 Boundary identifications

The fundamental domains for three small real quadratic fields were worked out by Claus in [2]. However, he does not consider the boundary identifications. He does suggest, like Cohn, that the floor is a complicated structure. To be able to reduce forms and calculate class numbers, it will be necessary to know when two forms are equivalent. For this reason, we need to at the very least observe the nature of the boundary identifications.

It turns out that the three types of boundaries mentioned above (corresponding to each step in the reduction) identify with only boundaries of the same type- that is, translational boundaries identify with translational boundaries, unit boundaries with unit boundaries, and floor boundaries with floor boundaries.

This is fairly clear for the translational boundaries. If $\mathcal{O}_k = [1, \omega]$, the two fundamental translations are $T_1 = (1, 1)$ and $T_2 = (\omega, \omega')$. If one centers a parallelogram about the origin in the x_1x_2 plane, one gets the following boundary conditions associated with translations:

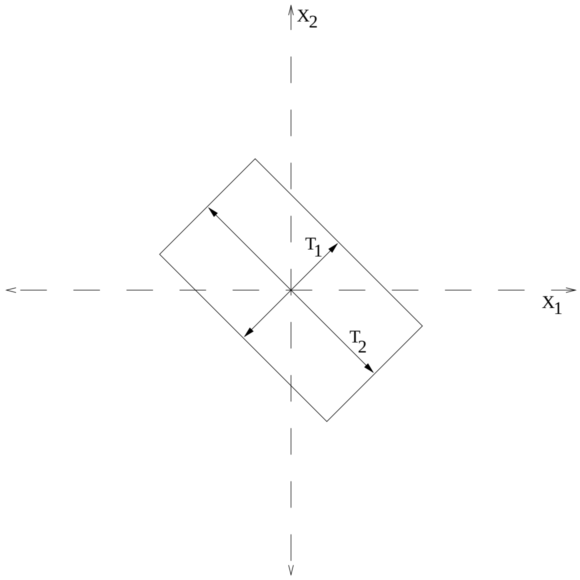

Figure 4.1: Translational Fundamental Domain

$$-\frac{\omega-\omega'}{2} \leq x_2 - x_1 < \frac{\omega-\omega'}{2}; -\frac{\omega-\omega'}{2} \leq \omega x_2 - \omega' x_1 < \frac{\omega-\omega'}{2}$$

Obviously, opposite sides of the parallelogram are equivalent under the appropriate translation, as shown in Figure 4.1.

The second type of boundary occurs when $\mathbf{z}$ is in the interior of the parallelogram, above the floor, and $|\frac{y_1}{y_2}| = \epsilon_+^{-1}$ or $|\frac{y_1}{y_2} = \epsilon_+|$. These two regions identify with each other in pieces in the following way. Suppose $\mathbf{z} = (z_1, z_2)$ and $\frac{y_1}{y_2} = \epsilon_+^{-1}$. Now consider the point $\mathbf{z}^* = \begin{pmatrix} \epsilon_+ & 0 \\ 0 & 1 \end{pmatrix} z$. We have

$$\begin{aligned} \left|\frac{y_1^*}{y_2^*}\right| &= \left|\frac{\epsilon_+ y_1}{\epsilon_+' y_2}\right| \\ &= \epsilon_+^2 \left|\frac{y_1}{y_2}\right| \\ &= \epsilon_+. \end{aligned}$$

If $|\mathcal{N}(c\mathbf{z} + d\epsilon_+^{-1})| > 1$ then $|\mathcal{N}(c\mathbf{z}^* + d)| > 1$, since these two norms are equal; i.e., if $\mathbf{z}$ was above the floor, then so is $\mathbf{z}^*$. However, $\mathbf{z}^*$ is probably no longer inside the fundamental domain for translations. Let us investigate what happens to (x_1, x_2). Observe x_1 is stretched by a factor of ϵ_+ (which is greater than 1), and x_2 is compressed by a factor of $\epsilon_+{}'$ (which is less than 1). Our parallelogram becomes skewed. This skewed parallelogram is translationally equivalent to our original parallelogram in polygonal pieces. This is illustrated in Figures 4.2, 4.3, and 4.4.

Of course, the region need not be a parallelogram, but only a translational fundamental domain. The only concern one would have is that two pieces may overlap. This is not possible. Let x, w be two points in the interior $\mathcal{F}_T$ (we have dealt with the boundary of the parallelogram). If $\epsilon_+ x = \epsilon_+ w + \alpha$ for some α, (that is, two points in the skewed parallelogram are translationally equivalent), then we would have $x = w + (\epsilon_+)'\alpha$ making x and w translationally equivalent, which is impossible, as they are in the interior of the parallelogram.

We are left only with the floor, which by exhaustion, must identify with itself. In what manner this occurs, however, is not easily seen. We have not found any way to consider the floor as to find all the boundary identifications. Part of the problem is a visualization one- the floor is a three dimensional object which occupies four dimensions. More serious however is the complexity of the floor, which Cohn examined in [5]. The result of this complexity is that special care must be taken to distinguish whether two points on the floor boundary are equivalent. We shall mention how to deal with this problem in terms of our forms in a later section.

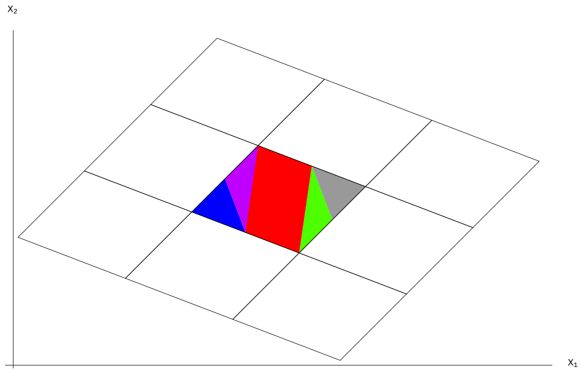

Figure 4.2: Unit Boundary in $Q(\sqrt{5})$ with $\frac{y_2}{y_1} = \epsilon_+$

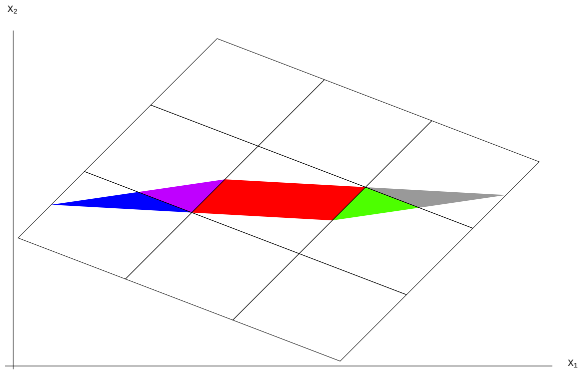

Figure 4.3: Altered Unit Boundary in $Q(\sqrt{5})$ with $\frac{y_2}{y_1} = \epsilon_+^{-1}$

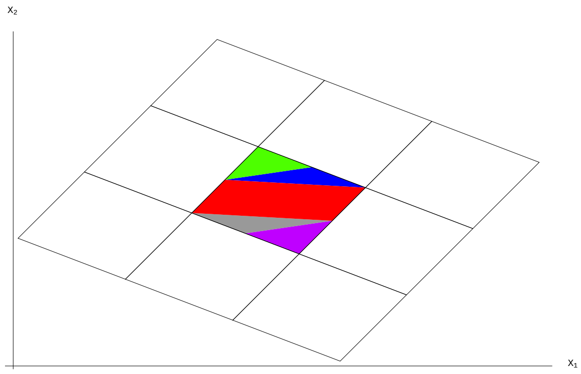

Figure 4.4: Unit Boundary in $Q(\sqrt{5})$ with $\frac{y_2}{y_1} = \epsilon_+^{-1}$

Chapter 5

Reducing quadratic forms with $\mathcal{O}_k$ coefficients

5.1 Identification of forms with points in $\mathcal{H}$

We will now demonstrate how to pick a representative quadratic form in each equivalence class. We saw how quadratic forms with negative discriminant could be identified with a point in the complex upper half plane. In a similar manner we now identify our new forms with a point in the Hilbert upper half plane by

$$ax^2 + bxy + cy^2 \longleftrightarrow \left(\frac{-b + \sqrt{\delta}}{2a}, \frac{-b' + \sqrt{\delta'}}{2a'} \right). \tag{5.1}$$

Some care needs to be taken when $\epsilon_+ = \epsilon_0$, since in this case there may be $+/-$ forms. When this occurs, we are identifying such a form with a point in $\mathfrak{h} \times \mathfrak{h}^-$ (by $\mathfrak{h}^-$ we mean $\{x + iy \in \mathbb{C} \mid y < 0\}$). Of course, $\mathrm{GL}_2(\mathcal{O}_k)^{++}$ acts on this set as well, and it will send points in $\mathfrak{h} \times \mathfrak{h}^-$ to points in $\mathfrak{h} \times \mathfrak{h}^-$. It turns out that one may use the same conditions to describe a fundamental domain for this action as well. Obviously, the translational boundaries are not effected. One can still use the same unit boundary condition, with the understanding that the ratio is to be taken positively. Finally, by taking the absolute value of the height, we will be able to construct the same highest point fundamental domain that we used for the action on $\mathcal{H} = \mathfrak{h} \times \mathfrak{h}$. Equivalently, we may identify a $+/-$ form with $\left(\frac{-b+\sqrt{\delta}}{2a}, \frac{-b'-\sqrt{\delta'}}{2a'}\right)$, which is in $\mathcal{H}$.

5.2 Reducing forms with $\mathcal{O}_k$ entries

At the end of the section 3.4, we saw that if we consider equivalent forms, $\widehat{Q} = {}^tMQM$ then $\widehat{\psi} = M\psi$. By acting on (ψ, ψ') by a linear fractional transformation, we find an equivalent form and conjugate whose roots are in the fundamental domain.

Definition *A quadratic form $Q(x, y)$ is called reduced if its roots (ψ, ψ') are in $\mathcal{F}$. For $+/-$ forms, this means that $(\psi, \bar{\psi}') \in \mathcal{F}$.*

We have seen how to determine the point which lies in the fundamental domain in the same orbit of a given point in the construction of the highest point fundamental domain. We give the equivalent algorithm in terms of forms.

1. Test whether $\epsilon_+^{-1} \leq \left|\frac{a\sqrt{\delta'}}{a'\sqrt{\delta}}\right| \leq \epsilon_+$, and apply $\begin{pmatrix} \epsilon_+ & 0 \\ 0 & 1 \end{pmatrix}^j$ for appropriate j if needed.

2. Test whether $(\frac{-b}{2a}, \frac{-b'}{2a'})$ is within the translational boundary. Apply $\begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}$ if not to make this so.

3. For each sphere comprised in the floor with center t and radius $|\mathcal{N}(u)|$ (it is the case that t and u are relatively prime), test whether $\left|\mathcal{N}\left(\frac{b\frac{t}{u}+a\frac{t^2}{u^2}+c}{a}\right)\right| \geq \left|\frac{1}{\mathcal{N}(u)^2}\right|$. Notice that for the simplest case $t = 0, u = 1$, the condition becomes $\mathcal{N}(a) \leq \mathcal{N}(c)$. If so, stop, making note if equality holds. Otherwise apply a totally positive unit matrix of the form $\begin{pmatrix} * & * \\ t & u \end{pmatrix}$. and return to step one. One can construct such a matrix by solving the equation $tx + uy = 1$.

Chapter 6

Class Number Calculations

6.1 Bounding the Search

In order to use our forms to calculate class numbers, we would like some bound on our search region, analogous to the condition $b < \sqrt{\frac{|d|}{3}}$ in the classical case. We do this by noting that the floor of the fundamental domain bounds $\mathcal{N}(y)$ sufficiently away from zero. Also, since the ratio of y_1 and y_2 is bounded, we can find a minimal value M for y_1. This means that

$$\begin{aligned} M &\leq \frac{\sqrt{\delta}}{2a} \text{ so that} \\ a &\leq \frac{\sqrt{\delta}}{M}. \end{aligned}$$

One can further use the relation between b and a from the translational fundamental domain in turn to get a maximal value for b. Cohn in [4] found values for the lowest points in the fundamental domains which were useful in computation.

6.2 Implementation of Algorithm with KASH

In order to expedite the calculations, the algorithm was implemented using KASH v. 1.9 [6], an algebraic number theory package developed at T.U. Berlin.

Programs were written to both reduce forms and make class number calculations. There is a certain amount of initialization that must be done which depends on the field. We restricted to the cases of $k = \mathbb{Q}(\sqrt{3})$ and $k = \mathbb{Q}(\sqrt{5})$ which cover both the unit of norm 1 and -1 cases respectively. The initial parameters needed were

1. An integral basis for $\mathcal{O}_k$.
2. The fundamental unit of $\mathcal{O}_k$.
3. The spheres comprising the floor of the fundamental domain for $\mathrm{GL}_2(\mathcal{O}_k)^{++}$, taken from [2].
4. A bound for M, the minimal value of y_1, from [4].

With those parameters in place, one does the following.

1. For all possible b, one factors the ideal $\frac{|\delta|+b^2}{4} = \mathfrak{a}\mathfrak{c}$ where $\mathcal{N}(\mathfrak{a}) \leq \mathcal{N}(\mathfrak{c})$ using the KASH function **IdealFactors**.
2. One then finds a positive generator a of the ideal $\mathfrak{a}$, which satisfies the unit boundary conditions. Notice that at most one can possibly work.
3. Find the number $c = \frac{b^2+|\delta|}{4a}$, and create the form $ax^2 + bxy + cy^2$.
4. If the form is reduced, add it to the list of reduced forms, and note if form is on a floor boundary.
5. When complete, check to see if forms on floor are equivalent.

The last step is non-trivial and deserves elaboration, which we provide in the next section.

6.3 Distinguishing points on the boundary

As we have noted, the floor boundaries are not very easy to study, and as a result the boundary relations related to the floor are not known. This presents a problem when counting reduced forms as we must determine whether two forms on the boundary are equivalent. The following method was used to determine equivalence of forms on the boundary.

There are two obvious ways 2 forms on the boundary can be equivalent. The first way is for the two forms to correspond to conjugate ideals, $\mathfrak{a}$ and $\bar{\mathfrak{a}}$, where $\mathfrak{a}$ has order 2 in the class group. Since $\mathcal{N}(\mathfrak{a}) = \mathfrak{a}\bar{\mathfrak{a}}$ is principal, $[\bar{\mathfrak{a}}] = [\mathfrak{a}^{-1}]$, so if $\mathfrak{a}$ has order 2, $[\mathfrak{a}] = [\mathfrak{a}^{-1}] = [\bar{\mathfrak{a}}]$. It is an easy matter to test this for all forms on the boundary. We find the ideal $\mathfrak{a}$ corresponding to the form on the boundary and find $Q_{\mathfrak{a}^2}(x, y)$ as in (3.8). We reduce this form, and if it is the principal form, our original form has order two. We shall see an example shortly.

The second way for two forms to be equivalent, is if they are related by the change of variables $(x, y) \to (-y, x)$. In terms of forms, we will see $ax^2 + bxy + cy^2$ and $cx^2 - bxy + ay^2$. This can be done by inspection instantly.

If this is insufficient, one can of course exhaustively check whether or not two forms are equivalent. Empirically, it was rarely the case that this was needed.

6.4 Examples

We use the same fields as we did in the examples at the end of chapter 4.

Example 1

$k = \mathbb{Q}(\sqrt{5})$, $K = k(\sqrt{-19})$.

We use all the same notation as in Example 1 from section 3.5. The fundamental domain of $\mathrm{GL}_2(\mathcal{O}_k)^{++}$ is given by the relations

$$\frac{\sqrt{5}}{2} \leq x_2 - x_1 < \frac{\sqrt{5}}{2},\ \frac{\sqrt{5}}{2} \leq \omega x_2 - \omega' x_1 < \frac{\sqrt{5}}{2},$$

$$\omega^{-2} \leq \frac{y_2}{y_1} < \omega^2,$$

$$\mathcal{N}(z) \geq 1,\ \mathcal{N}(z \pm 1) \geq 1,\ \mathcal{N}(z \pm \omega) \geq 1,\ \mathcal{N}(z \pm \omega') \geq 1.$$

Cohn in [4] gives $\frac{5^{\frac{1}{4}}}{2\omega}$ as a bound for the minimum value of y_1.

Table 6.1 shows the reduced forms returned by the KASH program. Notice that the two forms on the boundary are conjugates, and correspond to the factors of 5 in K. An easy calculation shows that they are order two, and thus equivalent. The class number of K is four. Our group is either $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}/4\mathbb{Z}$, depending on whether $(2, -1 + 2\omega, 3)$ has order 2 or not. If the corresponding ideal is $\mathfrak{P}_2$, we compute $\mathfrak{P}_2^2$, and use 3.7 to give the equivalent form. The reduction algorithm does not return the principal form and thus the class group is $\mathbb{Z}/4\mathbb{Z}$.

$(\mathbf{a}, \mathbf{b}, \mathbf{c})$	On Sphere
$(1, 1, 5)$	
$(2 + \omega, -1, 3 - \omega)$	0
$(2 + \omega, 1, 3 - \omega)$	0
$(2, -1 + 2\omega, 3)$	
$(2, 1 + 2\omega, 3 + \omega)$	

Table 6.1: Quadratic forms for $\mathbb{Q}(\sqrt{5})(\sqrt{-19})$

Example 2

$k = \mathbb{Q}(\sqrt{3}),\ K = k(\sqrt{-23})$.

The fundamental domain is given by the relations

$$-\sqrt{3} \leq x_2 - x_1 < \sqrt{3},\ -1 \leq x_2 + x_1 < 1,$$

$$\epsilon_+ \leq \frac{y_2}{y_1} < \epsilon_+,$$

$$\mathcal{N}(z) \geq 1,\ \mathcal{N}(z \pm 1) \geq 1,\ \mathcal{N}(z \pm \sqrt{3}) \geq 1,\ \mathcal{N}(z \pm \sqrt{3} \pm 2) \geq 1,\ \mathcal{N}(z \pm \sqrt{3} \pm 2) \geq 1,$$

$$\mathcal{N}\left(z + \frac{\pm 1 \pm \sqrt{3}}{2}\right) \geq \frac{1}{4},$$

$$\mathcal{N}\left(z \pm \frac{1}{\sqrt{3}}\right) \geq \frac{1}{9},\ \mathcal{N}\left(z \pm \frac{2}{\sqrt{3}}\right) \geq \frac{1}{9}.$$

Again from [4] we have $\frac{\sqrt{2-\sqrt{3}}}{2}$ as a bound for the minimum value of y_1.

Of the 15 forms in the Table 6.2, six are on the boundary. These are equivalent in conjugate pairs, as each of the forms has order 2. The class number is thus 12. The class group is one of the two following groups:

$$\mathbb{Z}/12\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}.$$

Since $\mathbb{Z}/12\mathbb{Z}$ has only 1 element of order 2, the group is $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$.

$(\mathbf{a}, \mathbf{b}, \mathbf{c})$	On Sphere
$(1, 1, 6)$	
$(2, 1, 3)$	
$(2, -1, 3)$	
$(-1+\omega, -1, 3+3\omega)$	
$(-1+\omega, 1, 3+3\omega)$	
$(\omega, -1, 2\omega)$	
$(\omega, 1, 2\omega)$	
$(3-\omega, -1+2\omega, 4+\omega)$	
$(3-\omega, 1-2\omega, 4+\omega)$	
$(2\omega, -5, 2\omega)$	0
$(2\omega, 5, 2\omega)$	0
$(-2+2\omega, -3, 2+2\omega)$	0
$(-2+2\omega, 3, 2+2\omega)$	0
$(3-\omega, -1, 3+\omega)$	0
$(3-\omega, 1, 3+\omega)$	0

Table 6.2: Quadratic forms for $\mathbb{Q}(\sqrt{3})(\sqrt{-23})$

Example 3

$k = \mathbb{Q}(\sqrt{5})$, $K = k(\sqrt{-17-4\omega})$.

Here we give an example of when K is not a normal extension of k. The discriminant of K is $\delta_K = -68 - 16\omega$.

$(\mathbf{a}, \mathbf{b}, \mathbf{c})$	On Sphere
$(5, -4+4\omega, 5)$	0
$(2+\omega, -2-2\omega, 10-\omega)$	
$(5-\omega, -2, 4+2\omega)$	
$(1, 0, 17+4\omega)$	
$(4-\omega, 0, 5+3\omega)$	
$(2, 2, 9+2\omega)$	
$(5-\omega, 2, 4+2\omega)$	
$(2+\omega, 2+2\omega, 10-\omega)$	
$(5, 4-4\omega, 5)$	0

Table 6.3: Quadratic forms for $\mathbb{Q}(\sqrt{5})(\sqrt{-68-16\omega})$

We have observed that two forms (a, b, c) and $(c, -b, a)$ are equivalent, so the class number of this field is 8. We see that there are three elements of exact order 2: $(5, 4-4\omega, 5), (4-\omega, 0, 5+3\omega)$, and $(2+\omega, 2+2\omega, 10-\omega)$. The class group is therefore $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.

Chapter 7

The effect of $+/-$ forms on the class group

7.1 Identifying $+/+$ forms and ideals

We have seen when there is no unit of norm -1, there may be $+/-$ forms and ideals. For the remainder of the chapter we assume that k has no unit of norm -1, and investigate what effect this has on the class group of the quadratic extension K. A good place to start is stating some equivalent conditions for forms or ideals to be type $+/+$.

Proposition 7.1 *Let $\mathfrak{a} = [\alpha, \beta]$ be an ideal in K and $Q_{\mathfrak{a}}(x, y) = ax^2 + bxy + cy^2$ be the corresponding quadratic form given by (3.4). The following are equivalent.*

1. *$\mathfrak{a}$ is a $+/+$ ideal.*

2. *All ideals in the ideal class of $\mathfrak{a}$ are $+/+$ ideals.*

3. *$\mathcal{N}_{K/k}(\mathfrak{a})$ is totally positive, where $\mathcal{N}(\mathfrak{a})$ is given by equation (1.8).*

4. *$Q_{\mathfrak{a}}(x, y)$ is a $+/+$ form.*

5. *All forms equivalent to $Q_{\mathfrak{a}}(x, y)$ are $+/+$ forms.*

Proof.

For 1 implies 2, notice that the relative norm of an element $\gamma = x + y\sqrt{\Delta}$ of K is $\mathcal{N}(\gamma) = x^2 + \Delta y^2$ which is totally positive. Thus, if $\mathfrak{a}$ is $+/+$, so is $(\gamma)\mathfrak{a}$. Furthermore, 2 implies 1 is trivial.

To see 1 implies 3, we first recall that $\mathcal{N}(\mathfrak{a}) = \det(M)$ and notice that (1.8) can be manipulated to give

$$\begin{pmatrix} \beta \\ \alpha \end{pmatrix} = {}^tM \begin{pmatrix} \Omega \\ 1 \end{pmatrix},$$

and so also

$$\begin{pmatrix} \beta' \\ \alpha' \end{pmatrix} = {}^tM' \begin{pmatrix} \Omega \\ 1 \end{pmatrix}.$$

We have assumed that $\frac{\beta}{\alpha} \in \mathfrak{h}$, thus $\det(M) > 0$ because $\frac{\beta}{\alpha} = {}^tM(\frac{\Omega}{1})$ as a linear transformation, and $\frac{\Omega}{1}$ lies in $\mathfrak{h}$. Similarly, $\frac{\beta'}{\alpha'} \in \mathfrak{h}$ if and only if $\det(M') > 0$.

To prove 3 implies 4, We must show a, the coefficient of x^2 is totally positive. By the correspondence (3.7) $a = \frac{\mathcal{N}(\alpha)}{\mathcal{N}(\mathfrak{a})}$. We observed that $\mathcal{N}(\alpha)$ is totally positive, so a is totally positive and $Q_{\mathfrak{a}}(x, y)$ is $+/+$.

The statement 4 implies 5 is clear because we are restricting to totally positive unit change of basis and multiplication by totally positive units. The converse, 5 implies 4, is trivial.

We have only to prove 4 implies 1. Our correspondence gives a form $ax^2 + bxy + cy^2 \longrightarrow [a, a\theta]$. The ideal $[a, a\theta]$ is $+/+$ if both θ and θ' lie in $\mathfrak{h}$. Such is the case if and only if a is totally positive; i.e. our form is $+/+$. $\square$

Of course, one could also formulate a proposition for equivalent conditions for forms and ideals to be $+/-$. The statements and the proofs are clearly analogous. It has not yet been verified, however, that $+/-$ forms exist for all totally complex quadratic extensions of k. The answer is, with one exception, affirmative.

We will need to define the concept of narrow equivalence of ideals.

Definition *Two ideals $\mathfrak{a}$ and $\mathfrak{b}$ in a quadratic field are in the same narrow ideal class if $\mathfrak{a} = (\gamma)\mathfrak{b}$ for some γ of positive norm.*

For quadratic fields, the narrow ideal classes and usual (wide) ideal classes are the same, except when the field has no units of norm -1. When there is no unit of norm -1, there are twice as many narrow classes as wide classes.

Proposition 7.2 *If K is not the narrow Hilbert class field of k, then K has ideals of type $+/-$.*

Proof.

We shall find a prime ideal with the desired property. Let p be a rational prime, which splits in k, $p = \pi\pi'$, such that $\mathcal{N}(\pi) = -p$. Such an ideal is in the class which isn't the narrow principal class. It is possible to choose such a π because every narrow ideal class contains infinitely many primes. If K is the narrow Hilbert class field, than the only prime ideals that split are ideals in the narrow principal class. Otherwise, we can further restrict our choice of p such that $\mathfrak{p}$ splits in K, $\mathfrak{p} = \mathfrak{P}\bar{\mathfrak{P}}$, and $\mathfrak{P}$ is a $+/-$ ideal. $\square$

Notice that this proposition also implies that for any non-unit discriminant, there are $+/-$ forms of that discriminant.

7.2 A family of fields with even class number

If there are $+/-$ ideals in the class group, then it is seems plausible to expect half the ideals to be $+/-$ and half to be $+/+$. Indeed this is the case.

Proposition 7.3 *Suppose K is not the narrow Hilbert class field of k. The ideals of type $+/+$ form a subgroup of index 2 in $\mathcal{C}(K)$, the class group of K.*

Proof.

Firstly, we have seen that all ideals in the the same ideal class are of the same type. Thus the map $n : \mathcal{C}(K) \to \{\pm 1\}$, given by $n([\mathfrak{a}]) = \mathrm{sign}(\mathcal{N}(\mathfrak{a}))$ is well defined, and the $+/+$ classes are the kernel of this map. $\square$

The following theorem then is an immediate corollary.

Theorem 7.4 *Let k be a real quadratic field of class number one, which contains no units of norm -1. If $K = k(\sqrt{\delta})$, $\delta \ll 0$, is not the narrow Hilbert class field of k, then the class number of K is even.*

7.3 Class groups with a cyclic factor of $\mathbb{Z}/2\mathbb{Z}$

An interesting question arises. We have only two conjugacy classes in the class group modulo $+/+$ ideals- the nontrivial one being the conjugacy class of the $+/-$ ideals. One might wonder if the class group of K has a $\mathbb{Z}/2\mathbb{Z}$ as a cyclic factor of its class group. This is analogous to asking if there is a $+/-$ ideal of order 2. In that case, all the $+/-$ ideal classes can be achieved by multiplying a $+/+$ ideal by the $+/-$ ideal of order 2. One can construct rather easily a family of biquadratic fields with such a class group. For example, if $k = \mathbb{Q}(\sqrt{D})$ has $\mathcal{N}(\epsilon_0) = 1$, and class number one, we take a rational prime p such that $p = \pi\pi'$ in k and $\mathcal{N}(\pi) = -p$. Then the field $k(\sqrt{-m})$ has a $\mathbb{Z}/2\mathbb{Z}$ factor in the class group whenever m is divisible by p.

One can be more general than this and give a congruence to a family of biquadratic fields with such a class group. The genus theory of quadratic fields states that if k has class number one, and narrow class number 2 (i.e. no units of norm -1), then the discriminant d is divisible by exactly 2 distinct primes. Notice that if $d \equiv 1 \pmod 4$, is prime, than the Pellian equation $x^2 - py^2 = -4$ is solvable, and the field has units of norm -1. Thus there are only three cases to consider. First $d = 4q$ with $q \equiv 3 \pmod 4$ prime. Second is $d = qr$ with $q \equiv r \equiv 3 \pmod 4$, both q, r are prime. Lastly, $d = 8q$, with $q \equiv 3 \pmod 4$ prime.

Proposition 7.5 *Let $k = Q(\sqrt{q})$, with $q \equiv 3$ (mod 4) prime, have class number one. Then $k(\sqrt{-m})$ has a cyclic factor of $\mathbb{Z}/2\mathbb{Z}$ whenever m is divisible by a prime $p \equiv 3$ (mod 4) which is a quadratic non-residue modulo q.*

Proof.

Once we have that $\mathcal{N}(\pi) = -p$ where $\mathfrak{p} = (\pi)$ is a prime ideal in k we are done as $\mathfrak{p}$ ramifies in K. For this to happen $\mathfrak{p}$ must lie in the ideal class that is not the narrow principal class. This is the case when both Kronecker symbols $\left(\frac{-4}{p}\right)$ and $\left(\frac{-q}{p}\right)$ are equal to -1. We have $\left(\frac{-4}{p}\right) = -1$ if and only if $p \equiv 3 \pmod 4$, and then since p is a non-residue modulo q, $\left(\frac{-q}{p}\right) = \left(\frac{p}{q}\right)$. $\square$

In the example we have been using, $k = \mathbb{Q}(\sqrt{3})$, we get the following.

Corollary 7.6 *Let $k = \mathbb{Q}(\sqrt{3})$ and $K = k(\sqrt{m})$, m is divisible by $p \equiv 11$ (mod 12). Then $\mathcal{C}(K)$ has a cyclic factor of $\mathbb{Z}/2\mathbb{Z}$.*

Recall in Example 2 at the end of chapter 6, we saw that the class number of $\mathbb{Q}(\sqrt{3})(\sqrt{-23})$ was 12 and the class group was $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$, which agrees with the above corollary.

Proposition 7.7 *Let $k = \mathbb{Q}(\sqrt{rq})$, $r \equiv q \equiv 3$ (mod 4), r, q prime. Then $k(\sqrt{-m})$ has a cyclic factor of $\mathbb{Z}/2\mathbb{Z}$ whenever m is divisible by a prime p which is a quadratic non residue modulo both r and q.*

Proof.

We follow the proof given above. We now want $\left(\frac{-r}{p}\right) = \left(\frac{-q}{p}\right) = -1$. Simple manipulations using the laws of the Kronecker symbol give $\left(\frac{-r}{p}\right) = \left(\frac{p}{r}\right)$ and $\left(\frac{-q}{p}\right) = \left(\frac{p}{q}\right)$, which gives the result, since once again we have a $+/-$ ideal of K which lies in an ideal class of order 2. $\square$

Proposition 7.8 *Let $k = \mathbb{Q}(\sqrt{2q})$, $q \equiv 3$ (mod 4) prime. Then $k(\sqrt{-m})$ has a cyclic factor of $\mathbb{Z}/2\mathbb{Z}$ whenever m is divisible by a prime p such that $p \equiv 5$ or 7 (mod 8) and p is a non residue modulo q.*

Proof.

In this case, we desire that $\left(\frac{-8}{p}\right) = \left(\frac{-q}{p}\right) = -1$. One can easily verify that this implies the stated congruence conditions. $\square$

We point out that in all three propositions we have shown that the class group of K is the direct product of the classes of $+/+$ ideals and a subgroup generated by the class of a $+/-$ ideal of order 2.

Chapter 8

Prime Discriminants

For quadratic number fields, one is able to factor the field discriminant uniquely into prime discriminants, that is quadratic field discriminants which are only divisible by one prime.. The list of prime discriminants is as follows

$$(-1)^{\frac{p-1}{2}}p, \ -4, \ 8, \ -8$$

where p denotes any odd prime. Decomposing discriminants of quadratic fields into prime discriminants is instrumental in the genus theory of quadratic fields, and we shall attempt to duplicate some of the genus theory results in the extended setting of this paper. For treatments of classical results for quadratic fields, the reader is directed to [1] and [9].

8.1 Prime discriminants for primes of odd norm

Larry Goldstein in [8], proved the existence of prime discriminants for quadratic extensions of totally real fields of narrow class number one. We will provide a new proof which both demonstrates how to construct these discriminants, and also provides insight into the necessity of the narrow class number one assumption. We start by making a definition.

Definition *Let k be a totally real field of narrow class number one. If π is a relative discriminant of a quadratic extension of k, and π is divisible by only one prime ideal of k, we say π is a prime discriminant.*

Saying π is a discriminant means that π is the determinant of the matrix given in (3.3). The theorem is then as follows.

Theorem 8.1 (Goldstein) *Let k be a totally real field of narrow class number one, and let δ be a discriminant of a quadratic extension of K. Then δ can be written in the form*

$$\delta = \pi_1 \pi_2 \cdots \pi_t,$$

where the π_i are distinct prime discriminants.

What is not immediately clear from the definition and theorem is that for primes $\mathfrak{p}$ of odd norm, there is a unique generator of $\mathfrak{p}$ (up to the square of a unit) that is a prime discriminant. This can be made precise in the following theorem.

Theorem 8.2 *Let k be a totally real field of narrow class number one, and let $\mathfrak{p}$ be a prime ideal of k where $\mathfrak{p} \not| 2$. Then there exists a generator π of $\mathfrak{p}$ such that π is the field discriminant of some quadratic extension of k. Furthermore, π is unique up to the square of a unit.*

We will prove Theorem 8.2 after first proving some some preliminary lemmas.

For primes π which divide 2, it is unfortunately the case that π can not be a field discriminant. In fact, there may be more than one discriminant involving π (as -4, -8, 8 in the classical case). We will examine these facts more closely in the next section.

Let $K = k(\sqrt{\Delta})$, where Δ is square free, and suppose the relative discriminant of K/k is δ. Then $\delta s^2 = 4\Delta$, for some $s \in k$. The discriminant is Δ exactly when Δ is relatively prime to 2, and Δ is congruent to a square modulo 4.

We let

$$2 = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdots\mathfrak{p}_t^{e_t}$$

be a the factorization of 2 in k and set

$$\alpha = \mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_t. \tag{8.1}$$

It suffices to show that the units times squares cover all the congruence class in $(\mathcal{O}_k/4)^*$, and further that any unit other than one which is a square modulo 4 is itself a square. Thus, up to the square of a unit, there is a unique generator of $\mathfrak{p}$ which is congruent to a square modulo 4.

Lemma 8.3 *For any β, with $(\beta, 2) = 1$, there exists an odd a such that $\beta^a \equiv 1 \pmod{\alpha}$.*

Proof.

The order of the multiplicative groups $(\mathcal{O}_k/\mathfrak{p}_j)^*$ are $\mathcal{N}(\mathfrak{p}_j) - 1$, which are all odd. We can pick one a that works for all $\mathfrak{p}_j$ by taking the least common multiple of the $\mathcal{N}(\mathfrak{p}_j) - 1$, and thus by the Chinese Remainder Theorem, $\beta^a \equiv 1 \pmod{\alpha}$. □

In k the unit group has $n-1$ fundamental units. Applying the above lemma, we construct a list of n (including -1) units, $\epsilon_0, \epsilon_1, \ldots, \epsilon_{n-1}$, which are all 1 modulo α. From this this we can form 2^n units by considering all $\prod_{j=0}^{n-1} \epsilon_j^{b_j}$ with each $b_j = 0$ or 1.

Lemma 8.4 *The 2^n units mentioned above are all incongruent modulo 4. Further, none of the 2^n units is congruent to a square modulo 4, except for 1.*

Proof.

Suppose $\eta_1 \equiv \eta_2 \pmod 4$, for two of the units η_1, η_2. Then $\eta = \frac{\eta_1}{\eta_2} \equiv 1 \pmod 4$. Thus, (η) is a relative discriminant of the extension $k(\sqrt{\eta})$, and this field is an unramified extension of k. However, if k has narrow class number 1, there are no unramified extensions, yielding a contradiction. Additionally, all of the 2^n units are not squares, since they are products of odd powers of fundamental units. Therefore, if $\eta_j \equiv \square \pmod 4$, $k(\sqrt{\eta_j})$ would also be an unramified extension, which is impossible. $\square$

Here is the first indication of why the assumption of narrow class number one is necessary; with wide class number 1 only, there are ramified extensions at infinite primes, so negative units could be congruent to squares, and there will not be 2^n incongruent units modulo 4. Also, we need that k is totally real or there would again be a shortage of units.

Lemma 8.5 *Let α be as in (8.1). There are $\frac{2^n}{\mathcal{N}(\alpha)}$ congruence classes of numbers β modulo 4 in $\mathcal{O}_k$ such that $\beta \equiv x^2 \pmod 4$ and $\beta \equiv 1 \pmod \alpha$.*

Proof.

By the Chinese Remainder Theorem, $\beta \equiv 1 \pmod \alpha$ if and only if $\beta \equiv 1 \pmod{\mathfrak{p}_j}$ for all j. If we can show there are $\mathcal{N}(\mathfrak{p}_j^{e-1})$ such $\beta \pmod{\mathfrak{p}_j^e}$ which are congruent to $1 \pmod{\mathfrak{p}_j}$, the Chinese Remainder Theorem will give us the desired result. This is because $\frac{2^n}{\mathcal{N}(\alpha)} = \mathcal{N}(\frac{2}{\alpha}) = \prod_j \mathcal{N}(\mathfrak{p}_j^{e_j-1})$. We thus consider each $\mathfrak{p}_j$ separately.

Suppose we have two numbers x and x^* such that $x^2 \equiv (x^*)^2 \pmod{\mathfrak{p}_j^{2e_j}}$. This is the case if and only if $x \equiv x^* \pmod{\mathfrak{p}_j^{e_j}}$, since $x - x^* \equiv x + x^* \pmod{\pi_j^{e_j}}$. We therefore need only consider x modulo $\mathfrak{p}_j^e$. Express $x = x_0 + x_1\mathfrak{p}_j + x_2\mathfrak{p}_j^2 + \cdots + x_{e-1}\mathfrak{p}_j^{e-1}$, where the x_i are chosen from a fixed set of $\mathcal{N}(\mathfrak{p}_j)$ residues modulo $\mathfrak{p}_j$. If $x^2 \equiv 1 \pmod{\mathfrak{p}_j^e}$, then $x_0^2 \equiv 1 \pmod{\mathfrak{p}_j}$, and since $(\mathcal{O}_k/\mathfrak{p}_j)^*$ is a group of odd order there is only 1 square root modulo $\mathfrak{p}$. Thus x_0 is determined, and there are then $\mathcal{N}(\mathfrak{p}_j^{e-1})$ (from the choices of x_i $i = 1 \ldots e-1$) incongruent values of $x^2 \pmod{\mathfrak{p}_j^{2e}}$ that are $1 \pmod{\mathfrak{p}_j^e}$, as desired. $\square$

Proof of Theorem 8.2.

We have by Lemma 8.3 there is an *even* b with $\pi\pi^b \equiv 1 \pmod{\alpha}$. Lemma 8.4 gives 2^n units that are $1 \pmod{\alpha}$ that are not congruent to each other or to squares modulo 4. By Lemma 8.5, there are $\frac{2^n}{\mathcal{N}(\alpha)}$ elements which are squares modulo 4 which are 1 modulo α. Since 1 is the only one of the 2^n units which is a square, the units times squares cover all $\frac{4^n}{\mathcal{N}(\alpha)}$ congruence classes modulo 4 that are 1 modulo α. Thus there is a unique η and t such that $\pi\pi^b \equiv \eta t^2 \pmod 4$, and the π in Theorem 8.2 is exactly the generator of $\mathfrak{p}$ which satisfies the congruence

$$\pi \equiv \eta s^2 \pmod 4.$$

$\square$

This proof then gives us an explicit construction of π for primes of odd norm. The difficulty is determining the prime discriminants associated to primes dividing 2. For any real narrow class number 1 K, the construction of these prime discriminants must be possible. However, since this paper has been concentrating on real quadratic fields, this is where we direct our attention.

8.2 Narrow class number one quadratic fields

The possible even prime discriminants will depend on how 2 factors in the field. There are three cases which arise in narrow class number one real quadratic fields: 2 splits in k, 2 is prime in k, and $k = \mathbb{Q}(\sqrt{2})$. The methodology of the construction is essentially the same in all cases. For this reason, we provide a detailed construction only in the case where 2 is prime in k, as this is the situation in our recurring example $k = \mathbb{Q}(\sqrt{5})$. Having done so, we will also give a constructive proof of Theorem 8.1 in this case.

Let k be a real quadratic field, such that (2) is a prime ideal in k, and let ϵ_0 be the fundamental unit. When Δ is square free, the only possible field discriminants of $k(\sqrt{\Delta})$ are Δ and 4Δ. By Lemma 8.4, there are 4 incongruent units modulo

4 which are 1 modulo 2, which we denote $\{1, -1, \epsilon, -\epsilon\}$, where $\epsilon = \epsilon_0$ or $\epsilon = \epsilon_0^3$. According to lemma 8.5, 1 is the only square modulo 4 which is 1 modulo 2.

For primes $\mathfrak{p}$ of odd norm, Theorem 8.2 gives a unique generator π_p of $\mathfrak{p}$ which is a relative field discriminant. For primes dividing 2, there are only two possible discriminants when considered as ideals: (4) and (8). A discriminant of (4) corresponds to $k(\sqrt{\eta})$, η a unit, and (8) corresponds to $k(\sqrt{2\eta})$. The seven possibilities listed in Table 8.1 yield seven different numerical discriminants, each corresponding to a different quadratic extension.

discriminant	**integral basis**
π_p, $\pi_p \equiv s^2 \pmod 4$	$[1, \frac{s+\sqrt{\pi_p}}{2}]$
-4	$[1, \sqrt{-1}]$
-4ϵ	$[1, \sqrt{-\epsilon}]$
4ϵ	$[1, \sqrt{\epsilon}]$
8	$[1, \sqrt{2}]$
-8	$[1, \sqrt{-2}]$
8ϵ	$[1, \sqrt{2\epsilon}]$
-8ϵ	$[1, \sqrt{-2\epsilon}]$

Table 8.1: Prime Discriminants when 2 is prime in k

Theorem 8.6 *Let k be a real quadratic field of narrow class number one in which 2 is prime. Given δ the relative field discriminant of $k(\sqrt{\Delta})$, Δ square-free, we can factor δ uniquely up to squares of units as the product of the prime discriminants given in Table 8.1.*

Before we begin the proof, we will find the following two results useful.

Proposition 8.7 (Eisenstein Criterion)
Let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ be a polynomial with $\mathcal{O}_k$ coefficients. If there exists a prime ideal $\mathfrak{p} \in \mathcal{O}_k$ such that $\mathfrak{p}|a_i$ for all $i = 1, 2, \ldots, n$, but $\mathfrak{p}^2 \not| a_0$,

then the polynomial $f(x)$ is irreducible in $\mathcal{O}_k[x]$. Furthermore if α is a root of $f(x)$, then the power of $\mathfrak{p}$ in the field discriminant of $k(\alpha)$ is the same as the power of $\mathfrak{p}$ in the polynomial discriminant of $f(x)$.

Proposition 8.8 (Almost Eisenstein Criterion)

Let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ be an irreducible polynomial with $\mathcal{O}_k$ coefficients. Let $\mathfrak{p}$ of $\mathcal{O}_k$, such that $\mathfrak{p}$ divides the polynomial discriminant of $f(x)$, and further $\mathfrak{p}|a_i$ for all $i = 1, 2, \ldots, n$, and $\mathfrak{p}^2|a_0$. Then if α is a root of $f(x)$, the factor of $\mathfrak{p}$ in the field discriminant of $k(\alpha)$ is lower than the power of $\mathfrak{p}$ in the polynomial discriminant of $f(x)$ by at least $\mathfrak{p}^2$.

Proof of Theorem 8.6.

We will first show that one can factor a discriminant into prime discriminants from the table. One can factor δ

$$\delta = \epsilon_0^{2n}\ \eta\ 2^a \prod \pi_p = \epsilon_0^{2n}\ \eta\ 2^a\ \delta^*,$$

where $n \in \mathbb{Z}$, $a \in \{0, 2, 3\}$, and $\eta \in \{1, -1, \epsilon, -\epsilon\}$.

If a is even, there are no factors of 2 in Δ, and the field is generated by the polynomial $x^2 - \eta\delta^*$. The polynomial arrived at by making the change of variables $x \to x + 1$ generates the same field, and

$$x^2 + 2x + (1 - \eta\delta^*),$$

has discriminant $4\eta\delta^*$. If $\eta = 1$, then this polynomial is almost Eisenstein with respect to 2, since the π_p are all 1 modulo 4. The field discriminant then has no factor of 2, by proposition 8.8, and $a = 0$. If η is any of the other 3 units, the polynomial is Eisenstein with respect to 2 and by proposition 8.7 $a = 2$. Since -4, 4ϵ, -4ϵ all appear, the factorization is complete.

If $a = 3$, the field is generated by the polynomial $x^2 - 2\eta\delta^*$, which is Eisenstein with respect to 2, independent of the value of η. The list of prime discriminants has 8η for each value of η, and the factorization is complete.

The last detail that needs to be verified is that the factorizations given above are unique. We have shown that the factorization of the odd part of the discriminant is unique. The only concern, therefore, is that one could generate one of the even discriminants from a product of some others. However, although it is true that, for example, $k(\sqrt{(8)(-4\epsilon)})$ generates the same field as $k(\sqrt{-8\epsilon})$, the goal is to factor the discriminant uniquely up to the square of a unit. The discriminant of $k(\sqrt{-8\epsilon})$ is -8ϵ, and $-8\epsilon \neq (8)(-4\epsilon)\epsilon_0^{2n}$. The entire list from table 8.1 is thus necessary, and the factorizations are unique.

$\square$

We now give the list of the prime discriminants in the two remaining cases. Although we shall not go through the details, the last proof gives the idea of how this could be done.

In the case where $(2) = \pi_2\pi_2'$, we take $\pi_2 \equiv 1 \pmod{\pi_2'^2}$ and $\pi_2' \equiv 1 \pmod{\pi_2^2}$. Further, let $\epsilon = \pm\epsilon_0$ so that $\epsilon \equiv 1 \pmod{\pi_2'^2}$ and $\epsilon \equiv -1 \pmod{\pi_2^2}$. The only square modulo 4 is 1.

In the case $k = \mathbb{Q}(\sqrt{2})$, $2 = \pi_2^2, \epsilon_0 = 1 + \pi_2$. There are now 2 squares modulo 4 which are 1 modulo π_2, they are 1 and $3 + 2\pi_2$.

Example.

Consider again $k = \mathbb{Q}(\sqrt{5})$ and $K = k(\sqrt{-17-4\omega})$ of discriminant $\delta_K = -68 - 16\omega$, where $(\delta_K) = (4)\mathfrak{p}_{11}\mathfrak{p}_{31}$. The ideal $\mathfrak{p}_{11}$ is generated by $\pi_{11} = 1 - 3\omega$. This is not 1 modulo 2, so we consider $\pi_{11}^3 = 1 - 36\omega \equiv 1 \pmod 4$, so π_{11} is the prime discriminant. The prime$\mathfrak{p}_{31} = \pi_{31} = 2 - 5\omega$, which also is not 1 modulo 2, but $\pi_{31}^3 = 33 - 160\omega$ is, and π_{31} is a prime discriminant. One checks that $\delta_K/(pi_{11}\pi_{31}) = -4$. So the factorization of δ_K into prime discriminants is given by

$$\delta_K = -4 * \pi_{11} * \pi_{31}.$$

discriminant	**integral basis**
π_p, $\pi_p \equiv 1 \pmod 4$	$[1, \frac{1+\sqrt{\pi_p}}{2}]$
π_2^3	$[1, \frac{1+\sqrt{\pi_2}}{\pi_2'}]$
$\epsilon\pi_2^3$	$[1, \frac{1+\sqrt{\epsilon\pi_2}}{\pi_2'}]$
$\pi_2'^3$	$[1, \frac{1+\sqrt{\pi_2'}}{\pi_2}]$
$-\epsilon\pi_2'^3$	$[1, \frac{1+\sqrt{-\epsilon\pi_2'}}{\pi_2}]$
$\epsilon\pi_2^2$	$[1, \frac{1+\sqrt{\epsilon}}{\pi_2'}]$
$-\epsilon\pi_2'^2$	$[1, \frac{1+\sqrt{-\epsilon}}{\pi_2}]$

Table 8.2: Prime Discriminants when 2 splits in k

discriminant	**integral basis**
π_p, $\pi_p \equiv s^2 \pmod 4$	$[1, \frac{s+\sqrt{\pi_p}}{2}]$
-2	$[1, \frac{\sqrt{-1}}{\pi_2}]$
-4ϵ	$[1, \sqrt{-\epsilon}]$
4ϵ	$[1, \sqrt{\epsilon}]$
$4\pi_2$	$[1, \sqrt{\pi_2}]$
$-4\pi_2$	$[1, \sqrt{-\pi_2}]$
$4\epsilon\pi_2$	$[1, \sqrt{\epsilon\pi_2}]$
$-4\epsilon\pi_2$	$[1, \sqrt{-\epsilon\pi_2}]$

Table 8.3: Prime Discriminants in $\mathbb{Q}(\sqrt{2})$.

8.3 Narrow class number 2 quadratic fields

When the narrow class number is not 1, we no longer have enough units to cover all classes modulo 4. There may now be a unit other than 1 which is congruent to a square modulo 4 because there are now unramified extensions at infinite primes. This means that for some prime ideals, there is no relative discriminant which is divisible by only that prime ideal.

As an example, consider the field $\mathbb{Q}(\sqrt{3})$, in which $59 = \mathfrak{p}_{59}\mathfrak{p}'_{59}$. There is no generator of $\mathfrak{p}_{59}$ that is a relative field discriminant. The smallest discriminant involving $\mathfrak{p}_{59}$ is $2\mathfrak{p}_{59}$.

In light of the above observation, one can no longer hope to factor discriminants uniquely up to squares of units into prime discriminants. The best one could hope for is to factor discriminants uniquely up to a square factor of primes dividing two. While preliminary investigations indicate that this is possible, the proof is rather tedious and the usefulness that prime discriminants serve in the next chapter will not be directly applicable. To give a thorough examination of this situation would stray from the themes of this paper, and is mentioned as a possible future research subject of interest.

Chapter 9

Genus Theory

Gauss in his study of the class group of forms in [7] developed the notion of genus theory. In essence, he was able to categorize the 2-Sylow subgroup of the class group. This is essentially done by forming quadratic characters associated with prime discriminants, and categorizing forms according to the value they take on these characters. One of the fascinating consequences of this is the following theorem.

Theorem 9.1 (Gauss) *Let d be the discriminant of k, a complex quadratic field, and let d have exactly t prime factors. Then the class number $h(k)$ is divisible by a factor of 2^{t-1}.*

To prove an analogous theorem will be our first goal. We will do so, however, from the standpoint of ideals rather than forms. Once this is established, we will look at how this connects with quadratic forms. The proofs will be taking advantage of more sophisticated algebraic number theory machinery than has been previously necessary, and the reader is directed to [10] for details on these tools, and [1], [7], [9] for treatment of genus theory of quadratic fields.

9.1 The genus field

Let k be a real quadratic field of narrow class number 1, and let K be a totally complex quadratic extension of k. Also let L be the Hilbert class field of K, $G = \mathrm{Gal}(L/k)$, and $H = \mathrm{Gal}(L/K)$. There is an isomorphism between H and the ideal class group of K which identifies any $\sigma \in H$ with the class of a prime ideal $\mathfrak{P}$ having σ as its Frobenius automorphism.

Lemma 9.2 *Let τ be an element of G that is not an element of H. Then $\tau^2 = 1$. If σ is any element of H, then $\sigma\tau = \tau\sigma^{-1}$.*

Proof.

Note that for K totally complex, there will always be such a τ, namely complex conjugation. We fix a prime $\mathfrak{P}$ of L (which divides $\mathfrak{p}$ in k), such that $\mathfrak{P}$ is unramified in L/k, and $\tau = \sigma(\mathfrak{P}, L/k)$, the Frobenius automorphism of $\mathfrak{P}$ with respect to L/k. If $\mathfrak{p}$ splits in K, then $\langle\tau\rangle = G_D(\mathfrak{P}, L/k) \subset H$, which is a contradiction. Therefore $\mathfrak{p}$ is prime in K.

Since $\tau = \sigma(\mathfrak{P}, L/K)$,

$$\alpha^{\mathcal{N}(\mathfrak{p})} \equiv \tau(\alpha) \pmod{\mathfrak{P}},$$

and therefore

$$\alpha^{\mathcal{N}(\mathfrak{p}^2)} \equiv \tau^2(\alpha) \pmod{\mathfrak{P}}.$$

Now since $\mathfrak{p}$ is prime in K, $\mathcal{N}_{K/\mathbb{Q}}(\mathfrak{p}) = \mathcal{N}_{k/\mathbb{Q}}(\mathfrak{p}^2)$, and $\sigma(\mathfrak{P}, L/K) = \tau^2$. Furthermore, since $\tau^2 = \sigma(\mathfrak{P}, L/K)$, $\tau^2 \in H$, and using the class field isomorphism, τ^2 must be the identity element of H, since it corresponds to the ideal $\mathfrak{p}$, which is principal.

For the second part of the proof, choose a prime $\mathfrak{p}$ in k such that $\mathfrak{p} = \mathfrak{P}\bar{\mathfrak{P}}$ in K, with $\sigma(\mathfrak{P}, H/K) = \sigma$. We have that $\sigma(\bar{\mathfrak{P}}, L/K) = \sigma(\tau(\mathfrak{P}), L/K) = \tau^{-1}\sigma\tau$. Since $\mathfrak{P}\bar{\mathfrak{P}} = \mathfrak{p}$ is principal, the product of their Frobenius automorphisms is the identity. So recalling that $\tau^2 = 1$ implies $\tau = \tau^{-1}$,

$$\begin{aligned}(\sigma)(\tau\sigma\tau) &= 1 \\ \sigma\tau &= \tau\sigma^{-1}.\end{aligned}$$

$\square$

The group G might be thought of as "almost dihedral," since it has the same relations as a dihedral group except that H is not necessarily cyclic.

Definition *The genus field of K with respect to k is the maximal abelian extension of k contained in the Hilbert Class field of K.*

Theorem 9.3 *Let F be the genus field of K with respect to k. Then Gal(F/k) is an elementary abelian 2 group.*

Proof.

All of the relevant fields are shown in Figure 9.1. Since F is the maximal abelian extension of k contained in L, G_1 is the minimal normal subgroup of G such that $G/G_1 \cong$ Gal(F/k) is abelian. Consider the natural homomorphism from G to G/G_1, and denote the image of an element $g \in G$ by $\widehat{g}$. Let σ be an element of H, and τ be an element of G which is not in H. Since the group G/G_1 is abelian, $\widehat{\sigma}\widehat{\tau} = \widehat{\tau}\widehat{\sigma}$. Also by Lemma 9.2,

$$\begin{aligned}\widehat{(\sigma^{-1})} &= \widehat{(\tau\sigma\tau)} \\ &= \widehat{(\sigma\tau\tau)} \\ &= \widehat{\sigma}.\end{aligned}$$

Therefore,

$$\widehat{\sigma}^2 = \widehat{1}.$$

Thus every element of G/G_1 is of order 2, completing the proof. $\square$

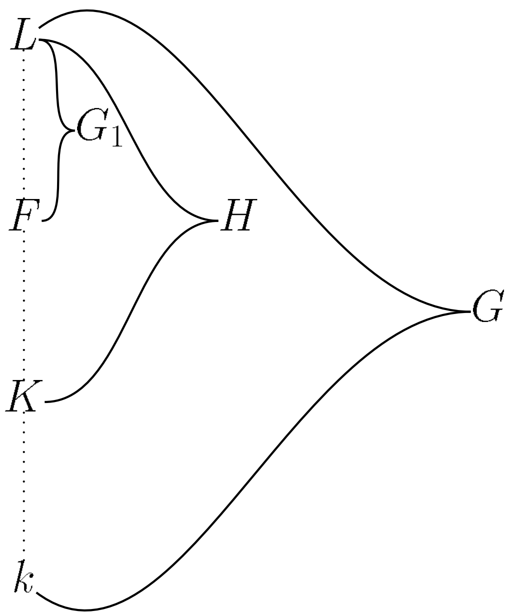

Figure 9.1: Genus field tower

Definition *The principal genus is the subgroup of the of the class group corresponding to the genus field.*

This corresponds to the group G_1 in the last theorem and in Figure 9.1. As stated in the proof of the theorem, the principal genus is also the minimal subgroup of the class group such that the quotient is abelian.

Proposition 9.4 *The principal genus is the subgroup of the class group consisting of the squares.*

Proof.

Let G_1 be the principal genus, and $S = \{s^2 \mid s \in H\}$. Since every element of H/G_1 is of order 2, in the projection $H \to H/G_1$, S is mapped to the identity, so $S \subset G_1$.

Further, S is normal in H as

$$(xsx^{-1})^2 = (xsx^{-1})(xsx^{-1})$$

so that the conjugate of a square is a square. Since every element of H/S has order 2, H/S is abelian. By the minimality of the principal genus, $G_1 \subset S$, and we are done. $\square$

We have demonstrated that for $K = k(\sqrt{\delta_K})$, with δ_K the relative discriminant of K/k, one can factor δ uniquely into a product of prime discriminants,

$$\delta = \prod_{j=1}^{t} \pi_{p_j}. \tag{9.1}$$

The aim now is to prove the following theorem.

Theorem 9.5 *The genus field of K is the composite of the quadratic fields $K_j = k(\sqrt{\pi_{p_j}})$, where the π_{p_j} are as in equation (9.1).*

Proof.

Let $K_n = k(\sqrt{\delta_n})$ be a quadratic extension of K, where δ_n is the discriminant relative to k. K_n is contained in F if and only if $M = K(\sqrt{\delta_n})$ is unramified over K. This is the case exactly when the relative discriminant of M over K, $\delta_{M/K} = (1)$. To calculate the discriminant $\delta_{M/K}$, notice that M is a degree 4 extension of k with three intermediate fields: K, K_n, $K_n' = k(\sqrt{\delta\delta_n})$ of discriminant $\delta_{n'}$. We will show that K_n is contained in F if and only if $\delta = \delta_n \delta_{n'}$, with $(\delta_n, \delta_{n'}) = 1$.

By the conductor discriminant formula, the discriminant of M relative to k, δ_M, is given by

$$(\delta_M) = (\delta\delta_n\delta_{n'}). \tag{9.2}$$

There is also another classical formula for computing δ_M given by

$$(\delta_M) = \mathcal{N}_{K/k}(\delta_{M/K})(\delta_K^{[K:k]}). \tag{9.3}$$

Let

$$\delta_n = \prod_{j=1}^{t_n} \pi_{p_j} \prod_{j=1}^{s_n} \pi^*_{p_j},$$

where we have suitably ordered the π_{p_j} in 9.1, and the $\pi^*_{p_j}$ are prime discriminants not dividing δ. Notice

$$\delta\delta_n = \prod_{j=1}^{t_n} \pi^2_{p_j} \prod_{j=t_n+1}^{t} \pi_{p_j} \prod_{j=1}^{s_n} \pi^*_{p_j},$$

and hence it follows that

$$\delta_{n'} = \prod_{j=t_n+1}^{t} \pi_{p_j} \prod_{j=1}^{s_n} \pi^*_{p_j}.$$

We then have by (9.2)

$$(\delta_M) = (\delta^2)(\prod_{j=1}^{s_n} \pi^*_{p_j})^2.$$

If $K_n \subset F$, we have $\delta_{M/K} = (1)$, so comparing (9.2) and (9.3) we see that

$$(\delta)^2(\prod_{j=1}^{s_n} \pi^*_{p_j})^2 \quad = \quad (\delta)^2$$

so that there are no primes $\pi^*_{p_j}$ in the factorization of δ_n. Thus $\delta_n|\delta$, and $\delta_{n'} = \frac{\delta}{\delta_n}$, and they are obviously relatively prime. If conversely, $\delta = \delta_n\delta_{n'}$, again comparing equations (9.2) and (9.3) leads to

$$(\delta)^2 = \mathcal{N}_{K/k}(\delta M/K)(\delta)^2,$$

so that M is unramified over K, and $K_n \subset F$. We then have that $F = k(\{\sqrt{\delta_n}\}) = k(\sqrt{\pi_{p_1}}, \sqrt{\pi_{p_2}}, \ldots, \sqrt{\pi_{p_t}})$. □

The next result is an immediate corollary.

Corollary 9.6 *Let k be a real quadratic field of narrow class number 1, and K be a totally complex extension of k. If the relative discriminant of K can be factored into t prime discriminants, then there is a factor of 2^{t-1} in the class number of K.*

9.2 Genus characters

We will now demonstrate how one can use quadratic characters to separate ideal and form classes into genera. Let χ be a quadratic character of conductor $\mathfrak{f}$ defined on the ideals of k. Since k has narrow class number 1, one can insist that we use only totally positive generators of ideals, and thus $\mathfrak{f}$ can be considered finite. Further since all ideals in k are principal, one has a character on the totally positive elements of k. Since k has narrow class number 1, the totally positive units are generated by ϵ_0^2, and so any quadratic character is automatically 1 on totally positive units. We can now extend χ to a character $\widehat{\chi}$ on the ideals of K by

$$\widehat{\chi}(\mathfrak{a}) = \chi(\mathcal{N}(\mathfrak{a})).$$

One could of course also think about this as a character on quadratic forms of discriminant δ, by

$$\widehat{\chi}(ax^2 + bxy + cy^2) = \chi(a), \tag{9.4}$$

recalling that a is the norm of the ideal $[a, a\theta]$ and is totally positive.

The genus characters, $\widehat{\chi}_{\delta_n}$, will be the quadratic characters corresponding to χ_{δ_n} of conductor δ_n where $\delta_n \mid \delta$. In turn, the χ_{δ_n} are related to the character of the field $K(\sqrt{\delta_n})/k$.

Proposition 9.7 *If $\mathfrak{P}$ in K divides (π) in k, for any prime $\mathfrak{P}$ such that $(\mathfrak{P}, \delta_n) = 1$, $\widehat{\chi}_{\delta_n}(\mathfrak{P}) = 1$ if and only if π splits in K_n.*

Proof.

This is follows immediately from the fact that δ_n is the discriminant of K_n, and thus the finite part of the conductor of K_n. By insisting on totally positive π, we can ignore the infinite primes in the conductor, and so χ_{δ_n} is the character corresponding to the extension K_n/k. Through Frobenius reciprocity, this is 1 on ideals prime ideals that split, and -1 on those that are inert. $\square$

In fact one has that in any class field extension, the primes that split completely are exactly those primes $\mathfrak{p}$ such that every character evaluated at $\mathfrak{p}$ is 1. In particular, the primes that split completely in the Hilbert class field are the principal prime ideals. Since the genus field is contained in the Hilbert class field, we have that the principal prime ideals split completely in it as well, and so all the genus characters are one on principal ideals. Thus our genus characters are well defined on ideal classes, and so are actually characters of the class group.

Proposition 9.8 *If $\delta = \delta_1\delta_2$, with $(\delta_1, \delta_2) = 1$, then $\widehat{\chi}_{\delta_1} = \widehat{\chi}_{\delta_2}$.*

Proof.

Since $(\delta_1, \delta_2) = 1$, one can factor $\widehat{\chi}_\delta = \widehat{\chi}_{\delta_1}\widehat{\chi}_{\delta_2}$. If $\mathfrak{P}$ is inert in K, $\mathcal{N}(\mathfrak{P}) = (\pi^2)$, $\widehat{\chi}_{\delta_1}(\mathfrak{P}) = \widehat{\chi}_{\delta_2}(\mathfrak{P}) = 1$. If π splits in K_n, $\widehat{\chi}_\delta(\mathfrak{P}) = 1$, and $\widehat{\chi}_{\delta_1}(\mathfrak{P}) = \widehat{\chi}_{\delta_2}(\mathfrak{P})$. □

We can utilize this relationship to now define $\widehat{\chi}_\delta(\mathfrak{P})$ for all $\mathfrak{P}$, including those $\mathfrak{P}|\delta$. If $\mathfrak{P}|\delta_1$, then we define $\widehat{\chi}_\delta(\mathfrak{P}) = \widehat{\chi}_{\delta_2}(\mathfrak{P})$.

We conclude with an examination of how to explicitly define the genus characters. For π_p not dividing two, since $(\mathcal{O}_k/\pi_p)^*$ is cyclic, it must be the case that

$$\widehat{\chi}_{\pi_p}(\mathfrak{a}) = \mathcal{N}(\mathfrak{a})^{\frac{\mathcal{N}(\pi_p)-1}{2}} \pmod{\pi_p}.$$

Note that this is exactly how the characters associated to odd primes are defined in the classical case. However, the characters corresponding to even prime discriminants are not so simple, and depend on the structure of $(\mathcal{O}_k/(\pi_p))^*$.

In the case where 2 is prime in k, one can verify that

$$(\mathcal{O}_k/4)^* \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z},$$

and

$$(\mathcal{O}_k/8)^* \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}.$$

Further, $(\mathcal{O}_k/4)^*$ is generated by ϵ_0 and -1, where $\epsilon_0^6 \equiv 1 \pmod 4$. One can see this by recalling that ϵ_0 and -1 are not squares modulo 4. The characters modulo

4 are thus determined by their values at ϵ_0 and -1. To determine which field correspond to which characters, we consider the infinite primes, and the fact that the character associated to a field is 1 on units.

The field $K = k(\sqrt{-4})$ is totally complex, both infinite primes are present in the conductor. Since -1 is totally negative also, we must have that $\chi_{-4}(-1) = 1$. Since ϵ_0 is not totally positive, we need $\chi_{-4}(\epsilon_0) = -1$. For $K = k(\sqrt{-4\epsilon_0})$, only the infinite prime associated to k is present. Since $\epsilon_0 > 0$ and $-1 < 0$, $\chi_{-4\epsilon_0}(-1) = -1$, and $\chi_{-4\epsilon_0}(\epsilon_0) = 1$. For $K = k(\sqrt{4\epsilon_0})$, the infinite prime associated to k' is present in the conductor. Since ${\epsilon_0}' < 0, -1 < 0$, we require $\chi_{4\epsilon_0}(-1) = -1$, and $\chi_{4\epsilon_0}(\epsilon_0) = -1$.

For the characters modulo 8, the characters are determined by their values on $-1, \epsilon_0$, and $1 + 4\epsilon_0$. The order of ϵ_0 is either 4 or 12 and not 3 or 6 because if it were, $(\epsilon_0^3 - 1)(\epsilon_0^3 + 1) \equiv 0 \pmod 8$. Therefore, $4|(\epsilon_0^3 - 1)$ or $(\epsilon_0^3 + 1)$, and $\pm\epsilon_0 \equiv s^2 \pmod 4$, for some s. For the characters to be primitive, they must be -1 at $1 + 4\epsilon_0$, or else we have one of the characters modulo 4.

For $K = k(\sqrt{8})$, there are no infinite primes in the conductor and $\chi_8(-1) = 1$, and $\chi_8(\epsilon_0) = 1$. For $K = k(\sqrt{-8})$, both infinite primes are in the conductor and we have $\chi_{-8}(-1) = 1$, and $\chi_{-8}(\epsilon_0) = -1$. In the case $K = k(\sqrt{8\epsilon_0})$ we need consider the infinite prime associated to k, and therefore $\chi_{8\epsilon_0}(-1) = -1$, and $\chi_{8\epsilon_0}(\epsilon_0) = 1$. Finally for $K = k(\sqrt{-8\epsilon_0})$ the infinite prime associated to k' is present, so $\chi_{-8\epsilon_0}(-1) = -1$, and $\chi_{-8}(\epsilon_0) = -1$.

In the case where $(2) = \pi_2\pi_2'$, we take $\pi_2 \equiv 1 \pmod{{\pi_2'}^2}$, and $\pi_2' \equiv 1 \pmod{\pi_2^2}$. Further, we take $\epsilon = \pm\epsilon_0$ such that $\epsilon \equiv 1 \pmod{{\pi_2'}^2}$. One can establish the genus characters as follows.

There will be one character arising from $(\mathcal{O}_k/\pi_2^2)^* \cong (\mathbb{Z}/4\mathbb{Z})^*$. Further the field, $K = k(\sqrt{\epsilon\pi_2^2})$ has the infinite prime of k' in the conductor. Since $\epsilon \equiv -1 \pmod{\pi_2^2}$, the character associated to $\epsilon\pi_2^2$ is the only character possible where $\chi(-1) = -1$. We have a similar result for the conjugate case, which has the infinite prime associated to k in the conductor, and $\epsilon \equiv 1 (\bmod\ \pi_2')$. Again $\chi(-1) = -1$, and the character of the field is 1 on all units.

There will also be 2 characters arising from $(\mathcal{O}_k/\pi_2^3)^* \cong (\mathbb{Z}/8\mathbb{Z})^*$. One of the primitive characters is 1 at 1 and -1, the other is 1 at 1 and 3. Notice that one of $\epsilon\pi_2^3$ and π_2^3 has both conjugates with the same parity, and the other has conjugates with opposite parity, so we pick π_2 such that it has positive norm. In this way $\chi_{\pi_2^3}(-1) = 1$, to satisfy the congruence of the infinite prime. In the other case, to satisfy the congruence of the infinite prime, we have $\chi_{\epsilon\pi_2^3}(-1) = -1$. A similar argument will give the characters associated to π_2'.

We note an interesting congruence that arises out of this theory. If we choose π_2 to have positive norm, then the congruence class of ϵ modulo π_2^3 depends on the sign of π_2. We have that $\epsilon \equiv -1 \pmod{\pi_2^2}$, so $\epsilon \equiv -1 \pmod{\pi_2^3}$ or $\epsilon \equiv 3 \pmod{\pi_2^3}$. If $\pi_2 < 0$, then both infinite primes appear in the conductor of $k(\sqrt{\pi_2^3})$, so we must have $\chi_{\pi_2^3}(\epsilon) = -1$. Therefore, $\epsilon \equiv 3 \pmod{\pi_2^3}$. If on the other hand $\pi_2 > 0$, there are no infinite primes in the conductor of $k(\sqrt{\pi_2^3})$, and $\chi_{\pi_2^3}(\epsilon) = 1$. In this case then, $\epsilon \equiv -1 \pmod{\pi_2^3}$. Naturally there is a similar congruence modulo ${\pi_2'}^3$.

$(\mathbf{a}, \mathbf{b}, \mathbf{c})$	$\widehat{\chi}_{-4}$	$\widehat{\chi}_{\pi_{11}}$	$\widehat{\chi}_{\pi_{31}}$
$(1, 0, 17 + 4\omega)$	1	1	1
$(5, -4 + 4\omega, 5)$	1	1	1
$(2 + \omega, -2 - 2\omega, 10 - \omega)$	1	-1	-1
$(2 + \omega, 2 + 2\omega, 10 - \omega)$	1	-1	-1
$(5 - \omega, -2, 4 + 2\omega)$	-1	1	-1
$(5 - \omega, 2, 4 + 2\omega)$	-1	1	-1
$(4 - \omega, 0, 5 + 3\omega)$	-1	-1	1
$(2, 2, 9 + 2\omega)$	-1	-1	1

Table 9.1: Genera of forms for $\mathbb{Q}(\sqrt{5})(\sqrt{-68 - 16\omega})$

Example.

Recall our recurring example where $k = \mathbb{Q}(\sqrt{5})$, and $K = -68 - 16\omega$. We saw that this factors into prime discriminants as

$$68 - 16\omega = (-4)(1 - 3\omega)(2 - 5\omega).$$

Corollary 9.6 predicts that there should be a factor of 4 in the class number of K, and we saw that in fact the class number was 8. This means that each of the four genera contain 2 ideal classes. The 3 genus characters are $\widehat{\chi}_{\mathfrak{p}_{11}}$, $\widehat{\chi}_{\mathfrak{p}_{31}}$, and $\widehat{\chi}_{-4}$. The character χ_{-4} is given by

$$\chi_{-4}(\mathfrak{a}) = \begin{cases} 1 & \mathcal{N}(\mathfrak{a}) \equiv \pm(\epsilon^2)^c \pmod 4 \\ -1 & \text{otherwise.} \end{cases}$$

and $\chi_{\pi_{11}}$ and $\chi_{\pi_{31}}$ are given in (9.2). Using equation (9.4), we calculate the four genera for the class group in terms of forms. The results are given in Table 9.1.

Bibliography

[1] Duncan Buell, *Binary quadratic forms : Classical theory and modern computations*, Springer-Verlag, 1989.

[2] G. Claus, *Die Randmannigfaltigkeiten und die 'tiefsten' Punkt des Fundamentalbereichs für drei Hilbertsche Modulgruppen.*, Math. Annalen **176** (1968), 225–256.

[3] Henri Cohen, *A course in computational algebraic number theory*, Springer-Verlag, 1993.

[4] Harvey Cohn, *A numerical survey of the floors of various hilbert fundamental domains*, Math. Comp. **19** (1965), 594–605.

[5] ______, *Note on how hilbert modular domains become increasingly complicated*, J. Math. Anal. Appl. **15** (1966), 55–59.

[6] Daberkow, Fieker, Klüners, Pohst, Roegner, and Wildanger, *KANT V4*, J. Symbolic Comp. **24** (1997), 267–283.

[7] Carl Friedrich Gauss, *Disquisitiones arithmeticae*, Springer-Verlag, 1986, translated by Arthur A. Clarke.

[8] L.J. Goldstein, *On prime discriminants*, Nagoya Math. J. **45** (1971), 119–127.

[9] Erich Hecke, *Lectures on the Theory of Algebraic Numbers*, Springer-Verlag, 1981, translated by George U. Brauer and Jay R. Goldman with the assistance of R. Kotzen.

[10] Wladyslaw Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, 2nd ed., Springer-Verlag, 1990.

[11] H. M. Stark, *Modular forms and related objects*, Canadian Mathematical Society Conference Proceedings, vol. 7 (Providence, R.I.), Amer. Math. Soc., 1987, pp. 421–455.

[12] ———, *Galois theory, algebraic number theory, and zeta functions*, From Number Theory to Physics, ch. 6 (M. Waldschmidt, et. al., ed.), Springer-Verlag, 1992, pp. 313–393.