Chapter 6

Quadratic Number Fields

6.1 Basic Algebraic Definitions

For the benefit of less experienced readers, we repeat some basic definitions of abstract algebra. A group is a pair \((G, +_G)\) in which \(G\) is a set and \(+_G\) is a closed associative binary operation on \(G\) for which the following hold:

a) there exists an element \(1_G\) of \(G\), called the identity, which has the property that for any element \(a\) in \(G\), we have \(a +_G 1_G = 1_G +_G a = a\);

b) for every element \(a\) of \(G\), there exists an element \(b\), called the inverse of \(a\), for which \(a +_G b = b +_G a = 1_G\).

A group is called commutative, or abelian, if the operation \(+_G\) is commutative. The order of \((G, +_G)\) is the cardinality of the set \(G\). Groups are called finite or infinite according as this cardinality is finite or infinite.

A ring is a triple \((R, +_R, \cdot_R)\) with the following properties:

a) \((R, +_R)\) is an abelian group of order at least 2;
b) $+_R$ is a closed associative binary operation on $R$;

c) for all elements of $R$, $*_R$ distributes over $+_R$.

The operation $+_R$ is usually called "addition" and the operation $*_R$ is usually called "multiplication." The identity under addition is usually called the "zero" of the ring. A ring with identity is a ring $R$ for which an identity exists for the operation $*_R$. This identity, if it exists, is usually called the "1" of the ring. A field is a ring $R$ for which $(R - \{0\}, *_R)$ is an abelian group. In any ring $R$, a subset $I$ of $R$ is called an ideal if, for any $\alpha, \beta \in I$, then for any $\lambda, \mu \in R$, $\lambda \alpha + \mu \beta \in R$.

We state without proof some propositions. To avoid confusion later, we shall begin to call the integers $\mathbb{Z}$ the rational integers. This distinction will be necessary, as we shall shortly define algebraic integers.

**Proposition 6.1.** The rational integers $\mathbb{Z}$ form a commutative ring with identity under ordinary addition and multiplication. The additive identity is 0, and the additive inverse of $n$ is $-n$. The multiplicative identity is 1.

**Proposition 6.2.** The rational numbers $\mathbb{Q}$ form a field under ordinary addition and multiplication. The multiplicative inverse of $a \neq 0$ is $1/a$.

**Proposition 6.3.** For any rational integer $n$, $n = \{kn : k \in \mathbb{Z}\}$ is an ideal of $\mathbb{Z}$. All ideals of $\mathbb{Z}$ are of this form.
6.2 Algebraic Numbers and Quadratic Fields

An algebraic number is a complex number \( \alpha \) which satisfies a polynomial equation \( f(x) = 0 \), in which \( f(x) \) is a polynomial in \( x \) with rational number coefficients. We can multiply this equation by the least common multiple of the denominators of the coefficients of \( f(x) \), and may thus equivalently require that \( f(x) \) be a polynomial with rational integer coefficients.

An algebraic integer is any algebraic number which satisfies a monic polynomial equation \( f(x) = 0 \) in which \( f(x) \) is a polynomial in \( x \) with coefficients that are rational integers.

Proposition 6.4. The only rational numbers that are algebraic integers are the rational integers.

Proof. Let \( a/b \in \mathbb{Q} \), with \( \gcd(a,b) = 1 \). Clearly, since \( a/b \) is a solution to \( x - a/b = 0 \), we know that \( a/b \) is an algebraic number, and if \( a/b \) is a rational integer (that is, if \( b = 1 \)), then \( a/b = a \) is an algebraic integer. If we assume that \( a/b \) is an algebraic integer and \( b > 1 \), then we have an equation with rational integer coefficients \( c_i \):

\[(a/b)^n + c_{n-1}(a/b)^{n-1} + \ldots + c_1(a/b) + c_0 = 0.\]

Multiplying through by \( b^n \) we get

\[a^n + c_{n-1}a^{n-1}b + \ldots + c_1ab^{n-1} + c_0b^n = 0.\]

Since \( b \) divides all terms except the first, it must also divide the first. This would, however, imply that \( \gcd(a,b) > 1 \), which is a contradiction.

We now turn our attention specifically to quadratic number fields. Although many of the terms and theorems are valid or have generalizations to all number fields, we shall prove them only for the quadratic
case. This is the case in which there are connections with binary quadratic forms, and in this case the proofs are often much simpler because we can simply and explicitly solve quadratic equations. We define a complex number $\alpha$ to be a *quadratic algebraic number* if it satisfies a polynomial equation

$$ax^2 + bx + c = 0,$$  \hfill (6.1)

where $a$, $b$, and $c$ are rational integers.

A *quadratic algebraic integer* is a quadratic algebraic number which satisfies a polynomial equation

$$x^2 + bx + c = 0,$$  \hfill (6.2)

where $b$ and $c$ are rational integers. The quadratic algebraic numbers are precisely the complex numbers of the form

$$\frac{-b + e\sqrt{d}}{2a},$$  \hfill (6.3)

where $a, b, d$, and $e$ are rational integers, and $d$ has no square factors other than 1. (We allow $d$ to be 1 so that the rational numbers are all quadratic algebraic numbers and the rational integers are all quadratic algebraic integers. That $d$ is 1 is equivalent to allowing the polynomial (6.1) to be factorable into two linear polynomial factors.) We shall call $d$ the *radicand* of a quadratic algebraic number $\alpha$. We shall also need the following notation: $\mathbb{Q}(\alpha)$ is the smallest field containing both $\mathbb{Q}$ and $\alpha$.

**Proposition 6.5.** Let $\alpha$ be any quadratic algebraic number of radicand $d$. Then $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{d}) = \{t + u\sqrt{d} : t, u \in \mathbb{Q}\}$. If $d$ is not a perfect
square, then \( \mathbb{Q}(\sqrt{d}) \) is a vector space of dimension 2 over the field of scalars \( \mathbb{Q} \) and has a basis \( <1, \sqrt{d}> \) over \( \mathbb{Q} \).

**Proof.** Any element \( \zeta \) of \( \mathbb{Q}(\alpha) \) is a finite sum of powers of \( \alpha \) multiplied by rational numbers. However, since \( \alpha \) satisfies a quadratic equation (6.2) with rational integer coefficients, we may substitute \( -(b/a)\alpha - c/a \) for \( \alpha^2 \) and reduce any powers higher than the first by one. Repeating this will eliminate all powers higher than the first. Thus \( \mathbb{Q}(\alpha) = \{t + u\sqrt{d} : t, u \in \mathbb{Q}\} \). The same process shows that \( \mathbb{Q}(\sqrt{d}) \) is the same set. That this set is the vector space as described is equally clear.

Let \( d \neq 1 \) be a rational integer without square factors (except 1). We define \( \Delta \) as follows:

a) if \( d \equiv 2 \) or \( d \equiv 3 \pmod{4} \), \( \Delta = 4d \);

b) if \( d \equiv 1 \pmod{4} \), \( \Delta = d \).

Now, with \( d \) and \( \Delta \) as defined, we shall call \( \mathbb{Q}(\sqrt{d}) \) the quadratic number field of radicand \( d \) and discriminant \( \Delta \). We note that \( \mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{\Delta}) \).

**Proposition 6.6.** Let \( d \neq 1 \) be a rational integer without square factors (except 1). The set of quadratic algebraic integers of radicand \( d \) is

\[ \{a + b\sqrt{d} : a, b \in \mathbb{Z}\}, \text{ if } d \equiv 2, 3 \pmod{4}; \]

\[ \{(a + b\sqrt{d})/2 : a, b \in \mathbb{Z}, a \equiv b \pmod{2}\}, \text{ if } d \equiv 1 \pmod{4}. \]

This set is a ring under ordinary addition and multiplication.

**Proof.** Considering the above definitions and equations (6.1)-(6.3), we see that a quadratic algebraic number \( \alpha \) is a quadratic algebraic integer if and only if \( \alpha \) is of the form \((-b + \sqrt{d})/2\), where \( b^2 - 4c = e^2d \). Considering this last equation modulo 4, we have, for \( d \equiv 2 \) or \( d \equiv 3 \),
ind 4), that \( b \) and \( e \) must both be even rational integers. If \( d \equiv 1 \) (mod 4), then \( b \) and \( e \) must be both even or both odd. And, as in Proposition 6.5, to show that this is a ring really only requires the observation that addition and multiplication are closed on these sets.

We shall call the ring defined in Proposition 6.6 the ring of integers of \( \mathbb{Q}(\sqrt{d}) \), written \( \mathcal{O}(\sqrt{d}) \), or sometimes just \( \mathcal{O} \) if the context is clear. However, the distinct terms “algebraic integer” and “rational integer” shall be retained to avoid any possible confusion. That the “algebraic integers” mentioned are actually “quadratic algebraic integers” should be clear since we will not deal further with any algebraic numbers which are not elements of a quadratic field. For convenience in expression, we shall let \( \delta \) be \(-\sqrt{d}\) or \((1 - \sqrt{d})/2\) according as the discriminant of the field in question is even or odd. With this notation, the ring of integers \( \mathcal{O}(\sqrt{d}) \) can then be written as \( \{a + b\delta : a, b \in \mathbb{Z}\} \). This will allow us to simplify statements about integers by covering both the cases of even and odd discriminants. For any quadratic algebraic number \( \alpha = (−b + c\sqrt{d})/2a \), the conjugate of \( \alpha \), written \( \bar{\alpha} \), is \( \bar{\alpha} = (−b - c\sqrt{d})/2a \). The norm of \( \alpha \), written \( N(\alpha) \), is \( N(\alpha) = a\bar{\alpha} = (b^2 + c^2d)/4a^2 \).

The norm of an algebraic integer is always a rational integer and is a multiplicative function; that is, for any integers \( \alpha \) and \( \beta \), we have \( N(\alpha\beta) = N(\alpha) \cdot N(\beta) \). An element \( \varepsilon \) in a ring of quadratic algebraic integers is a unit of the ring if it has norm \( \pm 1 \). Two algebraic integers will be called associates if their quotient is a unit.

**Proposition 6.7.** If \( d \neq 1 \) is a rational integer without square factors except 1, then the units of \( \mathbb{Q}(\sqrt{d}) \) are precisely the elements of \( \mathcal{O}(\sqrt{d}) \) which have inverses in the ring \( \mathcal{O}(\sqrt{d}) \), and are the integers:

a) if \( d = -1, \pm 1 \) and \( \pm \sqrt{-1} \);
b) if \( d = -3, \pm 1 \) and \( (\pm 1 \pm \sqrt{-3})/2 \), with the \( \pm \) signs being independent;

c) if \( d < -3, \pm 1 \);

d) if \( d > 1, \pm 1 \) and \( \pm \varepsilon^n \) for any rational integer \( n \), where \( \varepsilon \) is the fundamental solution to the appropriate Pell equation (3.11) or (3.2).

**Proof.** In the discussion of the Pell equation, these results were all proved. The only reason to repeat the results here is to phrase them in terms of units in a quadratic number field.
6.3 Ideals in Quadratic Fields

We now state, but do not prove, a special case of a major theorem.

**Theorem 6.8.** If \( a \) is an ideal in a ring of integers \( \mathcal{O} = \mathcal{O}(\sqrt{d}) \), then there exist algebraic integers \( \alpha_1 \) and \( \alpha_2 \) in \( \mathcal{O} \) such that any element of \( a \) can be written uniquely as \( \alpha_1 x + \alpha_2 y \), with rational integers \( x \) and \( y \).

Such a pair \( < \alpha_1, \alpha_2 > \) is called a basis of the ideal \( a \). We shall frequently write \( a =< \alpha_1, \alpha_2 > \). The feature of this theorem on which we will rely is the uniqueness of representation of elements of \( a \).

**Theorem 6.9.** Any ideal \( a \) has a basis \( < a, b + g\delta > \), where \( a, b, \) and \( g \) are rational integers, \( a > 0, 0 \leq b < a, \) and \( 0 < g \leq a, \) and \( g \) divides both \( a \) and \( b \). The basis with these properties is unique.

**Proof.** We shall prove this theorem by means of several smaller propositions.

**Proposition 6.10.** Any ideal \( a \) has a basis \( < a, \beta > \), where \( a \) is a rational integer and \( \beta \) is a quadratic algebraic integer.

**Proof.** The integers \( \mathcal{O} \) are of the form \( a + b\delta \), for \( a \) and \( b \) rational integers. This must, of course, be true for the basis elements, so we may write \( \alpha_1 = a_1 + b_1\delta \) and \( \alpha_2 = a_2 + b_2\delta \) with \( a_1, a_2, b_1, b_2 \in \mathbb{Q} \). Since \( \alpha_1 x + \alpha_2 y = \alpha_1 (x + ky) + (\alpha_2 - k\alpha_1)y \) for any rational integer \( k \), we have that \( < \alpha_1, \alpha_2 - k\alpha_1 > \) (and by symmetry \( < \alpha_1 - k\alpha_2, \alpha_2 > \)) is an equivalent basis for \( a \). This fact allows us to perform the Euclidean algorithm on \( b_1 \) and \( b_2 \). When this is finished, we will have a basis \( < a, b + g\delta > \) for \( a \), with rational integers \( a, b, \) and \( g \), which is equivalent
to the basis $\langle \alpha_1, \alpha_2 \rangle$, and for which $0 \neq g = \gcd(b_1, b_2)$. We may then go one step further, subtracting multiples of $a$ from $b$, to be able to assume that $0 \leq b < a$.

**Proposition 6.11.** Any rational integer $m$ which is an element of an ideal $a$ is a multiple of $a$.

**Proof.** Clearly, if there is a unique representation for $m$ by Theorem 6.8, then the representation $m = ax + (b + g\delta)y$, using the basis of Proposition 6.10, must also be unique. This implies that $y$ must be zero.

**Proposition 6.12.** $N(b + g\delta)$ is a multiple of $a$.

**Proof.** This norm is a rational integer and is also an element of $a$; we apply Proposition 6.11.

**Proposition 6.13.** An ideal $a$ has a unique basis of the form $\langle a, b + g\delta \rangle$, with rational integers $a$, $b$, and $g$, $a > 0$, $0 \leq b < a$, and $0 < g \leq a$.

**Proof.** Given any basis for $a$, we have by Proposition 6.9 an equivalent basis of the form $\langle a, b + g\delta \rangle$, with $a$, $b$, and $g$ rational integers, and $a$ and $b$ satisfying the desired conditions. By Proposition 6.11, the rational integer $a$ is uniquely determined for the entire ideal, regardless of the initial choice of basis. Now, if there were distinct bases $\langle a, b + g\delta \rangle$ and $\langle a, b' + g'\delta \rangle$, then we could find rational integers $x$ and $y$ such that $ax + (b + g\delta)y = b' + g'\delta$. This would require us to have $ax + by = b'$ and $gy = g'$. However, if both $b$ and $b'$ lie between 0 and $a$, we must have $x = 0$ and $y = 1$. This proves that $g$ is unique. That $g$ must also satisfy the above condition follows from the following
argument. Since $a$ is an element of $\mathfrak{a}$, so is $a\delta$. Thus there is a unique representation $a\delta = ax + (b + g\delta)y$. This, however, implies that $gy = a$ so that we must have $0 < g \leq a$.

**Proposition 6.14.** $g$ divides $a$ and $b$.

**Proof.** Using Proposition 6.12 we see that any common factor of $a$ and $g$ must also divide $b$. Thus, with no loss of generality, we may assume that $a$ and $g$ are relatively prime, having already removed the common factors. Let $x$ and $y$ be rational integers chosen so that $ax + by = 1$. Since we have $a \in \mathfrak{a}$ and since $\delta \in \mathcal{O}$, we have $a\delta \in \mathfrak{a}$. Thus $ax\delta + (b + g\delta)y = by + \delta$ is an element of $\mathfrak{a}$. However, we have a basis for $\mathfrak{a}$, so rational integers $r$ and $s$ exist such that $ar + s(b + g\delta) = by + \delta$. We conclude that $sg = 1$ and that $g$, being positive, is 1.

Propositions 6.10 through 6.14 prove Theorem 6.9. The basis defined by Theorem 6.9 is called the *canonical basis* for the ideal $\mathfrak{a}$. We now turn Theorem 6.9 around.

**Theorem 6.15.** Let $a$, $b$, $g$, and $k$ be rational integers, with $a > 0$, $0 \leq b < a$, $0 < g \leq a$, and $N(b + g\delta) = ka$. Then the ideal

$$\mathfrak{a} = \{a\alpha + (b + g\delta)\beta : \alpha, \beta \in \mathcal{O}\}$$

has canonical basis $<a, b + g\delta>$. 

**Proof.** Without loss of generality we may assume that $g = 1$. The ideal $\mathfrak{a}$ has some canonical basis $<t, r + s\delta>$. Since $b + \delta$ is in $\mathfrak{a}$ and since the canonical basis provides a unique representation for any element of the ideal, it is evident that we must have $s = 1$. What we shall now show is that all rational integers which are elements of $\mathfrak{a}$ are multiples of $a$. This would imply that $t = a$. Since this is true, and
since \( b + \delta \) and \( r + \delta \) are both elements of \( a \), so is their difference \( b - r \), which is a rational integer and therefore a multiple of \( a \). But from \( 0 \leq b < a \) and \( 0 \leq r < a \) we must then conclude that \( b = r \), which proves the theorem.

Now, the elements of \( a \) are the numbers of the form \( a\alpha + (b + \delta)\beta \), where \( \alpha \) and \( \beta \) are arbitrary algebraic integers of \( \mathcal{O} \). That is to say, they are the numbers

\[
a(x_1 + y_1\delta) + (b + \delta)(x_2 + y_2\delta) = ax_1 + bx_2 + y_2\delta^2 + \delta(ay_1 + by_2 + x_2),
\]

where \( x_1, x_2, y_1, \) and \( y_2 \) run through all the rational integers. In order that these numbers be rational integers, we must have \( ay_1 + by_2 + x_2 = 0 \), that is to say, \( ay_1 + by_2 = -x_2 \). In the case that \( \delta = -\sqrt{d} \), the rational integers in \( a \) are thus all of the form

\[
ax_1 + bx(-ay_1 - by_2) + y_2d = ax_1 - aby_1 - (b^2 - d)y_2 = ax_1 - aby_1 - k\gamma y_2.
\]

The case for odd discriminants is similar, but again more tedious.

Given any ideal \( a = \langle \alpha_1, \alpha_2 \rangle \), we define the norm of \( a \), written \( N(a) \), to be \( |\alpha_1\bar{\alpha}_2 - \bar{\alpha}_1\alpha_2|/\sqrt{\Delta} \), where \( \Delta \) is the discriminant of the field of radicand \( d \). None of the changes of basis used in proving Theorem 6.9 affect this quantity, so the norm of an ideal is well-defined regardless of basis and is in fact equal to \( a \) if the ideal is written with the canonical basis.

The product of two ideals \( a \) with basis \( \langle \alpha_1, \alpha_2 \rangle \) and \( b \) with basis \( \langle \beta_1, \beta_2 \rangle \) is defined simply as the ideal generated by \( \mathbb{Z}\text{-linear} \)
combinations of $\alpha_1 \beta_1$, $\alpha_1 \beta_2$, $\alpha_2 \beta_1$, and $\alpha_2 \beta_2$. A fractional ideal is a subset $I$ of $\mathbb{Q}(\sqrt{\Delta})$ for which the following two properties hold:

a) for any $\alpha, \beta \in I$, then for any $\lambda, \mu \in \mathcal{O}$, $\lambda \alpha + \mu \beta \in I$.

b) there exists an fixed algebraic integer $\nu$ such that, for every $\alpha \in I$,

$\nu \alpha \in \mathcal{O}$.

Clearly, every ideal (hereafter called "integral ideal") is also a fractional ideal. Intuitively, the fractional ideals are the closed linear combinations with a "common denominator." If we define $\nu$ as in b), then the set $\{\nu \alpha : \alpha \in I\}$ is an integral ideal, which has a canonical basis $<a, b + g\delta>$, and thus $I$ has a basis $<a/\nu, (b + g\delta)/\nu>$.

We define an ideal $a$ to be principal if there exists an algebraic integer $\alpha$ such that $a = \{\lambda \alpha : \lambda \in \mathcal{O}\}$. A principal ideal has a canonical basis, but we shall usually write simply $(\alpha)$, the ideal being in fact the set $(\alpha)\mathcal{O}$. We define two (integral or fractional) ideals $a$ and $b$ to be equivalent if there is a principal ideal $(\alpha)$ such that $a = (\alpha)b$. These ideals are narrowly equivalent if the norm of $\alpha$ is positive. The ideal $a$ conjugate to $a$ is the ideal with basis $<a, b + g\delta>$. Clearly $a$ is an ideal, although this basis is not necessarily the canonical basis.

We now prove a major theorem.

**Theorem 6.16.** Given any integral ideal $a$, there exists an integral ideal $b$ such that $ab$ is a principal ideal.

**Proof.** This theorem is actually true for ideals in any ring of algebraic integers, although the proof in general can be much more difficult. We shall take advantage of the fact that we work only in quadratic fields to prove this in a brutal, but elementary, way. We let $a = <a, b + g\delta>$ with the canonical basis. It is easy to see that we may remove the
principal ideal factor \((g)\) from \(a\): \(a = (g)a'\), with \(a'\) having a canonical basis \(<a/g, (b/g + \delta)\>\), and these are all integral ideals. Therefore, we need only consider ideals whose canonical basis has \(g = 1\).

Consider now the product \(I = a\tilde{a}\). This is the ideal consisting of all elements of \(\mathcal{O}\) of the form

\[
a^2xz + a(b + \delta)yz + a(b + \delta)xw + (b + \delta)(b + \delta)yw,
\]

where \(x, y, z,\) and \(w\) independently run through all possible rational integers. We note that \((b + \delta)(b + \delta)\) is a rational integer and is a multiple \(ka\) of \(a\). Thus the product consists of all elements of \(\mathcal{O}\) of the form

\[
a[axz + (b + \delta)yz + (b + \delta)xw + kyw]. \tag{6.4}
\]

This product ideal is, in fact, \((a)\). The principal ideal \((a)\) has canonical basis \(<a, a\delta>\). We first show that the expression in brackets in (6.4) represents 1. We shall prove this only for the case \(\delta = -\sqrt{d}\); the other case is similar, but more tedious and no more enlightening. It is easy to see that the expression represents \(a, k,\) and \(2b\) and hence represents \(\gcd(a, k, 2b)\). Now, using the equation \(b^2 - d = ka\) as a congruence modulo 4, we can readily see that at least one of \(a\) and \(k\) must be odd so that \(\gcd(a, k, 2b) = \gcd(a, k, b)\); this rational integer is represented by the expression in question. But by the same equation, if any prime \(p\) divides \(a, k,\) and \(b\) simultaneously, we must have \(p^2\) dividing \(d\); this contradicts our definition of \(d\).

Now, since the expression above represents 1, it must be the case that \(a\) is the smallest positive rational integer in the ideal \(I\). Thus the canonical basis for \(I\) is of the form \(<a, t + r\sqrt{d}>\), for some rational integers \(t\) and \(r\). But this would imply that, for any rational integer \(y,\)
(t + r\sqrt{d})y \in I. Looking again at (6.4), we see that every element of I is of the form an + am\sqrt{d}, for rational integers n and m. We conclude that t is zero and that r is a, proving the theorem.

It is immediately seen that Theorem 6.16 carries over to fractional ideals as well as integral ideals. We state, without proof, a straightforward proposition and use it to derive a main theorem.

**Proposition 6.17.**

a) The equivalence defined on ideals is an equivalence relation.

b) The narrow equivalence defined on ideals is an equivalence relation.

c) If, for ideals a and b, we have a \sim b, then for any ideal c, we have ac \sim bc.

d) If, for ideals a, b, and c, with c not the zero ideal, we have ac \sim bc, then we have a \sim b.

**Theorem 6.18.** The equivalence classes (respectively, narrow equivalence classes) of fractional ideals of a ring of quadratic algebraic integers \( \mathcal{O} \) form an abelian group under multiplication of ideals. The identity of the group is the class of all principal ideals (respectively, the class of all principal ideals \( \alpha \) with \( N(\alpha) > 0 \)).

**Proof.** The proof is immediate from part d) of the proposition above. The set of ideals by themselves forms a monoid—a set with a closed associative multiplication and an identity—and the introduction of the equivalence relation, together with Theorem 6.16, provides the means for obtaining the inverse of any class.
The groups of classes of ideals and of narrow classes of ideals are called the class group and the narrow class group of the field. The difference between equivalence and narrow equivalence is summed up as follows. For negative field discriminants $\Delta$, all norms are positive, and thus equivalence and narrow equivalence are identical. For positive field discriminants $\Delta$, norms may be positive or negative. Since the units of the ring of algebraic integers are precisely the elements of the ring which have inverses in the ring, multiplication of any ideal by a unit leaves the ideal unchanged. If there exists a unit $\varepsilon$ in $\mathcal{O}$ of norm $-1$, then all equivalent ideals are narrowly equivalent—the principal ideals $(\alpha)$ and $(\varepsilon\alpha)$ are equal, and one of $N(\alpha)$ and $N(\varepsilon\alpha)$ is positive. If there exists no such unit, then every equivalence class splits into two narrow equivalence classes.

**Theorem 6.19.**

a) If the discriminant $\Delta$ of the quadratic field $\mathbb{Q}(\sqrt{\Delta})$ is negative, then the class group and the narrow class group are isomorphic.

b) If the discriminant $\Delta$ of the quadratic field $\mathbb{Q}(\sqrt{\Delta})$ is positive, and a solution exists to the equation

$$x^2 - \Delta y^2 = -4,$$

then the class group and the narrow class group are isomorphic.

c) If the discriminant $\Delta$ of the quadratic field $\mathbb{Q}(\sqrt{\Delta})$ is positive, and no solution exists to the equation

$$x^2 - \Delta y^2 = -4,$$
then the class group consists of the subgroup of squares of the narrow class group.
6.4 Binary Quadratic Forms and Classes of Ideals

We can now prove the theorem which is the major object of this chapter.

**Theorem 6.20.** The group of classes of binary quadratic forms of discriminant $\Delta$ is isomorphic to the narrow class group of the quadratic number field $\mathbb{Q}(\sqrt{\Delta})$.

**Proof.** We follow somewhat the proof used in Hecke [HECK]. We shall show that to any ideal there corresponds a form, that to any form corresponds an ideal, and then that equivalent ideals correspond to equivalent forms, and conversely.

Any ideal $\alpha$ has a basis $\langle \alpha_1, \alpha_2 \rangle$. We choose to order the basis so that $\alpha_1 \overline{\alpha}_2 - \overline{\alpha}_1 \alpha_2 = N(\alpha) \sqrt{(\Delta)}$ is positive or positive imaginary. The binary quadratic form of discriminant $\Delta$ which we associate with this ideal is

$$\frac{[\alpha_1 x + \alpha_2 y][\overline{\alpha}_1 x + \overline{\alpha}_2 y]}{N(\alpha)}.$$

This is indeed a binary quadratic form with rational integer coefficients and discriminant $\Delta$, as can be verified by direct calculation. Further, for a negative discriminant, this is a positive definite form. We say that the form belongs to $\alpha$.

Conversely, with any binary quadratic form $(A, B, C)$ of discriminant $\Delta$ we can associate the ideal

$$\{A\alpha + (b + \delta)\beta : \alpha, \beta \in \mathcal{O}\}$$

if $A > 0$ and
\{A \delta \alpha + (b + \delta) \beta : \alpha, \beta \in \mathcal{O}\}

if \(A < 0\), where \(b\) is \(B/2\) or \((B - 1)/2\) according as \(\Delta\) is even or odd.

Now, by adding or subtracting rational integral multiples of \(A\) from \(b\), we produce an identical (not just equivalent) ideal

\[\{A \alpha + (b' + \delta) \beta : \alpha, \beta \in \mathcal{O}\}\]

or

\[\{A \alpha \delta + (b' + \delta) \beta : \alpha, \beta \in \mathcal{O}\},\]

with \(0 \leq b' < |A|\). Thus \(A\), \(b' + \delta\) is a canonical basis for an ideal, so that the ideal associated with the binary quadratic form \((A, B, C)\) has a basis \(A, b + \delta\) or \(A\delta, b\delta + \delta^2\), depending on whether \(A\) is positive or negative. Significantly, the norm of either ideal is positive or positive imaginary, and the form which belongs to that ideal is the original form \((A, B, C)\). Thus, to every binary quadratic form there corresponds an ideal to which that form belongs.

To show that equivalent forms belong to equivalent ideals and conversely, we need only show that this is true for the generators \(S\) and \(T\) of the modular group \(\Gamma\). For the generator \(S\) this has already been done—this is adding or subtracting multiples of \(A\) to \(b\). The other matrix produces the equivalence of forms \((A, B, C) \sim (C, -B, A)\). This corresponds to the following narrow ideal equivalence. The ideal

\[\{A \alpha + (b + \delta) \beta : \alpha, \beta \in \mathcal{O}\}\]

is narrowly equivalent to the ideal

\[\{A(b + \delta) \alpha + (b + \delta)(b + \delta) \beta : \alpha, \beta \in \mathcal{O}\}\]
if $N(b + \delta)$ is positive. If this norm is positive, then $A$ and $C$ are of like sign. We remove either the principal ideal $(A)$ or $(-A)$ to obtain an equivalent ideal

$$\{(b + \delta)\alpha + C\beta : \alpha, \beta \in \mathcal{O}\}$$

or

$$\{(-b - \delta)\alpha - C\beta : \alpha, \beta \in \mathcal{O}\}.$$  

Both of these are equal to an ideal

$$\{C\alpha - (b' + \delta)\beta : \alpha, \beta \in \mathcal{O}\}.$$  

If $C$ is positive, this is the ideal associated with a form $(C, B', \ast)$ equivalent under some matrix transformation $S^n$ to $(C, -B, A)$. If $C$ is negative, we must carry a factor of $\delta$ throughout; the form correspondence, however, is the same.

We make a final observation concerning the ability to use forms to explicitly compute in quadratic number fields. Given a field discriminant $\Delta$ and the field $\mathbb{Q}(\sqrt{\Delta})$, we can separate the rational primes $p$ into three categories.

a) $p$ divides $\Delta$. Then $p$ is representable by an ambiguous form $(p, p, \ast)$ of discriminant $\Delta$. Thus there is an ideal $p = < p, (-p + \sqrt{\Delta})/2 >$ of norm $p$ in $\mathcal{O}$, and the ideal $p$ is its own conjugate in the ring of algebraic integers. Such prime ideals $(p)$ in the rational integers are said to ramify in $\mathbb{Q}(\sqrt{\Delta})$. We note that the statement that the ideal is self-conjugate is equivalent to the statement that its square is a principal ideal since the product of any ideal $a$ and its conjugate $\bar{a}$ is always the principal ideal $(N(a))$.  

b. $p$ does not divide $\Delta$, and $b^2 \equiv \Delta \pmod{p}$ is solvable. Then there exist two inequivalent forms $(p, \pm b, *)$ of discriminant $\Delta$ which represent $p$. There are correspondingly two inequivalent but conjugate ideals $\mathfrak{p} = \langle p, (-p + \sqrt{\Delta})/2 \rangle$ and $\mathfrak{p} = \langle p, (+p + \sqrt{\Delta})/2 \rangle$ of norm $p$ in $\mathcal{O}$. Their product is the principal ideal $(p)$ of norm $p^2$. In this case $p$ is said to split in $\mathbb{Q}(\sqrt{\Delta})$.

c. $p$ does not divide $\Delta$, and $b^2 \equiv \Delta \pmod{p}$ is not solvable. There exist no forms of discriminant $\Delta$ which represent $p$, and no ideals of norm $p$ in $\mathcal{O}$. We can always represent $p^2$, however, by the principal form if by no other way. Such primes are said to remain prime in $\mathbb{Q}(\sqrt{\Delta})$, and any forms which represent $p^2$ must be in the principal genus since all quadratic characters for a perfect square must be $+1$. 
6.5 History

We have defined binary quadratic forms

\[ f(x, y) = ax^2 + bxy + cy^2 \]

of discriminant \( b^2 - 4ac = \Delta \). This is the definition of forms according to Eisenstein, and turns out, as we have seen, to be the appropriate definition for making the correspondence between the groups of classes of forms and the classes of ideals of quadratic number fields. It is entirely for this reason that Eisenstein forms have been considered in this book.

Following most mathematicians before him, however, Gauss in the *Disquisitiones Arithmeticae* defined forms to be

\[ \phi(x, y) = ax^2 + 2bxy + cy^2 \]

of determinant \( b^2 - ac = \delta \). There are annoying complications with either definition. With the Eisenstein forms, 2 has a special place and the odd and even discriminants usually have to be handled separately. With the forms of Gauss, both *properly primitive* forms, for which \( \gcd(a, 2b, c) = 1 \), and *improperly primitive* forms, for which \( \gcd(a, 2b, c) = 2 \), must be considered. Further complications arise, but none so serious as the fact that the groups of classes of Gauss forms do not correspond directly with all the class groups of quadratic number fields, and so do not provide the significant advantage of an elementary and explicit way for doing number-theoretic computations in those fields.