4

Quadratic Forms

We began our study of quadratic number theory with questions about sums of two squares. We saw that we could use the uniqueness of irreducible factorization in the Gaussian integers to describe the integers represented by $x^2 + y^2$. In §2.5, we found that we could similarly describe representations of integers by the principal form of discriminant Δ in cases where D_Δ is a unique factorization domain. While we found that unique factorization into irreducible elements is the exception in quadratic domains, we demonstrated in Chapter 3 that unique factorization into prime ideals occurs in every complete quadratic domain, and with every complete ideal in an arbitrary quadratic domain.

Our goal now is to apply prime ideal factorization to representations of integers by arbitrary binary quadratic forms. In this chapter, we compile definitions and terminology for these quadratic forms as objects in their own right. In particular, we introduce in §4.1 a notation for quadratic forms that is very similar to our numerical notation for ideals. Using an equivalence relation on quadratic forms defined in §4.2, we establish a criterion for representation of an integer by some quadratic form of a particular discriminant, and a formula for the number of such representations in §4.3. In Chapter 5, we will then see that our notation allows us to apply, in several ways, a close connection between quadratic forms and ideals.

4.1 Classification of Quadratic Forms

The following definition generalizes examples of quadratic expressions previously considered.

Definition. A *binary quadratic form*, which we will call simply a *quadratic form*, is a homogeneous degree two polynomial in two variables,

$$f(x,y) = ax^2 + bxy + cy^2, \tag{4.1.1}$$

with integer *coefficients* a, b, and c. The *discriminant* of f is

$$\Delta = \Delta(f) = b^2 - 4ac,$$

and we denote the set of all quadratic forms of discriminant Δ as $\mathcal{Q}_\Delta$. We say that f *represents* the integer m if $f(q,r) = m$ for some integers q and r, and that f *properly represents* m if $f(q,r) = m$ with $\gcd(q,r) = 1$.

If $f(q,r) = aq^2 + bqr + cr^2 = m$, then direct calculation shows that

$$4am = (2aq + br)^2 - \Delta r^2 \quad \text{and} \quad 4cm = (2cr + bq)^2 - \Delta q^2. \tag{4.1.2}$$

If Δ is a square, we can factor the right-hand side of each equation in (4.1.2) and solve for q and r by elementary means. We will assume instead that Δ is not a square. (Then Δ is a *discriminant* as defined in §2.2.) In that case, $f(q,r) = 0$ if and only if $q = 0 = r$. In particular, $f(1,0) = a$ and $f(0,1) = c$ cannot be zero. If Δ is positive, then (4.1.2) shows that f can represent either positive or negative integers. If Δ is negative, then all values of $f(q,r)$ have the same sign as a when $(q,r) \neq (0,0)$.

Definition. Let $f(x,y) = ax^2+bxy+cy^2$ be a quadratic form, with discriminant $\Delta = b^2 - 4ac$.

(1) If Δ is positive, we say that f is *indefinite*.

(2) If Δ is negative and a is positive, we say that f is *positive definite*.

(3) If Δ is negative and a is negative, we say that f is *negative definite*.

Definition. If $f(x,y) = ax^2+bxy+cy^2$ is a quadratic form, we define the *index* of f to be $\gamma(f) = \gcd(a,b,c)$. We say that f is *primitive* if $\gamma(f) = 1$.

If $\gamma(f) = \gamma$, with $a = \gamma a_1$, $b = \gamma b_1$, and $c = \gamma c_1$, then

$$\Delta(f) = \gamma^2(b_1^2 - 4a_1c_1) = \gamma^2\Delta_1$$

with $\Delta_1 \equiv 0$ or $1 \pmod 4$. It follows that the index of a quadratic form f of discriminant Δ divides the index of Δ, as defined in (2.2.1). That is, if $\Delta = \Delta(d,\gamma)$, then $\gamma(f)$ divides γ for each f in $\mathcal{Q}_\Delta$. In particular, if Δ is a primitive discriminant, then all quadratic forms in $\mathcal{Q}_\Delta$ are primitive.

The Matrix of a Quadratic Form. If f is a quadratic form, we can associate a particular 2×2 matrix to f, and calculate $f(q,r)$ for integers q and r via matrix multiplication. This will be useful for several definitions in this chapter.

Definition. If $f(x,y) = ax^2 + bxy + cy^2$ is a quadratic form, then the *matrix* of f is

$$M_f = \begin{bmatrix} 2a & b \\ b & 2c \end{bmatrix}. \tag{4.1.3}$$

The matrix of f is *symmetric*, that is, $M_f^T = M_f$. (In general, A^T denotes the *transpose* of a matrix A, that is, the matrix obtained by interchanging the rows and columns of A.) The discriminant of f is the negative of the determinant of M_f. If $\mathbf{x}$ is a column matrix with entries q and r, then

$$\mathbf{x}^T M_f \mathbf{x} = \begin{bmatrix} q & r \end{bmatrix} \cdot \begin{bmatrix} 2a & b \\ b & 2c \end{bmatrix} \cdot \begin{bmatrix} q \\ r \end{bmatrix} = [2f(q,r)]. \tag{4.1.4}$$

We may write $f(q,r) = f(\mathbf{x}) = \frac{1}{2}\mathbf{x}^T M_f \mathbf{x}$ in this case, identifying $\mathbf{x}$ with the ordered pair (q,r), and $f(\mathbf{x}) = m$ with the 1×1 matrix having m as its single entry.

Definition. If A is a 2×2 matrix, define the *conjugate* of A, written as $\overline{A}$, to be the matrix obtained by changing the sign of the off-diagonal entries of A. That is, if $A = \begin{bmatrix} q & s \\ r & t \end{bmatrix}$, then $\overline{A} = \begin{bmatrix} q & -s \\ -r & t \end{bmatrix}$.

Exercise 4.1.1. Let A and B be 2×2 matrices.

(a) Show that the determinant of A equals the determinant of $\overline{A}$.

(b) Show that $\overline{A} + \overline{B} = \overline{A+B}$.

(c) Show that $\overline{A}\cdot\overline{B} = \overline{A\cdot B}$.

Definition. Let $f(x,y) = ax^2 + bxy + cy^2$ be a quadratic form of discriminant Δ. Then the *conjugate* of f is $\overline{f}(x,y) = ax^2 - bxy + cy^2$, the *negative* of f is $-f(x,y) = -ax^2 - bxy - cy^2$, and the *negative conjugate* of f is $-\overline{f}(x,y) = -ax^2 + bxy - cy^2$.

If f is an element of $\mathcal{Q}_\Delta$, then $\overline{f}$, $-f$, and $-\overline{f}$ are likewise elements of $\mathcal{Q}_\Delta$. We have the following relation between the matrix of f and the matrices of these associated forms:

$$M_{(\overline{f})} = \overline{M_f}, \qquad M_{(-f)} = -M_f, \qquad M_{(-\overline{f})} = -\overline{M_f}.$$

Exercise 4.1.2. Let $f(x,y) = ax^2 + bxy + cy^2$ and let

$$\overline{f}(x,y) = ax^2 - bxy + cy^2 \quad \text{and} \quad -f(x,y) = -ax^2 - bxy - cy^2$$

be its conjugate and negative, respectively.

(a) Show that if $f(q,r) = m$, then $\overline{f}(q,-r) = m$.

(b) Show that f represents an integer m if and only if $\overline{f}$ represents m.

(c) Show that f represents m if and only if $-f$ represents $-m$.

Ideal Notation for Quadratic Forms. The following observation allows us to classify all quadratic forms of discriminant Δ, using a notation similar to that of ideals of the quadratic domain D_Δ.

Proposition 4.1.1. *Let $\phi(x)$ be the principal polynomial and let ε be the basis index of some discriminant Δ. If $f(x,y) = ax^2 + bxy + cy^2$ is a quadratic form of discriminant Δ, then $k = \frac{b-\varepsilon}{2}$ is an integer and $\phi(k) = ac$. Conversely, if a and k are integers for which a divides $\phi(k)$, and we let $b = \phi'(k)$ and $c = \frac{1}{a}\phi(k)$, then $f(x,y) = ax^2 + bxy + cy^2$ is a quadratic form of discriminant Δ.*

Proof. If $f(x,y) = ax^2 + bxy + cy^2$ is a quadratic form with $\Delta = b^2 - 4ac$, then b has the same parity as Δ, as does ε, as we saw in §2.2. So $k = \frac{b-\varepsilon}{2}$ is an integer, and we find that

$$\begin{aligned}\phi(k) &= \left(\frac{b-\varepsilon}{2}\right)^2 + \varepsilon\left(\frac{b-\varepsilon}{2}\right) + \frac{\varepsilon^2-\Delta}{4} \\ &= \frac{b^2 - 2b\varepsilon + \varepsilon^2 + 2b\varepsilon - 2\varepsilon^2 + \varepsilon^2 - \Delta}{4} = \frac{b^2-\Delta}{4} = ac.\end{aligned}$$

Conversely, let a and k be integers for which a divides $\phi(k)$, say with $\phi(k) = ac$, and let $b = \phi'(k) = 2k + \varepsilon$. Then

$$b^2 - 4ac = \phi'(k)^2 - 4\phi(k) = 4k^2 + 4\varepsilon k + \varepsilon^2 - 4\left(k^2 + \varepsilon k + \frac{\varepsilon^2-\Delta}{4}\right) = \Delta,$$

so that $f(x,y) = ax^2 + bxy + cy^2$ has discriminant Δ. □

Thus for a fixed discriminant Δ, binary quadratic forms f in $\mathcal{Q}_\Delta$ are in one-to-one correspondence with pairs of integers a and k for which a divides $\phi_\Delta(k)$. With this in mind, we introduce the following notation.

Definition. If $f(x,y) = ax^2 + bxy + cy^2$ is a quadratic form of discriminant Δ, and $k = \frac{b-\varepsilon}{2}$, where $\varepsilon = \varepsilon_\Delta$, then we also write $f = (a : k)_\Delta$, or $f = (a : k)$ if Δ is apparent from the context. Conversely, if $\phi(x)$ is the principal polynomial

of some discriminant Δ, and a and k are integers for which a divides $\phi(k)$, we write $f = (a : k)$ to denote the quadratic form $f(x, y) = ax^2 + bxy + cy^2$, where $b = \phi'(k)$ and $c = \frac{1}{a}\phi(k)$. We refer to $f(x, y) = ax^2 + bxy + cy^2$ as *standard notation* for a quadratic form f, and to $(a : k)$ as *ideal notation* for f, because of its similarity to our way of writing ideals of a quadratic domain.

Example. Since $a = 1$ divides $\phi(0) = \frac{\varepsilon^2 - \Delta}{4}$, we have that

$$(1 : 0)_\Delta = x^2 + \varepsilon xy + \frac{\varepsilon^2 - \Delta}{4} y^2.$$

This is same as the principal form, $\phi(x, y)$, of discriminant Δ as defined in equation (2.2.6). That is, $\phi = (1 : 0)$ in every set $\mathcal{Q}_\Delta$. ◊

Example. Let $\Delta = 13$, so that $\phi(x) = x^2 + x - 3$. For a particular integer a, we can determine all elements $(a : k)$ in $\mathcal{Q}_{13}$ by solving the congruence $x^2 + x - 3 \equiv 0 \pmod{a}$. For example, we find that $x^2 + x - 3 \equiv 0 \pmod{3}$ has solutions 0 and 2. So $\mathcal{Q}_{13}$ contains $(3 : k)$ and $(-3 : k)$ if and only if $k \equiv 0$ or $2 \pmod{3}$. Here $b = 2k + 1$ and $ac = k^2 + k - 3$, so that

$$(3 : 0) = 3x^2 + xy - y^2, \qquad (-3 : 2) = -3x^2 + 5xy - y^2,$$

and so forth. On the other hand, $x^2 + x - 3 \equiv 0 \pmod{5}$ has no solutions, so that $\mathcal{Q}_{13}$ contains no elements of the form $(5 : k)$ or $(-5 : k)$. ◊

Exercise 4.1.3. For each of the following quadratic forms $f(x, y)$, calculate the discriminant of f and write f using ideal notation.

(a) $f(x, y) = 5x^2 - 3xy + 7y^2$.

(b) $f(x, y) = 3x^2 - 6xy + 2y^2$.

(c) $f(x, y) = 6x^2 + 10xy + y^2$.

Exercise 4.1.4. Let $\Delta = -31$. For each of the following values of a, find (a pattern for) all values of k for which $(a : k)$ is an element of $\mathcal{Q}_\Delta$.

(a) $a = 5$.

(b) $a = 7$.

(c) $a = 35$.

Exercise 4.1.5. Let $f(x, y) = ax^2 + bxy + cy^2$ be a quadratic form of discriminant Δ, and suppose that $f = (a : k)$ in ideal notation.

(a) Show that $\overline{f} = (a : -k - \varepsilon)$.

(b) Show that $-f = (-a : -k - \varepsilon)$.

(c) Show that $-\overline{f} = (-a : k)$.

4.2 Equivalence of Quadratic Forms

We saw in §4.1 that if f is a quadratic form, then we can associate a particular 2×2 matrix to f, and calculate $f(q, r)$ for integers q and r via matrix multiplication. In this section, we demonstrate that this viewpoint allows us to define several equivalence relations on the set of all quadratic forms of some fixed discriminant, an important step in classifying these forms.

Definition. Let

$$\Gamma = \left\{ U = \begin{bmatrix} q & s \\ r & t \end{bmatrix} \mid q, r, s, t \in \mathbb{Z} \text{ and } \det U = qt - rs = 1 \right\}.$$

We refer to an element of Γ as a *unimodular* matrix. If M_f is the matrix of a quadratic form as in (4.1.3), and U is unimodular as above, then

$$\begin{aligned} U^T M_f U &= \begin{bmatrix} q & r \\ s & t \end{bmatrix} \cdot \begin{bmatrix} 2a & b \\ b & 2c \end{bmatrix} \cdot \begin{bmatrix} q & s \\ r & t \end{bmatrix} \\ &= \begin{bmatrix} 2(aq^2 + bqr + cr^2) & 2aqs + b(qt + rs) + 2crt \\ 2aqs + b(qt + rs) + 2crt & 2(as^2 + bst + ct^2) \end{bmatrix} \end{aligned}$$

is the matrix of a quadratic form g given by

$$\begin{aligned} (aq^2 + bqr + cr^2)x^2 + (2aqs + b(qt + rs) + 2crt)xy \\ + (as^2 + bst + ct^2)y^2. \end{aligned} \quad (4.2.1)$$

We write $g = f \circ U$ to mean that g is obtained from f via U in this way.

Exercise 4.2.1. Show that the set Γ of all unimodular matrices is a group under matrix multiplication. (Assume that the set of all nonsingular 2×2 matrices with real number entries is a group under matrix multiplication. Thus it suffices to show that Γ is closed under multiplication, and that the inverse of an element of Γ is also in Γ.)

Exercise 4.2.2. Let f be a quadratic form. If U is a unimodular matrix and $V = -U$, show that $f \circ U = f \circ V$.

The quadratic forms f and $g = f \circ U$ have the same discriminant, since $\det(U^T M_f U) = \det(U^T) \cdot \det(M_f) \cdot \det(U) = \det(M_f)$. Thus we can view the mapping that takes f to $f \circ U$ as a function on the set $\mathcal{Q}_\Delta$ for a fixed discriminant Δ. More precisely, the following exercise indicates that we have a *group action* by Γ on the set $\mathcal{Q}_\Delta$.

Exercise 4.2.3. Let I be the 2×2 identity matrix, and let U and V be unimodular matrices. Let f, g, and h be quadratic forms in $\mathcal{Q}_\Delta$ for some discriminant Δ.
(a) Show that $f \circ I = f$.

(b) Show that if $g = f \circ U$, then $f = g \circ U^{-1}$.

(c) Show that if $g = f \circ U$ and $h = g \circ V$, then $h = f \circ (UV)$.

Definition. Let H be a subgroup of the group Γ of 2×2 unimodular matrices. Then we define a relation $\sim_H$ on the set $\mathcal{Q}_\Delta$ of quadratic forms of determinant Δ by saying that $f \sim_H g$ if and only if $g = f \circ U$ for some U in H. If H is the entire group Γ, we write $\sim_H$ simply as $\sim$. We say that f is *equivalent* to g, and that f and g are in the same *class*, if $f \sim g$.

Exercise 4.2.4. If H is a subgroup of Γ, show that $\sim_H$ is an equivalence relation on $\mathcal{Q}_\Delta$. Show that if $f \sim_H g$ for some subgroup H of Γ, then $f \sim g$ is also true.

Exercise 4.2.5. Let f and g be quadratic forms of discriminant Δ, with the negatives of f and g defined as in §4.1. Show that if f is equivalent to g, then $-f$ is equivalent to $-g$. Specifically, show that if $g = f \circ U$, then $-g = -f \circ U$.

Exercise 4.2.6. Let f and g be quadratic forms of discriminant Δ, with the conjugates of f and g defined as in §4.1. Show that if f is equivalent to g, then $\overline{f}$ is equivalent to $\overline{g}$. Specifically, show that if $g = f \circ U$, then $\overline{g} = \overline{f} \circ \overline{U}$, where $\overline{U}$ is the conjugate of U as defined in §4.1.

Equivalence of Quadratic Forms in Ideal Notation. We can apply U to a form written in ideal notation, according to the following proposition.

Proposition 4.2.1. *Let $\phi(x)$ be the principal polynomial of discriminant Δ, and let $f = (a : k)$ be in $\mathcal{Q}_\Delta$, with $\phi(k) = ac$ and $\phi'(k) = b$. Let $U = \begin{bmatrix} q & s \\ r & t \end{bmatrix}$ be a unimodular matrix. Then $g = f \circ U = (m : \ell)$, where*

$$m = f(q,r) = aq^2 + bqr + cr^2 \quad \text{and} \quad \ell = aqs + brs + crt + k. \tag{4.2.2}$$

Proof. Since $qt - rs = 1$, we see that

$$\begin{aligned} \frac{(2aq + b(qt + rs) + 2crt) - \varepsilon}{2} &= \frac{2(aqs + brs + crt) + b - \varepsilon}{2} \\ &= aqs + brs + crt + k. \end{aligned}$$

The expression for g as $(m : \ell)$ then follows directly from equation (4.2.1). □

If $f = (a : k)$ is equivalent to $g = (m : \ell)$, then equation (4.2.2) shows that f properly represents m. (Note that q and r cannot have a prime common divisor since $qt - rs = 1$.)

Exercise 4.2.7. Verify that $f = (13 : 7)$ is a quadratic form of discriminant $\Delta = -35$. For each of the following unimodular matrices U, calculate the form $f \circ U$ in ideal notation.

(a) $U = \begin{bmatrix} 2 & 3 \\ 3 & 5 \end{bmatrix}$.

(b) $U = \begin{bmatrix} 7 & 3 \\ -5 & -2 \end{bmatrix}$.

(c) $U = \begin{bmatrix} 4 & 9 \\ 3 & 7 \end{bmatrix}$.

In practice, we will often be able to restrict our attention to two particular types of unimodular matrices, specified in the following two propositions.

Proposition 4.2.2. *Let $(a : k)$ be a quadratic form of discriminant Δ, so that $\phi(k) = ac$ for some integer c, where $\phi(x) = x^2 + \varepsilon x + \frac{\varepsilon^2 - \Delta}{4}$ is the principal polynomial of discriminant Δ. Then*

$$(a : k) \sim (c : -k - \varepsilon). \tag{4.2.3}$$

Proof. Let $b = \phi'(k)$ so that $f(x, y) = ax^2 + bxy + cy^2$ in standard form. We have that

$$\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 2a & b \\ b & 2c \end{bmatrix} \cdot \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 2c & -b \\ -b & 2a \end{bmatrix},$$

so that $f \sim g$, where $g(x, y) = cx^2 - bxy + ay^2$. We can write $g = (c : \ell)$, where $\ell = \frac{-b-\varepsilon}{2} = -\frac{b-\varepsilon}{2} - \varepsilon = -k - \varepsilon$. □

Definition. We refer to $g(x, y) = cx^2 - bxy + ay^2$ as the *involution* of $f(x, y) = ax^2 + bxy + cy^2$. Notice that the involution of $g(x, y)$ returns us to $f(x, y)$. When using ideal notation, we will write $(a : k) \leftrightarrow (c : -k - \varepsilon)$ for this relation.

Exercise 4.2.8. Show that $H = \left\{ \begin{bmatrix} 1 & u \\ 0 & 1 \end{bmatrix} \mid u \in \mathbb{Z} \right\}$ is a subgroup of the group of unimodular matrices.

Definition. Let H be defined as in Exercise 4.2.8, so that $\sim_H$ is an equivalence relation on $\mathcal{Q}_\Delta$. We write $\sim_H$ as $\simeq$ in this case, and say that f is *norm equivalent* to g, or that f and g are in the same *norm class*, if $f \simeq g$.

Proposition 4.2.3. *If $(a : k)$ is a quadratic form of discriminant Δ, then $(a : k)$ is norm equivalent to $(m : \ell)$ if and only if $m = a$ and $\ell \equiv k \pmod{a}$.*

Proof. Let $\phi(k) = ac$ and $\phi'(k) = b$ so that $f(x, y) = ax^2 + bxy + cy^2$. If u is an integer, then

$$\begin{bmatrix} 1 & 0 \\ u & 1 \end{bmatrix} \cdot \begin{bmatrix} 2a & b \\ b & 2c \end{bmatrix} \cdot \begin{bmatrix} 1 & u \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 2a & b + 2au \\ b + 2au & 2(c + bu + au^2) \end{bmatrix},$$

so that $f \simeq g$, where $g(x,y) = ax^2 + (b+2au)xy + (c+bu+au^2)y^2$. In ideal notation, $g = (m : \ell)$ if and only if $m = a$ and

$$\ell = \frac{b+2au-\varepsilon}{2} = \frac{b-\varepsilon}{2} + au = k + au,$$

so that $\ell \equiv k \pmod{a}$. □

Definition. We refer to $g = (a : k+au)$ as the *translation* of $f = (a : k)$ by u. We have that $(a : k) \simeq (a : k+au)$ for all integers u. Thus it is also true that $(a : k) \sim (a : k+au)$ for all u. We will also write $(a : k) \to_u (a : k+au)$ for this translation.

The following example illustrates how we might use involutions and translations to simplify the class representative of a quadratic form.

Example. Let $\Delta = -23$ so that $\phi(x) = x^2 + x + 6$. We find that $\phi(18) = 348 = 87 \cdot 4$, with $\phi'(18) = 37$, so that $f = (87 : 18) = 87x^2 + 37xy + 4y^2$ is a quadratic form of discriminant Δ. Using a sequence of involutions and translations from Propositions 4.2.2 and 4.2.3, then

$$(87 : 18) \leftrightarrow (4 : -19) \to_5 (4 : 1) \leftrightarrow (2 : -2) \to_1 (2 : 0),$$

so that f is equivalent to the quadratic form $g = (2 : 0) = 2x^2 + xy + 3y^2$. Specifically, we find that $g = f \circ U$ with

$$U = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 5 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} -1 & -1 \\ 5 & 4 \end{bmatrix},$$

as one can verify. Here U is the product of the unimodular matrices for the involutions and translations that convert f to g. ◊

Exercise 4.2.9. Let $\Delta = -51$. Verify that $f = (57 : 16)$ is an element of $\mathcal{Q}_\Delta$. Use a sequence of involutions and translations to show that f is equivalent to $g = (3 : 1)$, and find a matrix U for which $g = f \circ U$.

The reader might recognize a similarity between the procedure in this example and the *reduction* algorithms that we developed for ideal forms of Gaussian integers (Theorem 1.5.3), and then for ideal numbers in an arbitrary quadratic domain (Theorem 2.4.3). We will say more about this process in Chapters 6 and 10, where we will also use the following proposition.

Proposition 4.2.4. *Let $\phi(x)$ be the principal polynomial of discriminant Δ, and let $f = (a : k)$ in $\mathcal{Q}_\Delta$, with $ac = \phi(k)$ and $b = \phi'(k)$. If U is a unimodular matrix with q and r the entries of its first column, then $f \circ U \simeq (m : \ell)$, where $m = aq^2 + bqr + cr^2$ and ℓ satisfies the congruences*

$$q\ell \equiv cr + kq \pmod{m} \quad \text{and} \quad r\ell \equiv (k-b)r - aq \pmod{m}.$$

Here q and r must be relatively prime, and so Exercise 0.1.11 shows that this pair of congruences has a unique solution modulo m. The main claim of the proposition is that the first column of U is sufficient to determine $f \circ U$ up to norm equivalence.

Proof. Let s and t be integers so that $qt-rs = 1$. All integer solutions of $qx-ry = 1$ are given by $(x, y) = (t + ru, s + qu)$ for some integer u. (This is an application of Theorem 0.1.5.) Thus U has the form

$$U = \begin{bmatrix} q & s+qu \\ r & t+ru \end{bmatrix} = \begin{bmatrix} q & s \\ r & t \end{bmatrix} \cdot \begin{bmatrix} 1 & u \\ 0 & 1 \end{bmatrix},$$

and $f \circ U$ is unique up to norm equivalence.

Now $\ell = aqs + brs + crt + k$ by equation (4.2.2). We find that

$$\begin{aligned} q\ell &= aq^2s + bqrs + cqrt + qk \\ &= (aq^2 + bqr + cr^2)s + cr(qt - rs) + qk = ms + cr + qk, \end{aligned}$$

since $m = aq^2 + bqr + cr^2$ and $qt - rs = 1$. So $q\ell \equiv cr + kq \pmod{m}$. With $rs = qt - 1$, so that $\ell = aqs + bqt + crt + (k - b)$, we find in a similar way, multiplying both sides by r, that $r\ell = mt+(k-b)r-aq$, so that $r\ell \equiv (k-b)r-aq \pmod{m}$. □

4.3 Representations of Integers by Quadratic Forms

We can now use equivalence of quadratic forms to give a formula for the number of representations of an integer by a particular quadratic form. Throughout this section, we identify an ordered pair of integers (q, r) with the column matrix $\mathbf{x}$ having entries q and r. We say that $\mathbf{x}$ is *primitive* if $\gcd(q, r) = 1$. If $f(x, y)$ is a quadratic form, we also write $f(q, r)$ as $f(\mathbf{x})$. Recall that we have $f(\mathbf{x}) = \frac{1}{2}\mathbf{x}^T M_f \mathbf{x}$, where M_f is the matrix of f.

Our first theorem shows that equivalent forms represent, and properly represent, the same collection of integers.

Theorem 4.3.1. *Let f and g be equivalent quadratic forms, and suppose that m is an integer represented by f. Then there is a one-to-one correspondence between ordered pairs $\mathbf{x} = (q, r)$ for which $f(\mathbf{x}) = m$ and $\mathbf{y} = (s, t)$ for which $g(\mathbf{y}) = m$. In this case,* $\gcd(q, r) = \gcd(s, t)$.

Proof. Let U be a unimodular matrix for which $g = f \circ U$, and let $\mathbf{y} = U^{-1}\mathbf{x}$. Using properties of inverses and transposes, we find that

$$m = \tfrac{1}{2} \cdot \mathbf{x}^T M_f \mathbf{x} = \tfrac{1}{2} \cdot \mathbf{x}^T (U^{-1})^T \cdot U^T M_f U \cdot U^{-1}\mathbf{x} = \tfrac{1}{2} \cdot \mathbf{y}^T M_g \mathbf{y},$$

so that $g(\mathbf{y}) = m$. Conversely, if $g(\mathbf{y}) = m$ and $\mathbf{x} = U\mathbf{y}$, then $f(\mathbf{x}) = m$. The matrix equations show that the entries of $\mathbf{y}$ can be written as combinations of the entries of $\mathbf{x}$, and conversely, so that those entries have the same greatest common divisor. □

Example. Let $f(x, y) = x^2 + xy + 2y^2$. Since

$$\begin{bmatrix} 7 & 2 \\ 10 & 3 \end{bmatrix} \cdot \begin{bmatrix} 2 & 1 \\ 1 & 4 \end{bmatrix} \cdot \begin{bmatrix} 7 & 10 \\ 2 & 3 \end{bmatrix} = \begin{bmatrix} 142 & 205 \\ 205 & 296 \end{bmatrix},$$

then f is equivalent to $g(x, y) = 71x^2 + 205xy + 148y^2$. Now $f(4, -9) = 142$, and so g represents 142 also. In fact, since

$$\begin{bmatrix} 7 & 10 \\ 2 & 3 \end{bmatrix}^{-1} \cdot \begin{bmatrix} 4 \\ -9 \end{bmatrix} = \begin{bmatrix} 3 & -10 \\ -2 & 7 \end{bmatrix} \cdot \begin{bmatrix} 4 \\ -9 \end{bmatrix} = \begin{bmatrix} 102 \\ -71 \end{bmatrix},$$

we find that $g(102, -71) = 142$. ◊

Exercise 4.3.1. Let $f(x, y) = 3x^2 - 5xy + 4y^2$, a quadratic form of discriminant $\Delta = -23$, and note that $f(2, 1) = 6$. For each of the following unimodular matrices U, find the quadratic form $g = f \circ U$, and find a solution of $g(x, y) = 6$.

(a) $U = \begin{bmatrix} 1 & -3 \\ 0 & 1 \end{bmatrix}$.

(b) $U = \begin{bmatrix} 2 & -3 \\ -3 & 5 \end{bmatrix}$.

(c) $U = \begin{bmatrix} 7 & 9 \\ 3 & 4 \end{bmatrix}$.

Corollary 4.3.2. *Equivalent quadratic forms have the same index.*

Proof. Let $f(x, y) = ax^2 + bxy + cy^2$ with $\gamma = \gcd(a, b, c)$ the index of f. Then γ divides $f(q, r)$ for every pair of rational integers q and r. Suppose that $f \sim g$ and that γ' is the index of g. Theorem 4.3.1 implies that $f(1, 0) = a$, $f(0, 1) = c$, and $f(1, 1) = a + b + c$ must be represented by g also. Then γ' is a common divisor of a, c, and $b = (a + b + c) - a - c$, and so γ' divides γ. The same argument in reverse shows that γ divides γ', and then f and g must have the same index. □

The following theorem provides an important necessary condition for an integer m to be properly represented by a particular quadratic form.

Theorem 4.3.3. *Let $\phi(x)$ be the principal polynomial of discriminant Δ. Then an integer m is properly represented by some quadratic form of discriminant Δ if and only if $\phi(x) \equiv 0 \pmod{m}$ has a solution.*

Proof. Suppose that $f(x,y)$ is a quadratic form of discriminant Δ and that $f(q,r) = m$ with $\gcd(q,r) = 1$. Then there are integers s and t so that $qt - rs = 1$, and we can form the unimodular matrix $U = \begin{bmatrix} q & s \\ r & t \end{bmatrix}$. If $g = f \circ U$, then Proposition 4.2.1 implies that $g = (m : \ell)$ for some integer ℓ. But Proposition 4.1.1 shows that such a quadratic form can exist only when m divides $\phi(\ell)$. So $\phi(x) \equiv 0 \pmod{m}$ must have a solution. Conversely, if ℓ is a solution of $\phi(x) \equiv 0 \pmod{m}$, then a quadratic form $g = (m : \ell)$ exists with discriminant Δ. But then $g(1,0) = m$, so that m is properly represented by some quadratic form of discriminant Δ. □

Theorem 4.3.3 does not imply that *every* quadratic form of discriminant Δ represents all eligible values of m. For example, if $\Delta = -20$ so that $\phi(x) = x^2 + 5$, then the congruence $\phi(x) \equiv 0 \pmod{3}$ has solutions $x = 1$ and $x = -1$. But $m = 3$ is not represented by $\phi(x,y) = x^2 + 5y^2$, the principal form of discriminant $\Delta = -20$. (Following the method of the proof of Theorem 4.3.3, we find that $(3 : 1) = 3x^2 + 2xy + 2y^2$ in $\mathcal{Q}_\Delta$ represents 3, however.)

Automorphs of Quadratic Forms. In the remainder of this section, we will see that the *number* of proper representations of an integer m by quadratic forms in $\mathcal{Q}_\Delta$ is essentially the number of solutions of $\phi(x) \equiv 0 \pmod{m}$. The following definition and results provide our method of counting representations in the right way.

Definition. Let f be a quadratic form in $\mathcal{Q}_\Delta$ for some discriminant Δ. Then a unimodular matrix U is called an *automorph* of f if $f \circ U = f$. We denote the set of all automorphs of f as $\mathrm{Aut}(f)$.

Exercise 4.3.2. If f is a quadratic form, show that $\mathrm{Aut}(f)$ is a subgroup of the group Γ of all unimodular matrices.

We can describe all automorphs of an arbitrary quadratic form as follows.

Proposition 4.3.4. *If $f(x,y) = ax^2 + bxy + cy^2$, then*

$$\mathrm{Aut}(f) = \left\{ \begin{bmatrix} q & \frac{-cr}{a} \\ r & q + \frac{br}{a} \end{bmatrix} \;\middle|\; f(q,r) = a, \text{ and } a \text{ divides both } br \text{ and } cr \right\}.$$

Proof. If $f = (a : k)$ in ideal notation and $U = \begin{bmatrix} q & s \\ r & t \end{bmatrix}$ is a unimodular matrix, then Proposition 4.2.1 implies that $f \circ U = f$ if and only if $a = aq^2 + bqr + cr^2 = f(q,r)$ and $k = aqs + brs + crt + k$, so that $aqs + brs + crt = 0$. Assuming that these equations hold, then

$$as = (aq^2 + bqr + cr^2)s - (aqs + brs + crt)q = cr(rs - qt) = -cr$$

and

$$at = (aq^2 + bqr + cr^2)t - (aqs + brs + crt)r = (aq + br)(qt - rs) = aq + br.$$

Solving these equations for s and t yields the expression for U in Proposition 4.3.4. The assumption that a divides both br and cr is necessary and sufficient to ensure that U has integer entries, and if $f(q, r) = a$, then the determinant of any such matrix equals 1. □

Note that $q = \pm 1$ and $r = 0$ always satisfy the requirements of Proposition 4.3.4. It follows that $\mathrm{Aut}(f)$ always contains I and $-I$, where I is the 2×2 identity matrix.

Exercise 4.3.3. Let b and c be integers for which $b^2 - 4c < -4$. Use Proposition 4.3.4 and equation (4.1.2) to show that I and $-I$ are the only automorphs of $f(x, y) = x^2 + bxy + cy^2$.

Proposition 4.3.5. *Let f be an element of $\mathcal{Q}_\Delta$ for some Δ. If f is equivalent to g, say with $g = f \circ V$, then $g = f \circ W$ if and only if $W = UV$ for some automorph U of f. In this case, U' is an automorph of g if and only if $U' = V^{-1}UV$ for some automorph U of f.*

Proof. If $W = UV$ for some automorph U of f, then $f \circ W = (f \circ U) \circ V = f \circ V = g$. Conversely, if $f \circ W = g$, then $f \circ WV^{-1} = g \circ V^{-1} = f$, so that WV^{-1} is an automorph of f. But then $W = UV$ for some automorph U of f.

Now $g \circ V^{-1}UV = f \circ UV = f \circ V = g$, so that $V^{-1}UV$ is an automorph of g. Conversely, if U' is an automorph of g, then $f \circ VU' = g \circ U' = g$. But then, by the preceding part of this proof, $VU' = UV$ for some automorph U of f, so that $U' = V^{-1}UV$. □

In group terminology, Proposition 4.3.5 shows that if $f \sim g$ in $\mathcal{Q}_\Delta$, then the set of all W for which $g = f \circ W$ is a right coset of $\mathrm{Aut}(f)$ in Γ, and that $\mathrm{Aut}(g)$ is a conjugate of $\mathrm{Aut}(f)$. In practice then, it will suffice to describe the automorphs of class representatives of quadratic forms of discriminant Δ. We will do so for $\Delta < 0$ in Chapter 6 and for $\Delta > 0$ in Chapter 10.

Equivalence of Representations. Using automorphs of a quadratic form f, we can define an equivalence relation on representations of a particular integer m by f as follows.

Definition. If $\mathbf{x}$ and $\mathbf{y}$ are ordered pairs of integers and f is a quadratic form, we say that $\mathbf{x}$ is *f-equivalent* to $\mathbf{y}$, and write $\mathbf{x} \sim_f \mathbf{y}$, if there is an automorph U of f for which $\mathbf{y} = U\mathbf{x}$. If $\mathbf{x} \sim_f \mathbf{y}$, then

$$f(\mathbf{y}) = \tfrac{1}{2} \cdot \mathbf{y}^T M_f \mathbf{y} = \tfrac{1}{2} \cdot (U\mathbf{x})^T M_f (U\mathbf{x}) = \tfrac{1}{2} \cdot \mathbf{x}^T (U^T M_f U)\mathbf{x} = f(\mathbf{x}).$$

The *number of representations* of an integer m by f is then defined to be the number of distinct f-equivalence classes of $\mathbf{x}$ for which $f(\mathbf{x}) = m$.

Exercise 4.3.4. If f is a quadratic form of discriminant Δ, show that the relation of f-equivalence is an equivalence relation on the set $\mathbb{Z} \times \mathbb{Z}$ (viewed as a set of 2×1 matrices with integer entries).

We have the following connection between proper representations of m by f and equivalence of quadratic forms.

Theorem 4.3.6. *Let $f = (a : k)$ be a quadratic form with discriminant Δ. Then for every nonzero integer m, the number of distinct proper representations of m by f is equal to the number of distinct congruence classes of ℓ modulo m for which $(a : k) \sim (m : \ell)$.*

Thus the number of distinct proper representations of m by any f in $\mathcal{Q}_\Delta$ is no larger than the number of solutions of $\phi(x) \equiv 0 \pmod{m}$, where $\phi(x)$ is the principal polynomial of discriminant Δ.

Proof. Suppose that $f(\mathbf{v}) = m$, where $\mathbf{v} = (q, r)$ is primitive. There are integers s and t with $qt - rs = 1$, so that $V = \begin{bmatrix} q & s \\ r & t \end{bmatrix}$ is a unimodular matrix, and then $f \circ V = (m : \ell)$ for some ℓ by Proposition 4.2.1. We will show that the function σ that sends $\mathbf{v}$ to ℓ is a bijection between f-equivalence classes of proper representations of m by f and congruence classes ℓ modulo m for which $f \sim (m : \ell)$.

We first show that ℓ is well-defined modulo m. If $qt - rs = 1$, then we know that *all* pairs of integers x and y for which $qx - ry = 1$ are given by $(x, y) = (t + ru, s + qu)$ for some integer u. Thus all unimodular matrices whose first column is $\mathbf{v}$ have the form

$$VU = \begin{bmatrix} q & s \\ r & t \end{bmatrix} \cdot \begin{bmatrix} 1 & u \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} q & s + qu \\ r & t + ru \end{bmatrix}.$$

But now $f \circ VU = (m : \ell) \circ U = (m : \ell + mu)$ by Proposition 4.2.3, and so ℓ is unique modulo m.

Next we show that σ is well-defined. Suppose that $\mathbf{v} \sim_f \mathbf{w}$, so that there is an automorph T of f for which $\mathbf{w} = T\mathbf{v}$. If we let $W = TV$, then the first column of W is $\mathbf{w}$, and we find that $f \circ W = (f \circ T) \circ V = f \circ V = (m : \ell)$. So σ is independent of the choice of $\mathbf{v}$ within its f-equivalence class.

To show that σ is injective, suppose that $\sigma(\mathbf{v}) = \sigma(\mathbf{w})$. Then there are unimodular matrices V and W, having first columns $\mathbf{v}$ and $\mathbf{w}$, respectively, for which $f \circ V = (m : \ell)$ and $f \circ W = (m : \ell')$, where $\ell' \equiv \ell \pmod{m}$. We can select a matrix $U = \begin{bmatrix} 1 & u \\ 0 & 1 \end{bmatrix}$ so that $(m : \ell) \circ U = (m : \ell')$, and then $f \circ VU = f \circ W$. By Proposition 4.3.5, there is an automorph T of f for which $W = TVU$. But

now we see that the first columns of W and TV are the same, which implies that $\mathbf{w} = T\mathbf{v}$, that is, $\mathbf{v} \sim_f \mathbf{w}$. Thus $\mathbf{v}$ and $\mathbf{w}$ are in the same f-equivalence class, and σ is injective.

Finally, suppose that ℓ is some integer for which $(a : k) \sim (m : \ell)$. Then by definition there is a unimodular matrix V so that $f \circ V = (m : \ell)$. If $\mathbf{v}$ is the first column of V, then $\mathbf{v}$ must be primitive since $\det V = 1$, and $f(\mathbf{v}) = m$. But then $\sigma(\mathbf{v})$ is the congruence class of ℓ modulo m, and σ is surjective. Since we have established that σ is a bijection, then the number of distinct proper representations of m by f is equal to the number of distinct congruence classes of ℓ modulo m for which $(a : k) \sim (m : \ell)$. □

Example. Let $\Delta = -23$, so that $\phi(x) = x^2 + x + 6$, and let $m = 87 = 3 \cdot 29$. Here $\left(\frac{-23}{3}\right) = 1 = \left(\frac{-23}{29}\right)$, so there are four solutions of $\phi(x) \equiv 0 \pmod{87}$, which we find to be $x = 18, -19, 39$, and -40. Theorem 4.3.3 implies that there is at least one quadratic form f in $\mathcal{Q}_{-23}$ that properly represents 87. We can go further by Theorem 4.3.6 to say that there are essentially four distinct proper representations of 87 by *classes* of forms of discriminant $\Delta = -23$.

In an example in §4.2, we found that $f = (87 : 18) \sim (2 : 0) = g$, specifically that $(2 : 0) = (87 : 18) \circ U$ with $U = \begin{bmatrix} -1 & -1 \\ 5 & 4 \end{bmatrix}$. Since $f(1,0) = 87$, then $g(x,y) = 2x^2 + xy + 3y^2$ must also represent 87. Using the proof of Theorem 4.3.1, we find in fact that

$$\begin{bmatrix} q \\ r \end{bmatrix} = U^{-1} \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 4 & 1 \\ -5 & -1 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 4 \\ -5 \end{bmatrix}$$

satisfies $g(q,r) = 87$, as one can verify. ◊

Exercise 4.3.5. Show that $(87 : 39) \sim (1 : 0)$ in $\mathcal{Q}_{-23}$. Use that fact to find a representation of 87 by $h(x,y) = x^2 + xy + 6y^2$.

4.4 Genera of Quadratic Forms

We conclude Chapter 4 by introducing another equivalence relation on quadratic forms of a fixed discriminant Δ. This relation is based on the following restrictions on representations of integers by *primitive* quadratic forms.

Proposition 4.4.1. *Let $f(x,y) = ax^2 + bxy + cy^2$ be a primitive quadratic form, and let p be a prime number that divides $\Delta = b^2 - 4ac$. Suppose that m and n are integers represented by f, and that p divides neither m nor n. If p is odd, then $\left(\frac{m}{p}\right) = \left(\frac{n}{p}\right)$. If $p = 2$ and $\Delta_0 = \frac{\Delta}{4}$, then the following statements are true.*

(1) *If $\Delta_0 \equiv 3 \pmod 4$ or $\Delta_0 \equiv 4 \pmod 8$, then $mn \equiv 1 \pmod 4$.*

(2) *If* $\Delta_0 \equiv 2 \pmod 8$, *then* $mn \equiv 1$ *or* $7 \pmod 8$.

(3) *If* $\Delta_0 \equiv 6 \pmod 8$, *then* $mn \equiv 1$ *or* $3 \pmod 8$.

(4) *If* $\Delta_0 \equiv 0 \pmod 8$, *then* $mn \equiv 1 \pmod 8$.

Note that if a discriminant Δ is even, then $\Delta \equiv 0 \pmod 4$, so that Δ_0 is an integer as given above.

Proof. If p divides $\Delta = b^2 - 4ac$ and p divides either a or c, then p also divides b. So if we assume that f is primitive, then a or c (or both) is *not* divisible by p. To simplify the proof, we will assume that p does not divide a. It then suffices to establish the statements above with a in place of n.

Recall from equation (4.1.2) that if $f(q, r) = m$ for some q and r, then $4am = (2aq + br)^2 - \Delta r^2$. If p divides Δ, then $4am$ is congruent to a square modulo p. In particular, if p is odd and p does not divide m, then $\left(\frac{4am}{p}\right) = 1$, from which it follows immediately that $\left(\frac{m}{p}\right) = \left(\frac{a}{p}\right)$.

Now suppose that $p = 2$ divides Δ, so that b is even. In this case, we have

$$am = \left(aq + \frac{b}{2} \cdot r\right)^2 - \frac{\Delta}{4} \cdot r^2 = t^2 - \Delta_0 r^2,$$

with $\Delta_0 = \frac{\Delta}{4}$, for some integers t and r. The square of an integer t is congruent to 0 modulo 4 (if t is even) or to 1 modulo 8 (if t is odd). Assume first that Δ_0 is odd, as are a and m. If $\Delta_0 \equiv 1 \pmod 4$, we find that am is congruent to $1 - 0$ or $0 - 1$ modulo 4, so that there is no restriction on this product. But if $\Delta_0 \equiv 3 \pmod 4$, then am is congruent to $1 - 0$ or $0 - 3$ modulo 4, that is, $am \equiv 1 \pmod 4$.

Now assume that Δ_0 is even. Here t must be odd if a and m are both odd. We conclude that am is congruent to $1 - 0$ modulo 8 if r is even, and am is congruent to $1 - \Delta_0$ modulo 8 if r is odd. Our conclusions in each of cases (1)–(4) follow directly. □

Definition. Let $f(x, y) = ax^2 + bxy + cy^2$ be a primitive quadratic form of discriminant Δ. Then we define a collection of *genus symbols* for f as follows. If p is an odd prime dividing Δ, and m is an integer represented by f with p not dividing m, let $\left(\frac{f}{p}\right) = \left(\frac{m}{p}\right)$. If $p = 2$ divides Δ, with $\Delta_0 = \frac{\Delta}{4}$, and m is an odd integer represented by f, then:

(1) If $\Delta_0 \equiv 0$ or $3 \pmod 4$, let $\left(\frac{-1}{f}\right) = \begin{cases} 1, & \text{if } m \equiv 1 \pmod 4, \\ -1, & \text{if } m \equiv 3 \pmod 4. \end{cases}$

(2) If $\Delta_0 \equiv 0$ or $2 \pmod 8$, let $\left(\frac{2}{f}\right) = \begin{cases} 1, & \text{if } m \equiv 1 \text{ or } 7 \pmod 8, \\ -1, & \text{if } m \equiv 3 \text{ or } 5 \pmod 8. \end{cases}$

(3) If $\Delta_0 \equiv 0$ or $6 \pmod 8$, let $\left(\frac{-2}{f}\right) = \begin{cases} 1, & \text{if } m \equiv 1 \text{ or } 3 \pmod 8, \\ -1, & \text{if } m \equiv 5 \text{ or } 7 \pmod 8. \end{cases}$

If $\Delta < 0$, we also let $\left(\frac{f}{\infty}\right)$ equal 1 if $m > 0$ and -1 if $m < 0$.

Proposition 4.4.1 shows that genus symbols are well-defined. When Δ is negative, the symbol $\left(\frac{f}{\infty}\right)$ merely distinguishes between positive definite and negative definite forms. In practice, we can always use $f(1,0) = a$ or $f(0,1) = c$ in place of m in calculating the relevant genus symbols.

Example. Let $f(x,y) = 15x^2 - 10xy + 6y^2$, with discriminant

$$\Delta = (-10)^2 - 4 \cdot 15 \cdot 6 = -260 = -1 \cdot 2^2 \cdot 5 \cdot 13.$$

Here $\frac{\Delta}{4} = -65 \equiv 3 \pmod 4$, so the symbols $\left(\frac{f}{5}\right)$, $\left(\frac{f}{13}\right)$, $\left(\frac{-1}{f}\right)$, and $\left(\frac{f}{\infty}\right)$ are defined. Since 5 does not divide $c = 6$, then $\left(\frac{f}{5}\right) = \left(\frac{6}{5}\right) = \left(\frac{1}{5}\right) = 1$. We can use $a = 15$ for each of the other symbols. We find that $\left(\frac{f}{13}\right) = \left(\frac{15}{13}\right) = \left(\frac{2}{13}\right) = -1$, $\left(\frac{-1}{f}\right) = -1$ since $15 \equiv 3 \pmod 4$, and $\left(\frac{f}{\infty}\right) = 1$ since 15 is positive. ◊

Definition. If f and g are primitive quadratic forms in $\mathcal{Q}_\Delta$ for some Δ, and f and g have the same collection of genus symbols, then we say that f is in the same *genus* as g (pluralized as *genera*), or that f is *genus equivalent* to g, and we write $f \approx g$. More generally, if f and g have the same index, $\gamma(f) = \gamma = \gamma(g)$, with $f(x,y) = \gamma \cdot f_1(x,y)$ and $g(x,y) = \gamma \cdot g_1(x,y)$, we define f to be genus equivalent to g if and only if $f_1 \approx g_1$.

Genus equivalence is an equivalence relation on $\mathcal{Q}_\Delta$. Furthermore, Theorem 4.3.1 shows that if f is equivalent to g, then f is genus equivalent to g, since then f and g represent the same integers, and so must have the same collection of genus symbols. Thus we can view a genus of forms as being made up of classes of forms.

The Number of Genera of a Discriminant. If there are t genus symbols defined for quadratic forms of some discriminant Δ, then there are 2^t different ways in which we can assign those symbols the values $+1$ or -1. But not all combinations of these symbols take place in practice. We describe those that can occur in the next two propositions. We will assume that if $f(x,y)$ is a quadratic form of discriminant Δ, then there is some odd positive integer q that is relatively prime to Δ so that f represents q (or f represents $-q$ when f is negative definite).

Proposition 4.4.2. *Let f be a quadratic form of primitive discriminant Δ. Then the product of all genus symbols defined for f must equal* 1.

Proof. If Δ is a primitive discriminant, we can write

$$\Delta = (-1)^e \cdot 2^j \cdot p_1 \cdots p_k \cdot p_{k+1} \cdots p_\ell,$$

where each p_i is a distinct odd prime, with $p_i \equiv 3 \pmod 4$ for $1 \le i \le k$ and $p_i \equiv 1 \pmod 4$ for $k+1 \le i \le \ell$, and where $e = 0$ or 1 and $j = 0$, 2, or 3. (Either k or $\ell - k$ might equal 0.) Let f be a quadratic form of discriminant Δ, assumed at first to be positive definite, so that $\left(\frac{f}{\infty}\right) = 1$, if $\Delta < 0$. Suppose that q is an odd positive integer represented by f, relatively prime to Δ. By Theorem 4.3.3, we know that $\phi(x) \equiv 0 \pmod q$ must have a solution, where $\phi(x)$ is the principal polynomial of discriminant Δ, so it follows that the Jacobi symbol $\left(\frac{\Delta}{q}\right)$ must equal 1. (See Exercise 0.3.5.) If $p_i \equiv 1 \pmod 4$, then $\left(\frac{p_i}{q}\right) = \left(\frac{q}{p_i}\right)$, while if $p_i \equiv 3 \pmod 4$, then $\left(\frac{p_i}{q}\right) = \left(\frac{-1}{q}\right)\left(\frac{-p_i}{q}\right) = \left(\frac{-1}{q}\right)\left(\frac{q}{p_i}\right)$. (See Exercise 0.2.7.) So we find that

$$\begin{aligned} 1 = \left(\frac{\Delta}{q}\right) &= \left(\frac{-1}{q}\right)^e \left(\frac{2}{q}\right)^j \left(\frac{p_1}{q}\right) \cdots \left(\frac{p_k}{q}\right) \cdot \left(\frac{p_{k+1}}{q}\right) \cdots \left(\frac{p_\ell}{q}\right) \\ &= \left(\frac{-1}{q}\right)^{e+k} \left(\frac{2}{q}\right)^j \left(\frac{q}{p_1}\right) \cdots \left(\frac{q}{p_k}\right) \cdot \left(\frac{q}{p_{k+1}}\right) \cdots \left(\frac{q}{p_\ell}\right). \end{aligned} \tag{4.4.1}$$

Each $\left(\frac{q}{p_i}\right)$ is the same as the genus symbol $\left(\frac{f}{p_i}\right)$ for $1 \le i \le \ell$. We now consider four cases, one of which must occur if Δ is primitive.

(1) If $\Delta \equiv 1 \pmod 4$, then $j = 0$, and we find that if $e = 0$, then k is even, while if $e = 1$, then k is odd. So $e + k$ is even in either case, and equation (4.4.1) becomes $1 = \left(\frac{f}{p_1}\right) \cdots \left(\frac{f}{p_\ell}\right)$. That is, the product of all defined genus symbols equals 1.

(2) If $\frac{\Delta}{4} \equiv 3 \pmod 4$, then $j = 2$, and k is odd when $e = 0$ but k is even if $e = 1$. Now $e + k$ is odd in each case, so that equation (4.4.1) becomes $1 = \left(\frac{-1}{q}\right)\left(\frac{f}{p_1}\right) \cdots \left(\frac{f}{p_\ell}\right)$. Here $\left(\frac{-1}{q}\right) = \left(\frac{-1}{f}\right)$, and again the product of all genus symbols equals 1.

(3) If $\frac{\Delta}{4} \equiv 2 \pmod 8$ (or equivalently $\frac{\Delta}{8} \equiv 1 \pmod 4$), then $j = 3$, and we again find that $e + k$ is even in every case. So now $1 = \left(\frac{2}{q}\right)\left(\frac{f}{p_1}\right) \cdots \left(\frac{f}{p_\ell}\right)$. Here $\left(\frac{2}{q}\right) = \left(\frac{2}{f}\right)$ is a defined genus symbol.

(4) If $\frac{\Delta}{4} \equiv 6 \pmod 8$, then $j = 3$ and $e+k$ is odd. In this case, equation (4.4.1) implies that $1 = \left(\frac{-1}{q}\right)\left(\frac{2}{q}\right)\left(\frac{f}{p_1}\right)\cdots\left(\frac{f}{p_\ell}\right) = \left(\frac{-2}{q}\right)\left(\frac{f}{p_1}\right)\cdots\left(\frac{f}{p_\ell}\right)$. Here $\left(\frac{-2}{q}\right) = \left(\frac{-2}{f}\right)$ is a defined genus symbol.

So if Δ is positive, or if Δ is negative and f is positive definite, then the product of all genus symbols equals 1. If g is negative definite, then $g = -f$ for some positive definite quadratic form f, and if f represents q as above, then g represents $-q$. We find that $\left(\frac{g}{p_i}\right) = \left(\frac{-q}{p_i}\right) = -\left(\frac{f}{p_i}\right)$ for $1 \le i \le k$, but $\left(\frac{g}{p_i}\right) = \left(\frac{f}{p_i}\right)$ for $k+1 \le i \le \ell$. Also $\left(\frac{-1}{g}\right) = -\left(\frac{-1}{f}\right)$ since if $q \equiv 1 \pmod 4$, then $-q \equiv 3 \pmod 4$. But $\left(\frac{2}{g}\right) = \left(\frac{2}{f}\right)$ since $q \equiv 1$ or $7 \pmod 8$ if and only if $-q \equiv 1$ or $7 \pmod 8$. In each of the four cases above, we find that an odd number of symbols are changed in sign, but since $\left(\frac{g}{\infty}\right) = -1$, we still have the product of all defined genus symbols equal to 1. □

Proposition 4.4.3. *Let $\Delta = \Delta(d,\gamma)$ for some $\gamma > 1$ and let $\Delta_1 = \Delta(d,1)$. If f is a primitive quadratic form of discriminant Δ, then the product of all genus symbols for f that are also defined for a quadratic form of discriminant Δ_1 must equal 1. If $\frac{\Delta}{4} \equiv 0 \pmod 8$, so that $\left(\frac{-1}{f}\right)$, $\left(\frac{2}{f}\right)$, and $\left(\frac{-2}{f}\right)$ are all defined, then their product must equal 1. Any other genus symbols defined for f can equal either 1 or -1.*

Proof. Suppose that q is an odd positive integer, relatively prime to Δ, that is represented by f. If $\Delta = \gamma^2\Delta_1$ with Δ_1 primitive, we have that $\left(\frac{\Delta}{q}\right) = \left(\frac{\Delta_1}{q}\right)$. The proof of Proposition 4.4.2 shows that the product of all genus symbols defined for Δ_1 must equal 1. If $\left(\frac{-1}{f}\right)$, $\left(\frac{2}{f}\right)$, and $\left(\frac{-2}{f}\right)$ are all defined, we find by testing all possibilities for q modulo 8 that the product of these symbols must be 1. There are no restrictions on any remaining symbols. □

We illustrate the claims of these propositions with some examples to conclude this section. Here the listing of certain quadratic forms of a particular genus is by trial-and-error. We will see a systematic method of finding representatives of all possible classes and genera of quadratic forms of negative discriminant in §6.1 and of positive discriminant in §10.1 and §10.2.

Example. Let $\Delta = \Delta(6,1) = 24 = 2^3 \cdot 3$, a primitive discriminant. The genus symbols defined for a form f of discriminant Δ are $\left(\frac{f}{3}\right)$ and $\left(\frac{-2}{f}\right)$. Their product must equal 1, so there are only two possible genera. We find that $f(x,y) = x^2 - 6y^2$

is a quadratic form of discriminant $\Delta = 24$ with $\left(\frac{f}{3}\right) = 1 = \left(\frac{-2}{f}\right)$, while for $g(x,y) = 2x^2 - 3y^2$, we have $\left(\frac{g}{3}\right) = -1 = \left(\frac{-2}{g}\right)$. ◊

Example. Let $\Delta = \Delta(6,2) = 96 = 2^5 \cdot 3$, so that $\Delta_1 = 24$ in the notation of Proposition 4.4.3. From the preceding example, we see that $2x^2 - 12y^2$ and $4x^2 - 6y^2$ are forms of index two in $\mathcal{Q}_\Delta$, representing distinct genera. (We do not define genus symbols for these forms, however.) For primitive forms, the genus symbols $\left(\frac{f}{3}\right)$, $\left(\frac{-2}{f}\right)$, $\left(\frac{-1}{f}\right)$, and $\left(\frac{2}{f}\right)$ are defined, but we must have $\left(\frac{f}{3}\right)\left(\frac{-2}{f}\right) = 1$, as for $\Delta_1 = 24$. There is no restriction on $\left(\frac{-1}{f}\right)$, but then $\left(\frac{-2}{f}\right)\left(\frac{-1}{f}\right)\left(\frac{2}{f}\right) = 1$. So there are at most four genera. In fact, we find the following representatives of each possible genus:

$$\begin{aligned} ++++ &: \quad x^2 - 24y^2 \\ ---+ &: \quad -x^2 + 24y^2 \\ ++-- &: \quad 3x^2 - 8y^2 \\ --+- &: \quad -3x^2 + 8y^2. \end{aligned}$$

Here we write the symbols as $+$ or $-$, in order as $\left(\frac{f}{3}\right)$, $\left(\frac{-2}{f}\right)$, $\left(\frac{-1}{f}\right)$, and $\left(\frac{2}{f}\right)$. ◊

Example. Let $\Delta = \Delta(2,15) = 1800 = 2^3 \cdot 3^2 \cdot 5^2$, so that $\Delta_1 = 8$. The genus symbols $\left(\frac{2}{f}\right)$, $\left(\frac{f}{3}\right)$, and $\left(\frac{f}{5}\right)$ are defined for elements of $\mathcal{Q}_\Delta$, with $\left(\frac{2}{f}\right) = 1$ the only restriction. We find the following representatives of the possible genera of primitive forms:

$$\begin{aligned} +++ &: \quad x^2 - 450y^2 \\ +-+ &: \quad -x^2 + 450y^2 \\ +-- &: \quad 2x^2 - 225y^2 \\ ++- &: \quad -2x^2 + 225y^2 \end{aligned}$$

with symbols $\left(\frac{2}{f}\right)$, $\left(\frac{f}{3}\right)$, and $\left(\frac{f}{5}\right)$ in order. ◊

Exercise 4.4.1. In each part, find all genus symbols that are defined for a primitive quadratic form of discriminant Δ, determine the combinations of genus symbols that can actually occur, and find an example of a quadratic form having that collection of genus symbols.

(a) $\Delta = 21$.

(b) $\Delta = 28$.

(c) $\Delta = 56$.

(d) $\Delta = 84$.

(e) $\Delta = 112$.

(f) $\Delta = 224$.

Quadratic Forms—Review

In this chapter, we introduced collections $\mathcal{Q}_\Delta$ of quadratic forms $f(x, y) = ax^2 + bxy + cy^2$ of a fixed discriminant Δ as our objects of study, with the question of which integers are *represented* by f as our main motivation. We summarize our main definitions and results as follows.

(1) Elements of $\mathcal{Q}_\Delta$ are in one-to-one correspondence with pairs $(a : k)$ for which a divides $\phi(k)$, where $\phi(x)$ is the principal polynomial of discriminant Δ. In this way, we define an alternative notation for a quadratic form f, which we call *ideal notation* because of its similarity to our notation for ideals of the quadratic domain of discriminant Δ.

(2) There is a relation of *equivalence* on quadratic forms of a given discriminant defined in terms of matrix multiplication. Equivalent forms represent the same collection of integers.

(3) The number of representations of a particular integer m by some quadratic form of discriminant Δ is essentially the same (using *automorphs* of a form, and a relation of *f-equivalence* on ordered pairs) as the number of solutions of the congruence $\phi(x) \equiv 0 \pmod{m}$.

(4) There is a relation of *genus equivalence* on quadratic forms of a particular discriminant, defined in terms of congruence classes of integers represented by a given form. We can determine the number of distinct equivalence classes (*genera*) of $\mathcal{Q}_\Delta$ under this relation in terms of the prime factorization of Δ.

In the following chapter, we explore the connection between quadratic forms and ideals, which is suggested by our similar notation for both types of objects.

5

Correspondence between Forms and Ideals

Let $\phi(x)$ be the principal polynomial of some discriminant Δ. In Chapter 3, we showed that every primitive ideal of the quadratic domain D_Δ can be expressed as

$$A = [a : k] = \{ma + n(k + z) \mid m, n \in \mathbb{Z}\},$$

where a and k are integers for which a divides $\phi(k)$, and z is the basis element of discriminant Δ. In Chapter 4, we found that every quadratic form of discriminant Δ can be written as

$$f = (a : k) = ax^2 + bxy + cy^2,$$

where $\phi(k) = ac$, so that a again divides $\phi(k)$, and $\phi'(k) = b$. This similarity suggests a close relation between quadratic forms with a particular discriminant Δ and ideals of the quadratic domain D_Δ. Our goal in this chapter is to justify this similar "ideal number" notation for ideals and quadratic forms by exploring connections between these objects more fully.

In §5.1 and §5.2, we define an equivalence relation on ideals of a quadratic domain. We will find that equivalence classes of ideals and of quadratic forms (under the equivalence relation introduced in §4.2) are essentially identical. In §5.3, we introduce an operation of composition on classes of quadratic forms. We will establish that this operation is interchangeable with ideal multiplication, as defined and computed in §3.4 and §3.6. We conclude this chapter with the definition of a group structure on equivalence classes of ideals or of quadratic domains in §5.4. In later chapters, we will see how we can apply these *class groups* to describe representations of integers by quadratic forms.

5.1 Equivalence of Ideals

We can define a mapping from quadratic forms to ideals as follows.

Definition. If $f = (a : k)$ is a quadratic form of discriminant Δ, then $A_f = [a : k]$ is a primitive ideal of D_Δ, which we call the *ideal of* f.

As noted above, A_f is in fact an ideal of D_Δ since a divides $\phi(k)$. If $k = \frac{b-\varepsilon}{2}$ and $z = \frac{\varepsilon+\sqrt{\Delta}}{2}$ as in (2.2.2), then $k + z = \frac{b+\sqrt{\Delta}}{2}$. Therefore, if $f(x, y) = ax^2 + bxy + cy^2$ is a quadratic form of discriminant Δ, then we can also express this ideal as

$$A_f = \left\{ ma + n\left(\frac{b+\sqrt{\Delta}}{2}\right) \mid m, n \in \mathbb{Z} \right\}.$$

It is also true that if $A = [a : k]$ is an ideal of D_Δ, then $(a : k)$ is a quadratic form of discriminant Δ. But we have noted that $[a : k] = [-a : k]$ and $[a : k] = [a : \ell]$ if $\ell \equiv k \pmod{a}$, whereas $(a : k) \neq (-a : k)$ and $(a : k) = (a : \ell)$ only when $k = \ell$. Thus a mapping in this direction is not well-defined. In this section, we define an equivalence relation on ideals, and we will then establish a precise correspondence between *equivalence classes* of ideals and of quadratic forms.

Definition. Let A and B be nontrivial ideals of $D = D_\Delta$. We say that A is *equivalent* to B, written $A \sim B$, if there is a nonzero rational integer m and a nonzero element v of D so that $mA = vB$.

The definition of ideal equivalence is often given as $A \sim B$ if $wA = vB$ for nonzero elements w and v of D. But since then $N(w)A = \overline{w} \cdot wA = (\overline{w}v)B$, we may assume without loss of generality that w is a rational integer.

Exercise 5.1.1. Show that $vB = \{vx \mid x \in B\}$ is equal to the product of ideals $\langle v \rangle B$.

We compile some important properties of this relation in the following propositions and exercises.

Proposition 5.1.1. *Equivalence of ideals is an equivalence relation on the set of nontrivial ideals of a quadratic domain D.*

Proof. Let A, B, and C be nontrivial ideals of D.

(1) Since $1 \cdot A = 1 \cdot A$, then $A \sim A$ and $\sim$ is reflexive.

(2) Suppose that $A \sim B$, so that $mA = vB$ for some nonzero integer m and nonzero element v of D. Then $\overline{v}(vB) = \overline{v}(mA)$, implying that $N(v)B = (m\overline{v})A$. So $B \sim A$ and $\sim$ is symmetric.

(3) Suppose that $A \sim B$ and $B \sim C$, so that $mA = vB$ and $nB = wC$ for some nonzero integers m and n, and nonzero elements v and w of D. Then $(mn)A = n(mA) = n(vB) = v(nB) = (vw)C$, so that $A \sim C$, and $\sim$ is transitive. □

Proposition 5.1.2. *A nontrivial ideal A of a quadratic domain D is a principal ideal if and only if A is equivalent to D (as an ideal of itself).*

Proof. If $A = \langle u \rangle$, then $1 \cdot A = u \cdot D$, so that $A \sim D$. Conversely, suppose that $A \sim D$, so that $mA = vD$ for some $m \neq 0$ in $\mathbb{Z}$ and $v \neq 0$ in D. Then $v = v \cdot 1 = mu$ for some u in A. Since $mA = muD$ with $m \neq 0$, then $A = uD = \langle u \rangle$, a principal ideal. □

Exercise 5.1.2. Let A_1, A_2, B_1, and B_2 be nontrivial ideals of a quadratic domain D. Show that if A_1 is equivalent to B_1 and A_2 is equivalent to B_2, then A_1A_2 is equivalent to B_1B_2.

Exercise 5.1.3. If A is a nontrivial ideal of a quadratic domain D, and v is a nonzero element of D, show that vA is equivalent to A.

Exercise 5.1.4. If A and B are nontrivial ideals of a quadratic domain D, and A is equivalent to B, show that $\overline{A}$ is equivalent to $\overline{B}$.

Proposition 5.1.3. *If A and B are equivalent ideals of a quadratic domain D, then A and B have the same index.*

Proof. Suppose that $A \sim B$, so that $mA = vB$ for some $m \neq 0$ in $\mathbb{Z}$ and $v \neq 0$ in D. Then $\langle m \rangle A = \langle v \rangle B$, so that

$$\gamma(\langle m \rangle A) = \operatorname{lcm}(\gamma(\langle m \rangle), \gamma(A)) = \operatorname{lcm}(\gamma(\langle v \rangle), \gamma(B)) = \gamma(\langle v \rangle B),$$

by Theorem 3.6.6. But a principal ideal always has index 1 by Corollary 3.6.4. It follows that $\operatorname{lcm}(\gamma(\langle m \rangle), \gamma(A)) = \gamma(A)$ and $\operatorname{lcm}(\gamma(\langle v \rangle), \gamma(B)) = \gamma(B)$, and so $\gamma(A) = \gamma(B)$. □

Exercise 5.1.5. If f is a quadratic form of discriminant Δ and A_f is its corresponding ideal of D_Δ, show that the index of f is the same as the index of A_f.

Proposition 5.1.4. *Let A and B be nontrivial ideals of a quadratic domain D. If $A\overline{B}$ is a principal ideal, then A is equivalent to B. Conversely, if A is equivalent to B and $\gamma(A) = 1$, then $A\overline{B}$ is a principal ideal.*

Proof. Suppose that $A\overline{B}$ is a principal ideal. Since a principal ideal has index 1, it follows that $\gamma(A\overline{B}) = \operatorname{lcm}(\gamma(A), \gamma(\overline{B})) = 1$ and thus $\gamma(A) = 1 = \gamma(\overline{B})$. Now Proposition 5.1.2 implies that $A\overline{B} \sim D$, and so $(A\overline{B})B \sim DB$ by Exercise 5.1.2.

But $DB = B$, and $(A\overline{B})B = (B\overline{B})A = N(B)A$ using Theorem 3.4.2. Thus we have $A \sim N(B)A \sim B$ by Exercise 5.1.3.

Conversely, suppose that $A \sim B$, and that $\gamma(A) = 1$, so that $\gamma(B) = 1$ by Proposition 5.1.3. Now $A\overline{B} \sim B\overline{B}$ by Exercise 5.1.2, and $B\overline{B} = \langle N(B)\rangle$ is a principal ideal by Theorem 3.4.2. □

The converse statement of Proposition 5.1.4 is not generally true without the additional assumption that $\gamma(A) = 1$. For example, consider $A = [2 : 0]$ in $D = D_{-12}$, for which $\gamma(A) = 2$. Here A is equivalent to itself, but $A\overline{A} = A^2 = 2[2 : 0]$ is not a principal ideal of D. Otherwise, $A = [2 : 0]$ would be principal, but we demonstrated that this is not the case in an example in §3.6.

We now state and prove our main result for this section, connecting equivalence of quadratic forms to equivalence of ideals.

Theorem 5.1.5. *Let $f = (a : k)$ and $f_1 = (a_1 : k_1)$ be quadratic forms of discriminant Δ, and let $A = A_f = [a : k]$ and $A_1 = A_{f_1} = [a_1 : k_1]$ be the corresponding ideals of D_Δ. If f is equivalent to f_1, then A is equivalent to A_1.*

Proof. Let $D = D_\Delta = \{m + nz \mid m, n \in \mathbb{Z}\}$, where $z = z_\Delta$. Let $w = k + z$ and $\overline{w} = k + \overline{z}$, and let $\phi(x)$ be the principal polynomial of discriminant Δ. We can write $f(x, y) = ax^2 + bxy + cy^2$, where

$$ac = \phi(k) = w\overline{w} \qquad \text{and} \qquad b = \phi'(k) = w + \overline{w}. \tag{5.1.1}$$

Let $U = \begin{bmatrix} q & s \\ r & t \end{bmatrix}$ be a unimodular matrix for which $f_1 = f \circ U$, so that

$$a_1 = aq^2 + bqr + cr^2 \qquad \text{and} \qquad k_1 = aqs + brs + crt + k, \tag{5.1.2}$$

as in Proposition 4.2.1.

We will show that $a_1 A = \upsilon A_1$, where $\upsilon = qa + rw$, so that $A \sim A_1$ as ideals of $D = D_\Delta$. We first establish that

$$\upsilon \cdot a_1 = a_1(qa + rw) \qquad \text{and} \qquad \upsilon \cdot w_1 = a_1(sa + tw), \tag{5.1.3}$$

where $w_1 = k_1 + z = aqs + brs + crt + w$, using (5.1.2). This will imply that υA_1 is a subset of $a_1 A$, since the typical element of υA_1, namely $\upsilon(ma_1 + nw_1) = m(\upsilon a_1) + n(\upsilon w_1)$, is then a $\mathbb{Z}$-combination of $a_1 a$ and $a_1 w$. The first equation in (5.1.3) is immediate from the definition of υ. For the second, note that

$$\begin{aligned} \upsilon w_1 &= (qa + rw)(aqs + brs + crt + w) \\ &= a^2q^2s + abqrs + acqrt + aqw + aqrsw + br^2sw + cr^2tw + rw^2 \end{aligned} \tag{5.1.4}$$

and

$$\begin{aligned} a_1(sa + tw) &= (aq^2 + bqr + cr^2)(sa + tw) \\ &= a^2q^2s + abqrs + acr^2s + aq^2tw + bqrtw + cr^2tw. \end{aligned} \tag{5.1.5}$$

Subtracting (5.1.5) from (5.1.4) produces

$$\begin{aligned} &vw_1 - a_1(sa+tw) = acr(qt-rs) + aqw + aqw(rs-qt) + brw(rs-qt) + rw^2 \\ &= acr - brw + rw^2 = r(w\overline{w} - (w+\overline{w})w + w^2) = r(w\overline{w} - w^2 - w\overline{w} + w^2) = 0, \end{aligned}$$

using the fact that $qt - rs = 1$ (as U is unimodular), and the expressions for ac and b in (5.1.1).

Now we show that

$$a_1 \cdot a = v(ta_1 - rw_1) \qquad \text{and} \qquad a_1 \cdot w = v(-sa_1 + qw_1). \tag{5.1.6}$$

Here the equations of (5.1.3) imply that

$$\begin{aligned} v(ta_1 - rw_1) &= tva_1 - rvw_1 = t(a_1(qa+rw)) - r(a_1(sa+tw)) \\ &= a_1(qta + rtw - rsa - rtw) = a_1(qt-rs)a = a_1 a \end{aligned}$$

and

$$\begin{aligned} v(-sa_1 + qw_1) &= -sva_1 + qvw_1 = -s(a_1(qa+rw)) + q(a_1(sa+tw)) \\ &= a_1(-qsa - rsw + qsa + qtw) = a_1(qt-rs)w = a_1 w. \end{aligned}$$

The equations in (5.1.6) establish that $a_1 A \subseteq vA_1$ and complete the proof. □

The following special case of Theorem 5.1.5, corresponding to the involution of a quadratic form, will be particularly useful.

Corollary 5.1.6. *Let $A = [a : k]$ be an ideal of a quadratic domain D_Δ. Let $\phi(x)$ be the principal polynomial of discriminant Δ. If $\phi(k) = ac$ for some integer c, then A is equivalent to the ideal $C = [c : -k - \varepsilon]$, with $cA = (k+z)C$.*

Proof. For quadratic forms, we have $(a : k) \sim (c : -k-\varepsilon)$ by Proposition 4.2.2, so the equivalence of $A = [a : k]$ and $C = [c : -k-\varepsilon]$ is immediate from Theorem 5.1.5. Specifically, $(c : -k-\varepsilon) = (a : k) \circ \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$, so the proof of Theorem 5.1.5 shows that $cA = vC$, where $v = 0 \cdot a + 1 \cdot (k+z) = k+z$. □

Example. Let $\Delta = \Delta(-79, 1) = -79$, so that $z = \frac{1+\sqrt{-79}}{2}$ and $\phi(x) = x^2 + x + 20$. Since $\phi(45) = 110 \cdot 19$, we have that $A = [110 : 45]$ is an ideal of D_{-79}. Corollary 5.1.6 implies that $A \sim C$, where $C = [19 : -46]$, specifically with $19A = (45+z)C$. Notice that C can also be written as $[19 : -8]$. Relabeling this ideal as A_1 and applying Corollary 5.1.6 again, we then find that $A_1 = [19 : -8] \sim [4 : 7] = [4 : -1] = C_1$, with $4A_1 = (-8+z)C_1$. Combining these calculations, we have

$$4 \cdot 19A = 4 \cdot (45+z)C = (45+z) \cdot 4A_1 = (45+z)(-8+z)C_1.$$

This equation simplifies to $2A = (-10+z)C_1$ (using the calculation that $z^2 = -20 + z$), which shows directly that $[110 : 45] \sim [4 : -1]$. ◊

Exercise 5.1.6. Let $D = D_{-79}$, as in the preceding example. For each ideal $A = [a : k]$ of D below, use Corollary 5.1.6 to find an ideal $B = [b : \ell]$ with $b < 5$ that is equivalent to A. In each case, find a nonzero rational integer m and an element v of D so that $mA = vB$.

(a) $A = [80 : 19]$.

(b) $A = [80 : -36]$.

(c) $A = [178 : 59]$.

(d) $A = [320 : -100]$.

(e) $A = [325 : 80]$.

(f) $A = [325 : -120]$.

(g) $A = [356 : 59]$.

(h) $A = [712 : 59]$.

These examples illustrate a reduction process for ideals similar to the one for ideal numbers in Theorem 2.4.3. We will use this process extensively in Chapter 6.

5.2 Quadratic Forms Associated to an Ideal

We saw in Theorem 5.1.5 that if $f = (a : k)$ and $f_1 = (a_1 : k_1)$ are equivalent quadratic forms of discriminant Δ, then the corresponding ideals $A = [a : k]$ and $A_1 = [a_1 : k_1]$ are equivalent in the quadratic domain D_Δ. Our main result for this section is the following theorem establishing a partial converse of Theorem 5.1.5.

Theorem 5.2.1. *Let $A = [a : k]$ and $A_1 = [a_1 : k_1]$ be primitive ideals of a quadratic domain D, with a and a_1 positive. Suppose that $gA = vA_1$ for some $g \neq 0$ in $\mathbb{Z}$ and $v \neq 0$ in D, so that A is equivalent to A_1. Then the following statements are true.*

(1) *If $N(v)$ is positive, then $(a : k)$ is equivalent to $(a_1 : k_1)$.*

(2) *If $N(v)$ is negative, then $(a : k)$ is equivalent to $(-a_1 : k_1)$.*

If Δ is negative, then $N(v) > 0$ for every nonzero element of $D = D_\Delta$. So in that case, an equivalence between ideals, $[a : k] \sim [a_1 : k_1]$ with a and a_1 positive, establishes a corresponding equivalence of *positive definite* quadratic forms, $(a : k) \sim (a_1 : k_1)$. More caution is necessary when Δ is positive, as the following examples illustrate.

Example. Let $D = D_\Delta$ with $\Delta = \Delta(3,1) = 12$, so that $z = \sqrt{3}$ and $\phi(x) = x^2 - 3$, and consider the principal ideal $A = \langle 1 + z \rangle$. We find, using Theorem 3.2.2, that A can be written as $[2 : 1]$. Since A is principal, we know that $A \sim D = [1 : 0]$, specifically with $1 \cdot A = (1 + z)D$. Here $N(1 + z) = -2$, and so Theorem 5.2.1 implies that $(2 : 1) \sim (-1 : 0)$ in $\mathcal{Q}_{12}$, that is, $f(x,y) = 2x^2 + 2xy - y^2$ is equivalent to $f_1(x,y) = -x^2 + 3y^2$.

In this example, f is not equivalent to $\phi = (1 : 0) = x^2 - 3y^2$. Notice that $f(0,1) = -1$. On the other hand, since $x^2 - 3y^2 \equiv x^2 + y^2 \pmod 4$ and a sum of two squares cannot be congruent to 3 modulo 4, we find that ϕ cannot represent -1. But equivalent forms must represent the same integers. ◊

Example. Consider the quadratic domain $D = D_8$, so that $z = \sqrt{2}$. If $A = D = [1 : 0]$, then we have $A \sim A$ with $1 \cdot A = 1 \cdot A$. Since $N(1) = 1 > 0$, it follows that $(1 : 0)$ is equivalent to $(1 : 0)$, as is obvious in any case. But note in this example that $1 + z$ is a unit in D, and so $D = \langle 1 + z \rangle$. Thus it is also true that $1 \cdot A = (1 + z)A$, and since $N(1 + z) = 1 - 2 = -1$, then $(1 : 0)$ is equivalent to $(-1 : 0)$ as well. ◊

Ordered Bases for Ideals. To lead to the proof of Theorem 5.2.1 at the end of this section, we define a correspondence between each $\mathbb{Z}$-basis for an ideal A and some quadratic form. Recall that a set $S = \{u, v\}$ is a $\mathbb{Z}$-basis for an ideal A of a quadratic domain D if each element of A can be written uniquely as $mu + nv$ for some rational integers m and n. When we write $A = g[a : k]$, we are stating that $\{ga, gk + gz\}$ is a $\mathbb{Z}$-basis for A. We have the following connection between this $\mathbb{Z}$-basis and the quadratic form $f = (a : k)$.

Proposition 5.2.2. *Let a be positive, and suppose that $A = g[a : k]$ is an ideal of the quadratic domain D of discriminant Δ. Let $u = ga$ and $v = gk + gz$, and let w be an element of A, written as $w = mu + nv$. Then the norm of w is $N(w) = N(A) \cdot f(m,n)$, where $f = (a : k)$ in $\mathcal{Q}_\Delta$. Furthermore, $\overline{u}v - u\overline{v} = N(A) \cdot \sqrt{\Delta}$.*

Proof. If $\phi(x)$ is the principal polynomial of discriminant Δ, and $\phi(k) = ac$ and $\phi'(k) = b$, then $f(x,y) = ax^2 + bxy + cy^2$. When $w = mu + nv$, we have

$$N(w) = (mu + nv)(m\overline{u} + n\overline{v}) = (u\overline{u})m^2 + (u\overline{v} + \overline{u}v)mn + (v\overline{v})n^2. \qquad (5.2.1)$$

If $u = ga$, then $u\overline{u} = g^2a^2$, and since $z = \frac{\varepsilon + \sqrt{\Delta}}{2}$ and $\overline{z} = \frac{\varepsilon - \sqrt{\Delta}}{2}$, we find that

$$u\overline{v} + \overline{u}v = ga \cdot g(k + \overline{z}) + ga \cdot g(k + z) = g^2a(2k + \varepsilon) = g^2ab,$$

while

$$v\overline{v} = g(k + z) \cdot g(k + \overline{z}) = g^2\left(k^2 + \varepsilon k + \frac{\varepsilon^2 - \Delta}{4}\right) = g^2 \cdot \phi(k) = g^2ac.$$

Therefore,

$$\begin{aligned} N(w) &= g^2a^2m^2 + g^2abmn + g^2acn^2 \\ &= g^2a(am^2 + bmn + cn^2) = N(A) \cdot f(m,n), \end{aligned}$$

since $N(A) = g^2a$ if a is positive. Finally,

$$\overline{u}v - u\overline{v} = ga \cdot g(k+z) - ga \cdot g(k+\overline{z}) = g^2a(z-\overline{z}) = N(A) \cdot \sqrt{\Delta},$$

as claimed. □

More generally, we can associate a quadratic form with each example of a $\mathbb{Z}$-basis of an ideal A. We begin with the following observation.

Proposition 5.2.3. *Let A be an ideal of a quadratic domain D, and let $S = \{u, v\}$ be a $\mathbb{Z}$-basis for A. Then $T = \{u_1, v_1\}$ is also a $\mathbb{Z}$-basis for A if and only if $u_1 = qu + rv$ and $v_1 = su + tv$ for some q, r, s, and t in $\mathbb{Z}$ with $qt - rs = \pm 1$. In this case, $\overline{u_1}v_1 - u_1\overline{v_1} = (qt - rs)(\overline{u}v - u\overline{v})$.*

Proof. Since S is a $\mathbb{Z}$-basis for A, we can write $u_1 = qu + rv$ and $v_1 = su + tv$ for some q, r, s, and t in $\mathbb{Z}$, and thus any $\mathbb{Z}$-combination of T is also a $\mathbb{Z}$-combination of S. We find that

$$tu_1 - rv_1 = (qt - rs)u \quad \text{and} \quad -su_1 + qv_1 = (qt - rs)v,$$

so if $qt - rs = \pm 1$, then any $\mathbb{Z}$-combination of S is likewise a $\mathbb{Z}$-combination of T. It follows that T is a $\mathbb{Z}$-basis for A in that case.

Conversely, if T is a $\mathbb{Z}$-basis for A, then we can write $u = q_1u_1 + r_1v_1$ and $v = s_1u_1 + t_1v_1$ for some q_1, r_1, s_1, and t_1 in $\mathbb{Z}$. In that case,

$$u = q_1(qu + rv) + r_1(su + tv) = (qq_1 + sr_1)u + (rq_1 + tr_1)v,$$

so that $qq_1 + sr_1 = 1$ and $rq_1 + tr_1 = 0$, and

$$v = s_1(qu + rv) + t_1(su + tv) = (qs_1 + st_1)u + (rs_1 + tt_1)v,$$

implying that $qs_1 + st_1 = 0$ and $rs_1 + tt_1 = 1$. But then

$$\begin{bmatrix} q & s \\ r & t \end{bmatrix} \cdot \begin{bmatrix} q_1 & s_1 \\ r_1 & t_1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},$$

and since the determinant of each matrix is a rational integer, this implies that $qt - rs = \pm 1$.

Finally, we find that

$$\begin{aligned} \overline{u_1}v_1 - u_1\overline{v_1} &= (q\overline{u} + r\overline{v})(su + tv) - (qu + rv)(s\overline{u} + t\overline{v}) \\ &= (qsu\overline{u} + qt\overline{u}v + rsu\overline{v} + rtv\overline{v}) - (qsu\overline{u} + qtu\overline{v} + rs\overline{u}v + rtv\overline{v}) \\ &= qt(\overline{u}v - u\overline{v}) - rs(\overline{u}v - u\overline{v}) = (qt - rs)(\overline{u}v - u\overline{v}), \end{aligned}$$

as claimed. □

Combining Propositions 5.2.2 and 5.2.3, we have that if $\{u, v\}$ is a $\mathbb{Z}$-basis for an ideal A of D_Δ, then $\overline{u}v - u\overline{v} = \pm N(A) \cdot \sqrt{\Delta}$. In fact, we can assume that $\overline{u}v - u\overline{v} = N(A) \cdot \sqrt{\Delta}$ by interchanging u and v if necessary. We will say that $\{u, v\}$ is an *ordered basis* for A if this equation holds. By Proposition 5.2.3, if $S = \{u, v\}$ is an ordered basis for A, then $S_1 = \{u_1, v_1\}$ is also an ordered basis for A if and only if $u_1 = qu + rv$ and $v_1 = su + tv$ with $U = \begin{bmatrix} q & s \\ r & t \end{bmatrix}$ a *unimodular* matrix, that is, $qt - rs = 1$. Here U is uniquely determined by the two ordered bases. We write $\{u_1, v_1\} = \{u, v\} \circ U$, or $S_1 = S \circ U$, to indicate that $S_1 = \{u_1, v_1\}$ is obtained from $S = \{u, v\}$ in this way.

Example. Let $\Delta = -4$ so that $D = \mathbb{Z}[i]$ and $\phi(x) = x^2 + 1$. Here $A = [10 : 3]$ is an ideal of D since $\phi(3) = 10 \cdot 1$, and we have that $\{10, 3 + i\}$ is an ordered basis for A. (We can confirm that $\overline{10} \cdot (3 + i) - 10 \cdot (\overline{3 + i}) = 10(3 + i) - 10(3 - i) = 20i = 10 \cdot \sqrt{-4} = N(A) \cdot \sqrt{\Delta}$.) Using the unimodular matrix $U = \begin{bmatrix} 3 & 7 \\ 2 & 5 \end{bmatrix}$, we find that $\{10, 3 + i\} \circ U = \{36 + 2i, 85 + 5i\}$ is also an ordered basis for A. ◊

Exercise 5.2.1. Verify that $A = [8 : 3]$ is an ideal of the quadratic domain $D = D_{-111}$, so that $S = \{8, 3 + z\}$ is an ordered basis for A. For each unimodular matrix U below, find the ordered basis $S_1 = S \circ U$ for A.

(a) $U = \begin{bmatrix} 2 & 3 \\ 3 & 5 \end{bmatrix}$.

(b) $U = \begin{bmatrix} 4 & -1 \\ 5 & -1 \end{bmatrix}$.

(c) $U = \begin{bmatrix} 3 & 5 \\ 1 & 2 \end{bmatrix}$.

Theorem 5.2.4. *Let $S = \{u, v\}$ be an ordered basis for A, an ideal of the quadratic domain $D = D_\Delta$. Let*

$$a = \frac{u\overline{u}}{N(A)}, \qquad b = \frac{u\overline{v} + \overline{u}v}{N(A)}, \qquad \text{and} \qquad c = \frac{v\overline{v}}{N(A)}. \tag{5.2.2}$$

Then a, b, and c are rational integers for which $b^2 - 4ac = \Delta$, so that

$$f_S(x, y) = ax^2 + bxy + cy^2 \tag{5.2.3}$$

is an element of $\mathcal{Q}_\Delta$. For all $w = mu + nv$ in A, we have that

$$N(w) = N(A) \cdot f_S(m, n). \tag{5.2.4}$$

Definition. If A is a nontrivial ideal of a quadratic domain D_Δ, and $S = \{u, v\}$ is an ordered basis for A, we refer to f_S given by equation (5.2.3) as the *quadratic form of S*.

Proof. Assume first that A is primitive, so that $N(A)$ is the smallest positive rational integer in A. Since u and v are elements of A, then $u\overline{u}$, $u\overline{v} + \overline{u}v$, and $v\overline{v}$ are also elements of A, by the closure properties of an ideal. But each of these elements is equal to its own conjugate in D, so is also a rational integer. Thus each is divisible by $N(A)$, implying that a, b, and c are rational integers. More generally, if $A = gA_1$ for some $g > 1$ in $\mathbb{Z}$, then $u = gu_1$ and $v = gv_1$ for some u_1 and v_1 in A_1. Since $u\overline{u} = g^2 u_1\overline{u_1}$, and similarly for the other elements, we draw the same conclusion about a, b, and c. Now

$$b^2 - 4ac = \frac{1}{(N(A))^2}\left[(u\overline{v} + \overline{u}v)^2 - 4u\overline{u}\cdot v\overline{v}\right] = \frac{1}{(N(A))^2}(\overline{u}v - u\overline{v})^2 = \Delta,$$

since $\{u, v\}$ is an ordered basis for A. Finally,

$$\begin{aligned} N(w) &= (mu + nv)(m\overline{u} + n\overline{v}) \\ &= (u\overline{u})m^2 + (u\overline{v} + \overline{u}v)mn + (v\overline{v})n^2 = N(A)(am^2 + bmn + cn^2), \end{aligned}$$

that is, $N(w) = N(A)\cdot f_S(m, n)$. □

Example. In the preceding example, we saw that $S = \{36 + 2i, 85 + 5i\}$ is an ordered basis for the ideal $A = [10 : 3]$ of $D = \mathbb{Z}[i]$. If $u = 36+2i$ and $v = 85+5i$, we find that

$$u\overline{u} = 36^2 + 2^2 = 1300, \qquad v\overline{v} = 85^2 + 5^2 = 7250,$$

and

$$u\overline{v} + \overline{u}v = 2(36\cdot 85 - 2\cdot 5\cdot i^2) = 6140.$$

Since $N(A) = 10$, then $f_S(x, y) = 130x^2 + 614xy + 725y^2$. One can verify that the discriminant of f_S is $\Delta = -4$. ◊

Exercise 5.2.2. For the ordered basis S in Exercise 5.2.1, find the corresponding quadratic form f_S of $\mathcal{Q}_{-111}$. Do the same for each of the ordered bases obtained in parts (a), (b), and (c) of Exercise 5.2.1.

Theorem 5.2.5. *Let A be an ideal of the quadratic domain $D = D_\Delta$, and let $S = \{u, v\}$ and $S_1 = \{u_1, v_1\}$ be ordered bases for A, so that $S_1 = S \circ U$ for some unimodular matrix U. If $f = f_S$ and $f_1 = f_{S_1}$ are the quadratic forms of these ordered bases, then $f_1 = f \circ U$.*

Proof. Let $f(x, y) = ax^2 + bxy + cy^2$, where a, b, and c are defined for the ordered basis $S = \{u, v\}$ as in equation (5.2.2). Let $U = \begin{bmatrix} q & s \\ r & t \end{bmatrix}$ be the unimodular matrix for which $u_1 = qu + rv$ and $v_1 = su + tv$. We find that

$$u_1\overline{u_1} = q^2 u\overline{u} + qr(u\overline{v} + \overline{u}v) + r^2 v\overline{v} = N(A)(aq^2 + bqr + cr^2),$$

$$u_1\overline{v_1} + \overline{u_1}v_1 = 2qs(u\overline{u}) + (qt + rs)(u\overline{v} + \overline{u}v) + 2rt(v\overline{v})$$
$$= N(A)(2aqs + b(qt + rs) + 2crt),$$

and

$$v_1\overline{v_1} = s^2u\overline{u} + st(u\overline{v} + \overline{u}v) + t^2v\overline{v} = N(A)(as^2 + bst + ct^2).$$

So then

$$f_1(x, y) = (aq^2 + bqr + cr^2)x^2 + (2aqs + b(qt + rs) + 2crt)xy + (as^2 + bst + ct^2)y^2,$$

that is, $f_1 = f \circ U$ by equation (4.2.1). □

We now prove Theorem 5.2.1, using the following fact.

Exercise 5.2.3. Show that if $S = \{u, v\}$ is a $\mathbb{Z}$-basis for an ideal A of some quadratic domain D, then $T = \{wu, wv\}$ is a $\mathbb{Z}$-basis for the ideal wA of D.

Proof of Theorem 5.2.1. We know that $S = \{ga, gk + gz\}$ is an ordered basis for gA, with $f_S = (a : k)$ the quadratic form of S. However, $\{va_1, v(k_1 + z)\}$ is a $\mathbb{Z}$-basis for vA_1, as in Exercise 5.2.3, but is not necessarily an ordered basis. Note that $N(vA_1) = N(\langle v\rangle A_1) = N(\langle v\rangle) \cdot N(A_1)$ by Theorem 3.6.6, since a principal ideal has index 1. It follows that $N(vA_1) = N(v) \cdot N(A_1)$ if $N(v)$ is positive, while $N(vA_1) = -N(v) \cdot N(A_1)$ if $N(v)$ is negative.

Suppose first that $N(v)$ is positive, so that $N(vA_1) = N(v) \cdot N(A_1)$. In that case, $S_1 = \{va_1, v(k_1 + z)\}$ is an ordered basis for vA_1, since

$$\overline{va_1} \cdot v(k_1 + z) - va_1 \cdot \overline{v(k_1 + z)} = N(v) \cdot a_1(z - \overline{z}) = N(vA_1)\sqrt{\Delta}.$$

We then can show that $f_{S_1} = (a_1 : k_1)$, using the equations of (5.2.2) in Theorem 5.2.4. Specifically,

$$va_1 \cdot \overline{va_1} = v\overline{v}a_1^2 = N(vA_1)a_1,$$

$$va_1 \cdot \overline{v(k_1 + z)} + \overline{va_1} \cdot v(k_1 + z) = N(vA_1)((k_1 + \overline{z}) + (k_1 + z))$$
$$= N(vA_1)b_1,$$

and

$$v(k_1 + z) \cdot \overline{v(k_1 + z)} = v\overline{v} \cdot (k_1 + z)(k_1 + \overline{z}) = N(vA_1)c_1,$$

where $a_1c_1 = \phi(k_1)$ and $b_1 = \phi'(k_1)$. But now since S and S_1 are ordered bases for the same ideal, $gA = vA_1$, there is a unimodular matrix U so that $f_S \circ U = f_{S_1}$, by Theorem 5.2.5. Thus $(a : k) \sim (a_1 : k_1)$.

Now suppose that $N(v)$ is negative, so that $N(vA_1) = -N(v) \cdot N(A_1)$. Here we find that $S_1 = \{va_1, -v(k_1 + z)\}$ is an ordered basis for vA_1, since

$$\overline{va_1} \cdot -v(k_1 + z) - va_1 \cdot \overline{-v(k_1 + z)} = -N(v) \cdot a_1(z - \overline{z}) = N(vA_1)\sqrt{\Delta}.$$

In this case, the equations of (5.2.2) show that $f_{S_1} = (-a_1 : k_1)$. Specifically,

$$va_1 \cdot \overline{va_1} = N(v)a_1^2 = -N(v) \cdot N(A_1)(-a_1) = N(vA_1)(-a_1),$$

$$\begin{aligned} \upsilon a_1 \cdot \overline{-\upsilon(k_1+z)} + \overline{\upsilon a_1} \cdot -\upsilon(k_1+z) &= -N(\upsilon)\cdot N(A_1)((k_1+\overline{z})+(k_1+z)) \\ &= N(\upsilon A_1)b_1, \end{aligned}$$

and

$$-\upsilon(k_1+z)\cdot\overline{-\upsilon(k_1+z)} = N(\upsilon)\cdot(k_1+z)(k_1+\overline{z}) = N(\upsilon A_1)(-c_1),$$

where $a_1c_1 = (-a_1)(-c_1) = \phi(k_1)$ and $b_1 = \phi'(k_1)$. Again, S and S_1 are ordered bases for the same ideal, and so $(a : k) \sim (-a_1 : k_1)$ in this case. □

5.3 Composition of Binary Quadratic Forms

In this section, we introduce another important connection between quadratic forms and ideals. We begin with the following claim, stated purely in terms of quadratic forms. If f_1 and f_2 are primitive quadratic forms of the same discriminant Δ, then there is a form f in $\mathcal{Q}_\Delta$ with the following property:

If f_1 represents m and f_2 represents n, then f represents mn.

We will give a formula for such a form f in terms of f_1 and f_2, and thus define an operation of *composition* on primitive quadratic forms of discriminant Δ. The concept of composition was present in the early development of quadratic forms, particularly in the work of Lagrange, but was made complete and precise by Gauss in *Disquisitiones Arithmeticae* (1801). Here we will demonstrate that composition of quadratic forms is consistent with multiplication of ideals. (The development of ideals was, as we have seen, a later innovation of Kummer and Dedekind.) We begin with some examples and general statements that illustrate a method of composition in practice, and suggest a connection with ideal multiplication.

Example. In considering sums of two squares in §1.1, we often used the following equation:

$$(q^2+r^2)(s^2+t^2) = (qs-rt)^2 + (qt+rs)^2.$$

While we established this fact first by direct calculation, it can be better explained using the multiplicative property of norms of Gaussian integers:

$$\begin{aligned} (q^2+r^2)(s^2+t^2) = N(q+ri)\cdot N(s+ti) &= N((q+ri)(s+ti)) \\ &= N((qs-rt)+(qt+rs)i) = (qs-rt)^2+(qt+rs)^2. \end{aligned}$$

If $f(x,y) = x^2+y^2$, this equation implies that if f represents m and f represents n, then f represents mn. We might interpret this as saying that the composition of f with itself is equal to f. Note that in $\mathcal{Q}_{-4}$, we can write $f = (1 : 0)$, with the corresponding ideal given by $A_f = [1 : 0]$. It is the case that $[1 : 0]\cdot[1 : 0] = [1 : 0]$. ◊

We can generalize this example with the following proposition, making a similar claim about the principal form of any discriminant.

Proposition 5.3.1. *Let $\phi(x,y) = x^2 + \varepsilon xy + \frac{\varepsilon^2-\Delta}{4}y^2$ be the principal form of some discriminant Δ. Suppose that $\phi(q,r) = m$ and $\phi(s,t) = n$ for some integers q, r, s, and t. Then $\phi(u,v) = mn$, where*

$$u = qs - \frac{\varepsilon^2-\Delta}{4}rt \qquad \text{and} \qquad v = qt + rs + \varepsilon rt. \tag{5.3.1}$$

Proof. Let $z = z_\Delta$ in the quadratic domain $D = D_\Delta$. By equation (2.2.5), we have that $\phi(q,r) = N(q+rz)$ for every pair of integers q and r. Using the multiplicative property of the norm, and the multiplication formula of equation (2.2.8), we then have that

$$mn = \phi(q,r)\cdot\phi(s,t) = N((q+rz)(s+tz)) = N(u+vz) = \phi(u,v),$$

where u and v are given as in equation (5.3.1). □

Example. Let $\Delta = -3$ so that $\varepsilon = 1$ and $\phi(x,y) = x^2+xy+y^2$. Proposition 5.3.1 implies that

$$(q^2+qr+r^2)(s^2+st+t^2) = (qs-rt)^2 + (qs-rt)(qt+rs+rt) + (qt+rs+rt)^2,$$

which can be verified by direct calculation. ◊

We now consider a discriminant for which there are distinct classes of quadratic forms.

Example. Let $\Delta = -20$, so that $z = \sqrt{-5}$ in the quadratic domain $D = D_\Delta$. Let

$$f = (1:0) = x^2 + 5y^2 \qquad \text{and} \qquad g = (2:1) = 2x^2 + 2xy + 3y^2,$$

quadratic forms of discriminant $\Delta = -20$. Here we find that f and g have different genus symbols,

$$\left(\frac{-1}{f}\right) = 1 = \left(\frac{f}{5}\right) \quad \text{while} \quad \left(\frac{-1}{g}\right) = -1 = \left(\frac{g}{5}\right),$$

so cannot be equivalent to each other. Since f is the principal form of discriminant -20, we have that $f(q,r) = N(q+rz)$ for all integers q and r. Proposition 5.3.1 implies that if $f(q,r) = m$ and $f(s,t) = n$, then $f(u,v) = mn$, where $u = qs - 5rt$ and $v = qt + rs$.

We will describe similar products of representations by g. First we observe the following equation relating a representation by g to the norm of an element of D:

$$\begin{aligned} 2g(q,r) = 4q^2 + 4qr + 6r^2 &= (4q^2+4qr+r^2) + 5r^2 \\ &= (2q+r)^2 + 5r^2 = N((2q+r)+rz). \end{aligned} \tag{5.3.2}$$

Notice that $w = (2q + r) + rz = q(2) + r(1 + z)$ is a typical $\mathbb{Z}$-combination of $\{2, 1 + z\}$, an ordered basis of the ideal $A_g = [2 : 1]$. Equation (5.3.2) states that $N(w) = N(A_g) \cdot g(q, r)$, as in equation (5.2.4) of Theorem 5.2.4.

Suppose that $f(q, r) = m$ and $g(s, t) = n$ for some integers q, r, s, and t. We will show that mn is represented by g. (This outcome is suggested by the fact that $A_f \cdot A_g = [1 : 0] \cdot [2 : 1] = [2 : 1] = A_g$.) Notice that

$$\begin{aligned} 2mn &= f(q, r) \cdot 2g(s, t) = N(q + rz) \cdot N((2s + t) + tz) \\ &= N((q + rz)((2s + t) + tz)) = N((2qs + qt - 5rt) + (qt + 2rs + rt)z), \end{aligned}$$

since $z^2 = -5$. This equals $2g(u, v)$ if

$$2u + v = 2qs + qt - 5rt \quad \text{and} \quad v = qt + 2rs + rt,$$

by equation (5.3.2). Thus if $f(q, r) = m$ and $g(s, t) = n$, then $g(u, v) = mn$, where

$$u = qs - rs - 3rt \qquad \text{and} \qquad v = qt + 2rs + rt.$$

Now suppose that $g(q, r) = m$ and $g(s, t) = n$ for some integers q, r, s, and t. Note that $A_g \cdot A_g = [2 : 1] \cdot [2 : 1] = 2[1 : 0]$, since A_g is its own conjugate. With $2[1 : 0]$ equivalent to $A_f = [1 : 0]$, we may conjecture that mn is represented by f. We can show as follows that this is the case. Here

$$\begin{aligned} 4mn = 2g(q, r) \cdot 2g(s, t) &= N(((2q + r) + rz)((2s + t) + tz)) \\ &= N((4qs + 2qt + 2rs + rt) + (2qt + rt + 2rs + rt)z + rtz^2) \\ &= N((4qs + 2qt + 2rs - 4rt) + (2qt + 2rs + 2rt)z). \end{aligned}$$

Since $N(2u + 2vz) = 4N(u + vz) = 4f(u, v)$, we conclude that $f(u, v) = mn$, where $u = 2qs + qt + rs - 2rt$ and $v = qt + rs + rt$. ◊

Exercise 5.3.1. Let $f(x, y) = x^2 + 5y^2$ and $g(x, y) = 2x^2 + 2xy + 3y^2$. Verify that

$$f(2, 1) = 9, \quad f(3, 1) = 14, \quad g(1, 1) = 7, \quad \text{and} \quad g(2, 1) = 15.$$

Use these facts to help find solutions of the following equations.

(a) $f(x, y) = 126 = 9 \cdot 14$.

(b) $f(x, y) = 105 = 7 \cdot 15$.

(c) $g(x, y) = 63 = 9 \cdot 7$.

(d) $g(x, y) = 98 = 14 \cdot 7$.

(e) $g(x, y) = 135 = 9 \cdot 15$.

(f) $g(x, y) = 210 = 14 \cdot 15$.

Formula for Composition. We can generalize the outcome of these examples in the following definition of composition.

Definition. Let $f_1 = (a_1 : k_1)$ and $f_2 = (a_2 : k_2)$ be primitive quadratic forms and $\phi(x)$ the principal polynomial of some discriminant Δ. Let $a_3 = k_1 + k_2 + \phi'(0)$ and let $g = \gcd(a_1, a_2, a_3)$. Then we define $f_1 \cdot f_2$ to be the quadratic form $f = (a : k)$, where $a = a_1 a_2 / g^2$ and k satisfies the congruences

$$k \equiv k_1 \pmod{a_1/g}, \qquad k \equiv k_2 \pmod{a_2/g},$$

and

$$a_3 k \equiv k_1 k_2 - \phi(0) \pmod{ag}.$$

(We select k so that $-a < \phi'(k) \leq a$.) We refer to this operation as *composition* of f_1 and f_2, and we call f the *composite* of f_1 and f_2.

Note that we do not require a_1 or a_2 to be positive in this formula. In the congruence statements, we replace each modulus by its absolute value if necessary. We will show that $f = f_1 \cdot f_2$ has the property by which we described composition at the beginning of this section. We begin with the following lemma.

Lemma 5.3.2. *Let D be the quadratic domain and $\phi(x)$ the principal polynomial of some discriminant Δ. Let a be a positive integer and let k be an integer so that a divides $\phi(k)$. Let $f = ((-1)^e a : k)$ for some integer e. Then for all integers q and r,*

$$N(q(-1)^e a + r(k + z)) = (-1)^e a f(q, r), \tag{5.3.3}$$

where $z = z_\Delta$ and N denotes the norm of an element of D.

Proof. Let $w = k + z$, and let $\phi(k) = ac = w\overline{w}$ and $\phi'(k) = b = w + \overline{w}$. If e is even, then $f = (a : k) = ax^2 + bxy + cy^2$, and we find that

$$\begin{aligned} N(qa + rw) &= (qa + rw)(qa + r\overline{w}) \\ &= a^2q^2 + aqr(w + \overline{w}) + r^2(w\overline{w}) = a(aq^2 + bqr + cr^2). \end{aligned}$$

If e is odd, then $f = (-a : k) = -ax^2 + bxy - cy^2$ (since $\phi(k) = -a \cdot -c$), and

$$\begin{aligned} N(-qa + rw) &= (-qa + rw)(-qa + r\overline{w}) \\ &= a^2q^2 - aqr(w + \overline{w}) + r^2(w\overline{w}) = -a(-aq^2 + bqr - cr^2). \end{aligned}$$

Both equations are in the form of (5.3.3). □

We can rephrase Lemma 5.3.2 as saying that if $f = (a : k)$, then

$$N(qa + r(k + z)) = af(q, r)$$

whether a is positive or negative.

Theorem 5.3.3. *Let f_1 and f_2 be primitive quadratic forms of discriminant Δ, and let $f = f_1 \cdot f_2$. If $f_1(q,r) = m$ and $f_2(s,t) = n$ for some integers q, r, s, and t, then there are integers u and v so that $f(u,v) = mn$. Specifically, let $f_1 = (a_1 : k_1)$ and $f_2 = (a_2 : k_2)$, let $\phi(x)$ be the principal polynomial of discriminant Δ, with $a_3 = k_1 + k_2 + \phi'(0)$ and $g = \gcd(a_1, a_2, a_3)$, and let $f = (a : k)$ as in the definition of composition. Then u and v satisfy the equations*

$$gv = a_1qt + a_2rs + a_3rt$$

and

$$(ga)u = (a_1a_2)qs - a_1(k - k_2)qt - a_2(k - k_1)rs + (k_1k_2 - \phi(0) - a_3k)rt.$$

Proof. Let $A_1 = [a_1 : k_1]$ and $A_2 = [a_2 : k_2]$ be the ideals of f_1 and f_2, respectively, and let $A = A_1 \cdot A_2$. The assumption that f_1 and f_2 are primitive quadratic forms ensures that A_1 and A_2 have index 1, so the ideal multiplication formula of Theorem 3.6.1 implies that $A = g[a : k]$, where g and $f = (a : k)$ are as given in the definition of $f = f_1 \cdot f_2$. Let $w = k + z$, $w_1 = k_1 + z$, and $w_2 = k_2 + z$. We have that

$$N(qa_1 + rw_1) = a_1 \cdot f_1(q,r) = a_1m$$

and

$$N(sa_2 + tw_2) = a_2 \cdot f_2(s,t) = a_2n$$

by Lemma 5.3.2, and so

$$a_1a_2mn = N(qa_1 + rw_1) \cdot N(sa_2 + tw_2) = N((qa_1 + rw_1)(sa_2 + tw_2)). \quad (5.3.4)$$

Now the product $(qa_1 + rw_1)(sa_2 + tw_2)$ is an element of $A_1A_2 = A$ so can be written as $u(ga) + v(gw)$ for some integers u and v. But then

$$N(u(ga) + v(gw)) = g^2N(ua + vw) = g^2a \cdot f(u,v), \quad (5.3.5)$$

again by Lemma 5.3.2. Since $g^2a = a_1a_2$ by the definition of composition, combining equations (5.3.4) and (5.3.5) yields the conclusion that $f(u,v) = mn$.

The formulas for v and u in Theorem 5.3.3 are obtained by expanding the product

$$(qa_1 + rw_1)(sa_2 + tw_2) = ((qa_1 + rk_1) + rz)((sa_2 + tk_2) + tz) \quad (5.3.6)$$

and setting that expression equal to

$$u(ga) + v(gw) = ((ga)u + (gk)v) + (gv)z. \quad (5.3.7)$$

Applying the multiplication formula of equation (2.2.8) to (5.3.6) and comparing coefficients of z produces the equation for gv. Comparing the coefficients of 1, we find

$$(ga)u + k(gv) = (qa_1 + rk_1)(sa_2 + tk_2) - rt \cdot \phi(0).$$

Using the formula for gv and the definition of $\phi(x)$ produces the equation for $(ga)u$. We omit the details. □

Example. Let $\Delta = 21$, so that $\phi(x) = x^2 + x - 5$. Let

$$f_1 = (-3 : 1) = -3x^2 + 3xy + y^2 \quad \text{and} \quad f_2 = (5 : 4) = 5x^2 + 9xy + 3y^2.$$

Here $a_1 = -3$, $a_2 = 5$, and $a_3 = k_1 + k_2 + \phi'(0) = 6$, so that $g = \gcd(-3, 5, 6) = 1$. The composition formula implies that

$$f = f_1 \cdot f_2 = (-15 : 4) = -15x^2 + 9xy - y^2.$$

If $f_1(q, r) = m$ and $f_2(s, t) = n$, then $f(u, v) = mn$, where

$$v = a_1qt + a_2rs + a_3rt = -3qt + 5rs + 6rt$$

and

$$-15u = (a_1a_2)qs - a_1(k - k_2)qt - a_2(k - k_1)rs + (k_1k_2 - \phi(0) - a_3k)rt$$

so that

$$u = -\frac{1}{15}(-15qs + 0qt - 15rs + (4 + 5 - 24)rt) = qs + rs + rt.$$

For example, $f_1(1, 5) = 37$ and $f_2(2, 1) = 41$, so if

$$u = 1(2) + 5(2) + 5(1) = 17 \quad \text{and} \quad v = -3(1)(1) + 5(5)(2) + 6(5)(1) = 77,$$

we find that $f(17, 77) = 1517 = 37 \cdot 41$. ◊

Example. Let $\Delta = -84$, so that $\phi(x) = x^2 + 21$. Let

$$f_1 = (2 : 1) = 2x^2 + 2xy + 11y^2 \quad \text{and} \quad f_2 = (3 : 0) = 3x^2 + 7y^2,$$

and then

$$f = f_1 \cdot f_2 = (6 : 3) = 6x^2 + 6xy + 5y^2.$$

If $f_1(q, r) = m$ and $f_2(s, t) = n$, we find that $f(u, v) = mn$ if

$$v = a_1qt + a_2rs + a_3rt = 2qt + 3rs + rt$$

(here $a_3 = k_1 + k_2 + \phi'(0) = 1$) and

$$6u = (a_1a_2)qs - a_1(k - k_2)qt - a_2(k - k_1)rs + (k_1k_2 - \phi(0) - a_3k)rt$$

so that

$$u = \frac{1}{6}(6qs - 6qt - 6rs + (0 - 21 - 3)rt) = qs - qt - rs - 4rt.$$

For example, since $f_1(3, -1) = 23$ and $f_2(2, 1) = 19$, we find that $f(9, -1) = 437 = 23 \cdot 19$. ◊

Exercise 5.3.2. In each part, use Theorem 5.3.3 to find a composite form f for the given quadratic forms f_1 and f_2 in $\mathcal{Q}_\Delta$, and find u and v, in terms of q, r, s, and t, for which $f_1(q, r) \cdot f_2(s, t) = f(u, v)$.

(a) $f_1(x, y) = x^2 + 2y^2 = f_2(x, y)$ in $\mathcal{Q}_{-8}$.

(b) $f_1(x, y) = 2x^2 + 3y^2 = f_2(x, y)$ in $\mathcal{Q}_{-24}$.

(c) $f_1(x,y) = 2x^2 + xy + 3y^2 = f_2(x,y)$ in $\mathcal{Q}_{-23}$.

(d) $f_1(x,y) = 2x^2 + xy + 3y^2$ and $f_2(x,y) = 2x^2 - xy + 3y^2$ in $\mathcal{Q}_{-23}$.

(e) $f_1(x,y) = 2x^2 + xy + 6y^2 = f_2(x,y)$ in $\mathcal{Q}_{-47}$.

(f) $f_1(x,y) = 2x^2 + xy + 6y^2$ and $f_2(x,y) = 3x^2 + xy + 4y^2$ in $\mathcal{Q}_{-47}$.

(g) $f_1(x,y) = x^2 - 2y^2 = f_2(x,y)$ in $\mathcal{Q}_8$.

(h) $f_1(x,y) = x^2 - 10y^2 = f_2(x,y)$ in $\mathcal{Q}_{40}$.

(i) $f_1(x,y) = 2x^2 - 5y^2 = f_2(x,y)$ in $\mathcal{Q}_{40}$.

(j) $f_1(x,y) = x^2 - 10y^2$ and $f_2(x,y) = 2x^2 - 5y^2$ in $\mathcal{Q}_{40}$.

5.4 Class Groups of Ideals and Quadratic Forms

Throughout this chapter, we have made connections between quadratic forms of discriminant Δ and ideals of the quadratic domain D_Δ. We have seen in particular that the relation of equivalence of quadratic forms carries over to a similar relation on ideals. In §5.3, we found that ideal multiplication induces an operation of composition on primitive quadratic forms. To conclude Chapter 5, we combine these concepts with a multiplication operation defined on classes under equivalence, first for ideals and then for quadratic forms. We first note a connection between principal ideals of a quadratic domain and unique irreducible factorization as follows.

Principal Ideals. Recall that a quadratic domain D is called a *principal ideal domain* if every ideal of D is a principal ideal. Corollary 3.6.4 states that every principal ideal of a quadratic domain D has index 1. So if D is not a *complete* quadratic domain, then D cannot be a principal ideal domain.

Theorem 5.4.1. *Let D be a quadratic domain. Then D is a principal ideal domain if and only if D is a unique factorization domain.*

In more general examples of integral domains, it is always the case that a principal ideal domain is a unique factorization domain. We will outline the proof of this claim in the following exercises. The converse of this statement is not always true in an arbitrary integral domain. We will prove that it is the case for quadratic domains, however, using properties that we have established in that setting.

Exercise 5.4.1. Let D be a quadratic domain. Recall that an element u of D that is neither zero nor a unit is called *irreducible* if when $u = vw$, then either v or

w is a unit in D. Show that if u is irreducible in D, and $\langle u\rangle \subseteq \langle v\rangle$ for some v in D, then either $\langle v\rangle = \langle u\rangle$ or $\langle v\rangle = D$. (We may say that $\langle u\rangle$ is *maximal among principal ideals* in this case.)

Exercise 5.4.2. Let D be a quadratic domain, and suppose that D is a principal ideal domain. Use Exercise 5.4.1 to show that if u is an irreducible element of D, then $\langle u\rangle$ is a prime ideal of D.

Exercise 5.4.3. Let D be a quadratic domain. Recall that an element u of D that is neither zero nor a unit is called *prime* if when u divides vw in D, then u divides v or u divides w. Show that if $\langle u\rangle$ is a prime ideal of D, then u is prime as an element of D. (Hint: Use the characterization of prime ideals in Proposition 3.3.2.)

Exercise 5.4.4. Let D be a quadratic domain. Show that if D is a principal ideal domain, then D is a unique factorization domain. (Hint: Use the fact noted in §2.5 that a quadratic domain D is a unique factorization domain if and only if every irreducible element of D is also prime.)

Proof of Theorem 5.4.1. Let D be a quadratic domain. We will show that if D is *not* a principal ideal domain, then D must contain an irreducible element that is not prime, so is not a unique factorization domain. (This indirectly proves the converse of the claim in Exercise 5.4.4, and thus completes the proof of Theorem 5.4.1.)

First note as follows that if not every ideal of D is principal, then D contains a *prime* ideal that is not principal. If D is a complete quadratic domain, then every ideal of D other than $\{0\} = \langle 0\rangle$ and $D = \langle 1\rangle$ can be written as a product of prime ideals. If all prime ideals were principal, then all such products would also be principal. On the other hand, suppose that $D = D_\Delta$ is not a complete quadratic domain, so that $\Delta = \Delta(d, \gamma)$ with $\gamma > 1$, and let p be a prime number dividing γ. In that case, $P = [p : 0]$ is a prime ideal of D that is not a principal ideal, since we find that $\gamma(P) = p$.

Let P be a prime ideal of D with $P \neq \langle u\rangle$ for all u in D. We know that there is a rational prime p contained in P, and in this case, $N(P) = p$. (The only other possibility is $N(P) = p^2$, but that occurs only when $P = \langle p\rangle$, which is principal.) We claim that p is an irreducible element in D. Otherwise, $p = vw$ for some v and w in D with neither v nor w a unit in D. Then $N(p) = p^2 = N(v)N(w)$, which implies that $N(v) = \pm p = N(w)$. On the other hand, since $vw = p$ is in the prime ideal P, then either v or w is in P. We can assume that v is in P without loss of generality. But now notice that $\langle v\rangle \subseteq P$ and that $N(\langle v\rangle) = |N(v)| = p = N(P)$, from which we conclude that $P = \langle v\rangle$. This is impossible since P is not a principal ideal.

On the other hand, we can show that p is not prime as an element of D. Let v be an element of P that is not divisible by p. (Such an element must exist since

otherwise $P = \langle p \rangle$.) In that case, $\overline{v}$ is an element of D that is also not divisible by p, but then $v\overline{v} = N(v)$ is a rational integer in the ideal P. We know that every rational integer in P is divisible by p, so we have that p divides $v\overline{v}$, but does not divide either v or $\overline{v}$. Thus p is not prime in D, but is irreducible in D, and so we conclude that D is not a unique factorization domain. □

The Ideal Class Group. In §3.5, we noted that principal ideals of a quadratic domain D might be identified with elements of D, while ideals that are not principal play the part of "ideal numbers" that, while not elements of D, produce a form of unique irreducible factorization of elements of D. We now introduce a definition that we might interpret as determining how many (classes of) such ideal numbers are needed to produce unique factorization.

Let $D = D_\Delta$ be a quadratic domain and consider the collection of all classes of nontrivial ideals of D under the relation of equivalence defined in §5.1. We denote the class of an ideal A as $[A]$. Proposition 5.1.3 implies that we can define the *index* of $[A]$ to be the same as $\gamma(A)$. (That is, this characteristic of an ideal class is well-defined, since if A is equivalent to B, then $\gamma(A) = \gamma(B)$.) We write $\mathcal{C}_\Delta$ for the collection of ideal classes of D_Δ of index 1.

Proposition 5.4.2. *Let D be the quadratic domain of discriminant Δ, and let $\mathcal{C}_\Delta$ be the set of all equivalence classes, under the $\sim$ relation, of ideals A for which $\gamma(A) = 1$. Then there is a well-defined operation of multiplication on $\mathcal{C}_\Delta$ given by $[A]\cdot[B] = [AB]$. This operation has the following properties.*

(1) *Multiplication is commutative:* $[A] \cdot [B] = [B] \cdot [A]$ *for all* $[A], [B] \in \mathcal{C}_\Delta$.

(2) *Multiplication is associative:* $([A]\cdot[B])\cdot[C] = [A]\cdot([B]\cdot[C])$ *for all* $[A], [B], [C] \in \mathcal{C}_\Delta$.

(3) *The class of D, as an ideal of itself, is an identity element for multiplication:* $[A] \cdot [D] = [A]$ *for all* $[A] \in \mathcal{C}_\Delta$.

(4) *For each* $[A] \in \mathcal{C}_\Delta$, *the class of* $\overline{A}$ *is an inverse for* $[A]$ *under multiplication:* $[A] \cdot [\overline{A}] = [D]$.

In algebraic terminology, Proposition 5.4.2 implies that $\mathcal{C}_\Delta$ has the properties of an *abelian group* under multiplication.

Definition. We refer to $\mathcal{C}_\Delta$ as the *ideal class group* of discriminant Δ.

Proof. By Exercise 5.1.2, multiplication is a well-defined operation on the set of all classes of nontrivial ideals of D. Theorem 3.6.6 implies that $\gamma(AB) = \operatorname{lcm}(\gamma(A), \gamma(B))$, so that $\mathcal{C}_\Delta$ is closed under multiplication. Note that $[D]$ is an element of $\mathcal{C}_\Delta$ for every Δ, since $D = \langle 1 \rangle$ is a principal ideal, so has index 1

by Corollary 3.6.4. Now statements (1), (2), and (3) of this proposition hold in $\mathcal{C}_\Delta$ because they are true for ideal multiplication in general. (See Exercise 3.4.2.) Finally, if A has index 1, then Theorem 3.4.2 implies that $A\overline{A} = \langle N(A)\rangle$, a principal ideal. Notice that Theorem 3.6.6 and Corollary 3.6.4 then imply that $\overline{A}$ must also have index 1. It follows that $[A] \cdot [\overline{A}] = [D]$ in $\mathcal{C}_\Delta$, since a principal ideal is equivalent to D by Proposition 5.1.2. □

Exercise 5.1.3 shows that if $B = \upsilon A$ for some nonzero element υ and nontrivial ideal A of $D = D_\Delta$, then $[B] = [A]$. So we can restrict our attention to *primitive* ideals of D as representatives of elements of $\mathcal{C}_\Delta$. If A and B are primitive ideals, their product is not necessarily primitive. But if $AB = gC$, then $[A] \cdot [B] = [C]$.

In Theorem 5.4.1, we saw that a quadratic domain D is a unique factorization domain if and only if all of its ideals are principal ideals. In that case, $[A] = [D]$ for all ideals A of D. So we can now also say that if D is a *complete* quadratic domain (so that $\gamma(A) = 1$ for all ideals A of D), then D is a unique factorization domain if and only if its ideal class group is trivial, that is, contains only the identity element $[D]$. In a sense, we may think of the ideal class group as a measure of how far the quadratic domain D is from having unique factorization.

The Form Class Group. Let $\mathcal{Q}_\Delta$ be the set of all quadratic forms of some discriminant Δ, and consider the collection of all classes, $[f]$, of elements f of $\mathcal{Q}_\Delta$. We can define the *index* of $[f]$ to be the same as $\gamma(f)$, since Corollary 4.3.2 shows that equivalent forms have the same index. Then let $\mathcal{F}_\Delta$ be the set of all classes of quadratic forms in $\mathcal{Q}_\Delta$ that have index 1, that is, primitive quadratic forms of discriminant Δ. In §5.3, we defined an operation of composition on primitive quadratic forms in $\mathcal{Q}_\Delta$. This operation makes $\mathcal{F}_\Delta$ into a group.

Proposition 5.4.3. *Let $\mathcal{F}_\Delta$ be the set of all classes, under the $\sim$ relation, of primitive quadratic forms of discriminant Δ. Then there is a well-defined operation on $\mathcal{F}_\Delta$ given by $[f] \cdot [g] = [f \cdot g]$ (where $f \cdot g$ is the composite of f and g), and $\mathcal{F}_\Delta$ is an abelian group under this operation.*

Definition. We call $\mathcal{F}_\Delta$ the *form class group* of discriminant Δ. We will usually refer to the operation on $\mathcal{F}_\Delta$ defined above as multiplication.

Proof. We show that the operation of multiplication on $\mathcal{F}_\Delta$ is well-defined. Verification of the group properties then follows immediately from the same properties for ideal class multiplication. So suppose that $f_1 = (a_1 : k_1)$ and $f_2 = (a_2 : k_2)$ are equivalent primitive quadratic forms in $\mathcal{Q}_\Delta$ for some Δ. If $A_1 = [a_1 : k_1]$ and $A_2 = [a_2 : k_2]$ are the corresponding ideals of f_1 and f_2, respectively, then the proof of Theorem 5.1.5 shows that A_1 is equivalent to A_2, and that we can write $a_2 A_1 = \upsilon A_2$ for some υ with $N(\upsilon) = a_1 a_2$. Similarly, suppose that $g_1 = (b_1 : \ell_1)$ and $g_2 = (b_2 : \ell_2)$ are equivalent, with corresponding ideals

$B_1 = [b_1 : \ell_1]$ and $B_2 = [b_2 : \ell_2]$. Again, we know that $b_2 B_1 = wB_2$ for some w with $N(w) = b_1 b_2$. Let $f_1 \cdot g_1 = (c_1 : m_1)$ and $f_2 \cdot g_2 = (c_2 : m_2)$. We would like to show that $f_1 \cdot g_1$ is equivalent to $f_2 \cdot g_2$. We know that $A_1 B_1 = [c_1 : m_1]$ and $A_2 B_2 = [c_2 : m_2]$ are equivalent, with

$$a_2 b_2 \cdot A_1 B_1 = a_2 A_1 \cdot b_2 B_1 = vA_2 \cdot wB_2 = vw \cdot A_2 B_2.$$

Note that $N(vw) = N(v) \cdot N(w) = a_1 a_2 \cdot b_1 b_2 = (a_1 b_1)(a_2 b_2)$ has the same sign as $c_1 c_2$ by the definition of quadratic form composition. It follows that $f_1 \cdot g_1$ is equivalent to $f_2 \cdot g_2$ in every case by Theorem 5.2.1. □

Connection between Class Groups. To conclude this section, we note a general statement about similarities between $\mathcal{C}_\Delta$ and $\mathcal{F}_\Delta$ for the same discriminant Δ. Here we will assume that $\mathcal{C}_\Delta$ is always finite, a fact we will verify in Chapter 6 for $\Delta < 0$ and in Chapter 10 for $\Delta > 0$.

Proposition 5.4.4. *Let Δ be a discriminant, and suppose that*

$$A_1 = [a_1 : k_1], \quad A_2 = [a_2 : k_2], \quad \dots, \quad A_n = [a_n : k_n]$$

are representatives of all distinct classes of ideals in $\mathcal{C}_\Delta$. Then every primitive quadratic form of discriminant Δ is equivalent to (at least) one of the following:

$$\begin{aligned}(a_1 : k_1), \quad (a_2 : k_2), \quad \dots, \quad (a_n : k_n),\\ (-a_1 : k_1), \quad (-a_2 : k_2), \quad \dots, \quad (-a_n : k_n).\end{aligned} \tag{5.4.1}$$

If D_Δ has an element of norm -1, then $(a_i : k_i) \sim (-a_i : k_i)$ for $1 \le i \le n$, and $\mathcal{F}_\Delta$ consists precisely of the classes of $(a_1 : k_1), (a_2 : k_2), \dots, (a_n : k_n)$. If not, then the classes of the forms in (5.4.1) *are all distinct, so $\mathcal{F}_\Delta$ has $2n$ elements.*

Proof. By Theorem 5.2.1, if $[a_i : k_i] \sim [a_j : k_j]$, then $(a_i : k_i) \sim (a_j : k_j)$ or $(a_i : k_i) \sim (-a_j : k_j)$ or both. So every primitive form in $\mathcal{Q}_\Delta$ is equivalent to at least one of the forms in (5.4.1). On the other hand, by Theorem 5.1.5, we have that if $(a_i : k_i) \sim (a_j : k_j)$ or $(a_i : k_i) \sim (-a_j : k_j)$, then $[a_i : k_i] \sim [a_j : k_j]$. If v is an element of $D = D_\Delta$ with $N(v) = -1$, then v is a unit in D so that $\langle v \rangle = D$. In that case, $1 \cdot A = v \cdot A$ for every ideal, and so $(a_i : k_i) \sim (-a_i : k_i)$ for all $1 \le i \le n$. Conversely, if $(a_i : k_i) \sim (-a_i : k_i)$ for any i, then we find, by multiplying the classes of both forms by the inverse of one of those classes, that $(1 : 0) \sim (-1 : 0)$. In that case, D contains an element v of norm -1. □

When Δ is negative, then $N(v) \ge 0$ for all v in D_Δ, so in that case, $\mathcal{F}_\Delta$ always has twice the number of elements as $\mathcal{C}_\Delta$. We will often restrict our attention to positive definite forms, however. When Δ is negative, we will view $\mathcal{C}_\Delta$ either as the group of ideal classes of D_Δ or as the subgroup of $\mathcal{F}_\Delta$ consisting of classes of primitive positive definite forms.

When Δ is positive, then $|\mathcal{F}_\Delta|$ can equal either $|\mathcal{C}_\Delta|$ or $2|\mathcal{C}_\Delta|$. As Proposition 5.4.4 indicates, the determining factor is whether or not D_Δ contains an element of norm -1.

Example. If $\Delta = 8$, then $z = \sqrt{2}$ and $N(q+rz) = q^2-2r^2$. We find that $v = 1+z$ is an element of D_8 with $N(v) = -1$. So $|\mathcal{F}_8| = |\mathcal{C}_8|$. ◊

Example. If $\Delta = 12$, then $z = \sqrt{3}$ and $N(q + rz) = q^2 - 3r^2$. Since $q^2 - 3r^2 \equiv q^2 + r^2 \pmod 4$, we find that there is no v with $N(v) = -1$, as a sum of two squares cannot be congruent to 3 modulo 4. So $|\mathcal{F}_{12}| = 2|\mathcal{C}_{12}|$. ◊

Exercise 5.4.5. Let $\Delta = -20$. Assuming (as is the case), that $\mathcal{C}_\Delta$ consists of the classes of $D = [1 : 0]$ and $A = [2 : 1]$, write a complete operation table of the group $\mathcal{C}_\Delta$. Do the same for the group $\mathcal{F}_\Delta$.

Exercise 5.4.6. Let $\Delta = -56$. Assuming that $\mathcal{C}_\Delta$ consists of the classes of $D = [1 : 0]$, $A = [2 : 0]$, $B = [3 : 1]$, and $C = [3 : -1]$, write a complete operation table of the group $\mathcal{C}_\Delta$.

Correspondence between Forms and Ideals—Review

In this chapter, we saw several important connections, which we will use often in the remainder of this text, between quadratic forms of a particular discriminant Δ and ideals of the quadratic domain D_Δ. We summarize our main results as follows.

(1) There is an equivalence relation on ideals of a quadratic domain D defined by saying that A is *equivalent* to B (written as $A \sim B$) if $mA = vB$ for some $m \neq 0$ in $\mathbb{Z}$ and $v \neq 0$ in D.

(2) If $f = (a : k)$ is a quadratic form of discriminant Δ, then there is a corresponding ideal $A_f = [a : k]$ in the quadratic domain D_Δ.

(3) In the reverse direction, if $A = [a : k]$ is an ideal of D_Δ, then we can associate a quadratic form f_S of discriminant Δ to each *ordered basis* S of A. (The definition of f_S appears in Theorem 5.2.4. A $\mathbb{Z}$-basis $S = \{u, v\}$ for A is ordered if $\overline{u}v - u\overline{v} = N(A) \cdot \sqrt{\Delta}$.) A unimodular matrix converts one ordered basis for A into another, and the corresponding quadratic forms are all equivalent to $(a : k)$ (by the definition of equivalence of quadratic forms in Chapter 4).

(4) If f_S is the quadratic form of an ordered basis $S = \{u, v\}$ for some ideal A, and $w = mu+nv$ is written as a $\mathbb{Z}$-combination of S, then $N(w) = N(A) \cdot f_S(m, n)$.

(5) If $f = (a : k)$ is equivalent to $f_1 = (a_1 : k_1)$, then $A = [a : k]$ is equivalent to $A_1 = [a_1 : k_1]$. Specifically, if $f_1 = f \circ \begin{bmatrix} q & s \\ r & t \end{bmatrix}$, then $a_1 A = vA_1$, where $v = q(a) + r(k + z)$.

(6) Conversely, if $A = [a : k]$ is equivalent to $A_1 = [a_1 : k_1]$, then either $(a : k) \sim (a_1 : k_1)$ or $(a : k) \sim (-a_1 : k_1)$. (It is possible that both of these statements are true when the discriminant of these forms is positive.) Specifically, if a and a_1 are positive, and $mA = \upsilon A_1$ for some nonzero m in $\mathbb{Z}$ and nonzero υ in D, then $(a : k) \sim (a_1 : k_1)$ if $N(\upsilon)$ is positive, and $(a : k) \sim (-a_1 : k_1)$ if $N(\upsilon)$ is negative.

(7) There is an operation of composition, $f = f_1 \cdot f_2$, on primitive quadratic forms of a particular discriminant. This operation has the property that if $f_1(q, r) = m$ and $f_2(s, t) = n$, then $f(u, \upsilon) = mn$ for some pair of integers u and υ that can be calculated explicitly in terms of q, r, s, and t. Composition is essentially the same as ideal multiplication, when applied to quadratic forms in ideal notation.

(8) The set $\mathcal{C}_\Delta$ of classes (under equivalence as defined in this chapter) of ideals of a quadratic domain D_Δ having index 1 is well-defined. Ideal multiplication is a well-defined operation on this set, and $\mathcal{C}_\Delta$ has the properties of an abelian group under multiplication, which we call the *ideal class group* of discriminant Δ.

(9) Likewise, composition is a well-defined operation on the set $\mathcal{F}_\Delta$ of classes (under equivalence) of primitive quadratic forms of discriminant Δ, and $\mathcal{F}_\Delta$ has the structure of an abelian group, called the *form class group* of discriminant Δ, under composition.

(10) The number of elements in $\mathcal{F}_\Delta$ is either the same as or twice the number of elements in $\mathcal{C}_\Delta$, depending on whether or not D_Δ contains an element υ with $N(\upsilon) = -1$.

The structure of these class groups and their applications to representations of integers by quadratic forms will be our main consideration in the next two chapters for negative discriminants, and in Chapters 10 and 11 for positive discriminants.