Gauss's Composition Law and the Group of Binary Quadratic Forms

Sanjana Das

April 28, 2023

1 Introduction

A *binary quadratic form* over the integers is a function $f(x, y) = ax^2 + bxy + cy^2$ for integers a, b, and c. Gauss defined a *composition law* on binary quadratic forms, a ternary relation which gives a natural way of defining what it means for a binary quadratic form f to be a 'product,' or composition, of two binary quadratic forms f_1 and f_2. Gauss provided a complete characterization of when there exists a composition of two forms f_1 and f_2, and proved that composition possesses various nice properties. In particular, Gauss proved that the composition law provides a binary operator on *equivalence classes* of binary quadratic forms, and that this binary operator is associative; this allows one to use Gauss's composition law to place a group structure on equivalence classes of binary quadratic forms.

Gauss originally proved the properties of the composition law by directly using the equations used to define the composition law and equivalence of quadratic forms; these proofs are complicated and involve a lot of clever algebraic manipulation. Later, it has been realized that there is a natural correspondence between binary quadratic forms and ideals in quadratic number fields. It turns out that in this correspondence, Gauss's composition law corresponds to ideal multiplication; this can be used to provide more conceptual proofs of many of these properties.

In this paper, we will explain the correspondence between binary quadratic forms and ideals in quadratic number fields, and we will prove that multiplication of ideals provides a composition of the corresponding forms under Gauss's composition law. We will use this to prove that Gauss's composition law provides a group structure on equivalence classes of binary quadratic forms. We will then explain one application of this group structure, to *genus theory*. Genus theory classifies binary quadratic forms into classes, called *genera*, based on certain properties of the integers they represent. It turns out that these genera can be viewed in terms of a certain group homomorphism. We will explain this connection and use it to prove the principal genus theorem, which essentially characterizes when two quadratic forms are in the same genus based on Gauss's composition law. A more thorough description of these results is given in Subsection 1.3 (once the necessary terminology has been defined).

1.1 Basic Definitions

In this subsection, we will lay out a few basic definitions on binary quadratic forms, following [2, Chapter 1], which we will need in order to state and prove the main results described in the paper.

1.1.1 Discriminants

Definition 1.1. The *discriminant* of a binary quadratic form $f(x, y) = ax^2 + bxy + cy^2$ is $b^2 - 4ac$.

We usually denote the discriminant of a quadratic form by Δ. The importance of the discriminant arises from the fact that it appears when completing the square or factoring a quadratic form — if $f(x,y) = ax^2 + bxy + cy^2$ has discriminant Δ, then we can write

$$f(x,y) = a\left(x + \frac{b}{2a}y\right)^2 - \frac{\Delta}{4a}y^2 = a\left(x + \frac{b-\sqrt{\Delta}}{2a}y\right)\left(x + \frac{b-\sqrt{\Delta}}{2a}y\right). \tag{1}$$

In particular, the first equality in (1) implies that if $\Delta < 0$, then all integers represented by f have the same sign as a; we say that f is *positive definite* if all integers represented by f are positive, and *negative definite* if all integers represented by f are negative. Meanwhile, if $\Delta > 0$ then f represents integers of both signs.

Lemma 1.2. *There exists a binary quadratic form of discriminant Δ if and only if $\Delta \equiv 0$ or $1 \pmod 4$.*

Proof. First, if Δ is the discriminant of the quadratic form $f(x,y) = ax^2+bxy+cy^2$, then $\Delta = b^2-4ac \equiv b^2 \pmod 4$, so Δ must be 0 or 1 mod 4. Conversely, if $\Delta \equiv 0 \pmod 4$ then Δ is the discriminant of the form $x^2 - \frac{\Delta}{4}y^2$, while if $\Delta \equiv 1 \pmod 4$ then Δ is the discriminant of the form $x^2 + x - \frac{\Delta-1}{4}$. □

In this paper, we will primarily fix a non-square discriminant Δ, and work with only the forms of discriminant Δ. (When Δ is a square, $f(x,y)$ factors over the rationals, and in fact, over the integers as well; we will ignore this case.) In the case $\Delta < 0$, it will also generally be more convenient to only work with positive definite forms.

Notation 1.3. For a non-square integer $\Delta \equiv 0, 1 \pmod 4$, we use $\mathcal{F}_\Delta$ to denote the set of all binary quadratic forms of discriminant Δ if $\Delta > 0$, and the set of all positive definite binary quadratic forms of discriminant Δ if $\Delta < 0$.

1.1.2 Primitivity

Definition 1.4. A binary quadratic form $f(x,y) = ax^2 + bxy + cy^2$ is *primitive* if $\gcd(a,b,c) = 1$.

There is a straightforward characterization of primitivity in terms of which integers a form represents.

Lemma 1.5. *A binary quadratic form f is primitive if and only if for every prime p, f represents some integer not divisible by p.*

Proof. Let $f(x,y) = ax^2 + bxy + cy^2$. One direction is clear — if f is not primitive, then there exists a prime $p \mid \gcd(a,b,c)$, and all integers represented by f must be divisible by p.

For the reverse direction, suppose that f is primitive, and note that f represents a, c, and $a+b+c$, by taking (x,y) to be $(1,0)$, $(0,1)$, and $(1,1)$ respectively. Since $\gcd(a,c,a+b+c) = \gcd(a,b,c) = 1$, at least one of them must not be divisible by p. □

1.1.3 Equivalence of Quadratic Forms

It is useful to have a notion of what it means for two binary quadratic forms to be essentially the same; intuitively, two forms are equivalent if a suitable change of variables transforms one into the other.

Definition 1.6. Two binary quadratic forms f_1 and f_2 are *equivalent* if there exists a matrix $A \in \mathrm{SL}_2(\mathbb{Z})$ such that whenever $(x_2,y_2)^\intercal = A(x_1,y_1)^\intercal$, we have $f_2(x_2,y_2) = f_1(x_1,y_1)$. We write $f_1 \sim f_2$ to denote that f_1 and f_2 are equivalent, and $[f]$ to denote the equivalence class of f (i.e., the set of forms equivalent to f).

Example 1.7. The binary quadratic forms $f_1(x,y) = (2x+3y)^2 + 2(3x+5y)^2$ and $f_2(x,y) = x^2 + 2y^2$ are equivalent, as whenever

$$\begin{bmatrix} x_2 \\ y_2 \end{bmatrix} = \begin{bmatrix} 2 & 3 \\ 3 & 5 \end{bmatrix} \begin{bmatrix} x_1 \\ y_1 \end{bmatrix}$$

we have $f_2(x_2, y_2) = f_1(x_1, y_1)$, and the above matrix is in $\mathrm{SL}_2(\mathbb{Z})$ as its determinant is $2 \cdot 5 - 3 \cdot 3 = 1$.

It is clear from the definition that if $f_1 \sim f_2$, then f_1 and f_2 represent the same integers; in particular, by Lemma 1.5, this means f_1 is primitive if and only if f_2 is. It is also not hard to check that if $f_1 \sim f_2$, then f_1 and f_2 have the same discriminant.

Remark 1.8. It is perhaps not clear why the definition of equivalence should require that $A \in \mathrm{SL}_2(\mathbb{Z})$ rather than just that $A \in \mathrm{GL}_2(\mathbb{Z})$ (which would still be enough to ensure the above properties). However, it turns out that the restriction $A \in \mathrm{SL}_2(\mathbb{Z})$ really is important; without it, much of the theory in Section 2 would break.

1.2 Gauss's Composition Law

We will now define Gauss's composition law, following [4, Section 1].

Definition 1.9. Given two quadratic forms f_1 and f_2, we say that a quadratic form f is a *composition* of f_1 and f_2 if there exists a 2×4 integer matrix (p_{ij}), such that the greatest common divisor of the six 2×2 minors $p_{1i}p_{2j} - p_{2i}p_{1j}$ (over $1 \le i < j \le 4$) is 1 and such that the first two minors $p_{11}p_{21} - p_{21}p_{12}$ and $p_{11}p_{23} - p_{21}p_{13}$ are positive, for which

$$f_1(x_1, y_1) \cdot f_2(x_2, y_2) = f(x, y)$$

whenever x and y are the linear combinations of x_1x_2, x_1y_2, y_1x_2, and y_1y_2 given by

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} p_{11} & p_{12} & p_{13} & p_{14} \\ p_{21} & p_{22} & p_{23} & p_{24} \end{bmatrix} \begin{bmatrix} x_1x_2 \\ x_1y_2 \\ y_1x_2 \\ y_1y_2 \end{bmatrix}.$$

We refer to the matrix (p_{ij}) above as a *transformation matrix*. For convenience, we will use the following notation to refer to minors: if P is a $k \times \ell$ matrix with $k < \ell$, then for each subset $S \subseteq [\ell]$ of size k, we let P_S denote the submatrix of P consisting of all rows and the columns in S. Similarly, if P is a $k \times \ell$ matrix with $k > \ell$, then for each $S \subseteq [k]$ of size ℓ, we let P_S denote the submatrix of P consisting of the rows in S and all columns. Then the above conditions on the transformation matrix state that $\gcd(\det(P_{\{i,j\}})) = 1$ and that $\det(P_{\{1,2\}})$ and $\det(P_{\{1,3\}})$ are positive.

Example 1.10. For any integer d, the form $f(x,y) = x^2 - dy^2$ is a composition of $f_1(x,y) = x^2 - dy^2$ and $f_2(x,y) = x^2 - dy^2$ — we have the formula

$$(x_1^2 - dy_1^2)(x_2^2 - dy_2^2) = (x_1x_2 + dy_1y_2)^2 - d(x_1y_2 + y_1x_2)^2,$$

which states that $f_1(x_1, y_1) \cdot f_2(x_2, y_2) = f(x, y)$ whenever

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & d \\ 0 & 1 & 1 & 0 \end{bmatrix} \begin{bmatrix} x_1x_2 \\ x_1y_2 \\ y_1x_2 \\ y_1y_2 \end{bmatrix}.$$

The transformation matrix here is valid as its minors are 1, 1, 0, 0, $-d$, and $-d$; these have greatest common divisor 1, and the first two minors (1 and 1) are both positive.

Although the definition of the composition law may seem somewhat complicated, it is in some sense a natural way to define a product structure on quadratic forms, since if f_1 represents some integer r_1 and f_2 represents some integer r_2, then any composition f of f_1 and f_2 represents $r_1 r_2$.

Note that composition of quadratic forms is a *ternary relation* rather than a binary operation — given two quadratic forms f_1 and f_2, there may not exist any composition of f_1 and f_2, or there may exist many compositions. Gauss proved the following characterization of when there does exist a composition of two forms f_1 and f_2.

Theorem 1.11. *Given two binary quadratic forms f_1 and f_2, there exists a composition f of f_1 and f_2 if and only if the ratio of the discriminants of f_1 and f_2 is a rational square. In that case, the ratio of the discriminant of f and either discriminant is a rational square as well.*

We will not prove the necessity of this condition; a proof is given in [2, Section 7.2]. However, in Subsection 2.4, we will provide a method of composing two forms that have the *same* discriminant. This implies that it is possible to compose any two forms whose ratio of discriminants is a rational square — we may scale both forms to have the same discriminant, compose these scaled forms, and then scale the composition back — thus showing that the condition is sufficient.

Gauss also showed that if two forms f_1 and f_2 may be composed, then the set of their compositions forms an entire equivalence class.

Theorem 1.12. *Given two binary quadratic forms f_1 and f_2 with composition f, a form f' is a composition of f_1 and f_2 if and only if $f' \sim f$.*

In light of this theorem, we will write $[f_1 \cdot f_2]$ to denote the equivalence class of compositions of f_1 and f_2, and we will write $f \sim f_1 \cdot f_2$ to denote that f is a composition of f_1 and f_2.

The results in Section 2 will imply one direction of the above theorem, that if f is a composition of f_1 and f_2, then any form equivalent to f is a composition of f_1 and f_2 as well. We will not prove the reverse direction; [2, Chapter 7.2] contains a proof of both statements (using somewhat involved calculations with matrices).

1.3 Overview of Results

With these definitions, we are now in a position to more precisely describe the results mentioned in the beginning of Section 1 that we will see in this paper.

In Subsection 2.2 we will see a way to associate quadratic forms in $\mathcal{F}_\Delta$ to ideals of the order of discriminant Δ in the quadratic number field $\mathbb{Q}(\sqrt{\Delta})$ (which we will define in Subsection 2.1), and in Subsection 2.3 we will show that this correspondence produces a bijection between equivalence classes of forms and narrow equivalence classes of ideals. In Subsection 2.4 we will show that in this bijection, Gauss's composition law corresponds to the multiplication of ideals. Using these results, in Subsection 2.5 we will be able to deduce two theorems proved by Gauss (via different methods) regarding the composition law. The first is that compositions of equivalent forms are equivalent (under certain conditions), which will imply that composition provides a well-defined binary operation on *equivalence classes* of quadratic forms in $\mathcal{F}_\Delta$. The second is that this binary operation is associative. We will see that this implies the equivalence classes of *primitive* quadratic forms in $\mathcal{F}_\Delta$ form a group under composition, which we will denote by $\mathrm{Cl}(\mathcal{F}_\Delta)$.

In Section 3, we will see the connection between the group $\mathrm{Cl}(\mathcal{F}_\Delta)$ and genus theory (in the case where Δ is odd and squarefree). In Subsection 3.1 we will define the genus of a quadratic form, and we will see that the genera can be viewed as cosets in the group $\mathrm{Cl}(\mathcal{F}_\Delta)$. In Subsection 3.2 we will state and prove the principal genus theorem, which states that the principal genus (the genus of the identity of $\mathrm{Cl}(\mathcal{F}_\Delta)$) consists precisely of the squares of forms (under Gauss's composition law).

2 Connection to Quadratic Number Fields

In this section, we will describe a connection between binary quadratic forms and ideals in quadratic number fields, and see how this connection can be used to obtain conceptually simple proofs of many of the nice properties of Gauss's composition law.

2.1 Preliminaries

In this subsection, we will state the necessary definitions and results on quadratic number fields and orders which we will need in order to establish the connection with quadratic forms, following [3, Chapter 4]. We will state these definitions and results specifically for the fields and orders relevant to this connection, but most of them are part of a more general theory described in [3, Chapter 4].

We will always assume that the ideals referred to are nonzero.

Notation 2.1. For any $\alpha_1, \ldots, \alpha_n$, we use $\langle \alpha_1, \ldots, \alpha_n \rangle$ to denote the set of $\mathbb{Z}$-linear combinations of $\alpha_1, \ldots, \alpha_n$, or in other words $\langle \alpha_1, \ldots, \alpha_n \rangle = \{c_1\alpha_1 + \cdots + c_n\alpha_n \mid c_i \in \mathbb{Z}\}$.

For a non-square integer $\Delta \equiv 0, 1 \pmod 4$, the *quadratic number field* $\mathbb{Q}(\sqrt{\Delta})$ is the field obtained by adjoining $\sqrt{\Delta}$ to $\mathbb{Q}$ (which consists of $\mathbb{Q}$-linear combinations of 1 and $\sqrt{\Delta}$). The *order* of discriminant Δ in $\mathbb{Q}(\sqrt{\Delta})$, which we denote by $\mathcal{O}_\Delta$, is defined as $\mathcal{O}_\Delta = \langle 1, \frac{\Delta+\sqrt{\Delta}}{2} \rangle$. Note that $\mathcal{O}_\Delta$ is a subring of $\mathbb{Q}(\sqrt{\Delta})$ (as it can be checked to be closed under multiplication).

An *ideal* of $\mathcal{O}_\Delta$ is a subset $\mathfrak{a} \subseteq \mathcal{O}_\Delta$ which is closed under addition and is also closed under multiplication by any element of $\mathcal{O}_\Delta$. An ideal $\mathfrak{a}$ is *principal* if $\mathfrak{a} = \alpha\mathcal{O}_\Delta$ for some $\alpha \in \mathcal{O}_\Delta$ (i.e., it is generated as an ideal by one element). (These are the usual definitions of ideals and principal ideals in a ring.) A *fractional ideal* of $\mathcal{O}_\Delta$ is a subset of $\mathbb{Q}(\sqrt{\Delta})$ which is of the form $\gamma\mathfrak{a}$ for some ideal $\mathfrak{a}$ of $\mathcal{O}_\Delta$ and some $\gamma \in \mathbb{Q}(\sqrt{\Delta})$; we say such a fractional ideal is principal if $\mathfrak{a}$ is principal.

The field $\mathbb{Q}(\sqrt{\Delta})$ comes with the natural automorphism that fixes $\mathbb{Q}$ and sends $\sqrt{\Delta} \mapsto -\sqrt{\Delta}$. We denote this automorphism as $x \mapsto \overline{x}$ (note that the map $x \mapsto \overline{x}$ coincides with complex conjugation if $\Delta < 0$, but not if $\Delta > 0$).

Definition 2.2. The *norm* of an element $\gamma \in \mathbb{Q}(\sqrt{\Delta})$ is defined as $n(\gamma) = \gamma\overline{\gamma}$.

If $\gamma = a + b\sqrt{\Delta}$ for $a, b \in \mathbb{Q}$, then $n(\gamma) = a^2 - \Delta b^2$. In particular, if $\Delta < 0$ then $n(\gamma) > 0$ for all nonzero γ, but if $\Delta > 0$ then $n(\gamma)$ may be positive or negative (it cannot be zero as Δ is not a square).

Note that the norm is multiplicative, i.e., $n(\alpha\beta) = n(\alpha)n(\beta)$. (This follows from the fact that $\overline{\alpha \cdot \beta} = \overline{\alpha} \cdot \overline{\beta}$.)

2.1.1 Lattices and Ideal Norms

The order $\mathcal{O}_\Delta$ is a 2-dimensional lattice — it is a free rank-2 $\mathbb{Z}$-module with generators 1 and $\frac{\Delta+\sqrt{\Delta}}{2}$. The theory of $\mathbb{Z}$-modules in [3, Chapter 2.4] (together with the fact that any ideal is closed under multiplication by $\frac{\Delta+\sqrt{\Delta}}{2}$) implies that any fractional ideal $\mathfrak{a}$ is a 2-dimensional lattice as well. We will use this to define the norm of a fractional ideal. In order to do this, we will need the following fact, which we state without proof.

Lemma 2.3. *If L_1 and L_2 are 2-dimensional lattices and L and L' are 2-dimensional lattices each containing both L_1 and L_2, then*

$$\frac{[L : L_1]}{[L : L_2]} = \frac{[L' : L_1]}{[L' : L_2]}.$$

This allows us to define the norm of a fractional ideal in the following way.

Definition 2.4. Given a fractional ideal $\mathfrak{a}$ of $\mathcal{O}_\Delta$, the *norm* of $\mathfrak{a}$ is defined as

$$\mathcal{N}(\mathfrak{a}) = \frac{[L : \mathfrak{a}]}{[L : \mathcal{O}_\Delta]}$$

where L is any lattice containing both $\mathfrak{a}$ and $\mathcal{O}_\Delta$.

In particular, if $\mathfrak{a}$ is a non-fractional ideal of $\mathcal{O}_\Delta$, then $\mathcal{N}(\mathfrak{a})$ is simply $[\mathcal{O}_\Delta : \mathfrak{a}]$.

Note that if $\mathfrak{a} = \langle \alpha, \beta \rangle$ and A is the rational matrix such that $(\alpha, \beta) = A(1, \frac{\Delta+\sqrt{\Delta}}{2})$, then $\mathcal{N}(\mathfrak{a}) = |\det(A)|$. It will often be useful to understand the determinant of such a matrix without explicitly computing the matrix itself; the following lemma allows us to do so.

Lemma 2.5. *If $\alpha, \beta, \alpha', \beta' \in \mathbb{Q}(\sqrt{\Delta})$ are such that $(\alpha', \beta') = (\alpha, \beta)A$ for some matrix $A \in \mathrm{GL}_2(\mathbb{Q})$, then*

$$\alpha'\overline{\beta'} - \overline{\alpha'}\beta' = \det(A)(\alpha\overline{\beta} - \overline{\alpha}\beta).$$

This can be verified by direct computation; we will omit the proof here.

Corollary 2.6. *If $\mathfrak{a} = \langle \alpha, \beta \rangle$ is an ideal of $\mathcal{O}_\Delta$, then*

$$\mathcal{N}(\mathfrak{a}) = \left| \frac{\alpha\overline{\beta} - \overline{\alpha}\beta}{\sqrt{\Delta}} \right|.$$

Proof. Letting $A \in \mathrm{GL}_2(\mathbb{Q})$ be the matrix such that $(\alpha, \beta) = A(1, \frac{\Delta+\sqrt{\Delta}}{2})$, we have

$$\mathcal{N}(\mathfrak{a}) = |\det(A)| = \left| \frac{\alpha\overline{\beta} - \overline{\alpha}\beta}{1 \cdot \overline{\frac{\Delta+\sqrt{\Delta}}{2}} - \overline{1} \cdot \frac{\Delta+\sqrt{\Delta}}{2}} \right| = \left| \frac{\alpha\overline{\beta} - \overline{\alpha}\beta}{\sqrt{\Delta}} \right|. \qquad \square$$

Corollary 2.7. *If $\gamma \in \mathbb{Q}(\sqrt{\Delta})$ and $\mathfrak{a}$ and $\gamma\mathfrak{a}$ are both ideals of $\mathcal{O}_\Delta$, then $\mathcal{N}(\gamma\mathfrak{a}) = |n(\gamma)|\,\mathcal{N}(\mathfrak{a})$.*

Proof. Let $\mathfrak{a} = \langle \alpha, \beta \rangle$, so that $\gamma\mathfrak{a} = \langle \gamma\alpha, \gamma\beta \rangle$. Then

$$\mathcal{N}(\gamma\mathfrak{a}) = \left| \frac{\gamma\alpha\overline{\gamma\beta} - \overline{\gamma\alpha}\gamma\beta}{\sqrt{\Delta}} \right| = |\gamma\overline{\gamma}| \left| \frac{\alpha\overline{\beta} - \overline{\alpha}\beta}{\sqrt{\Delta}} \right| = |n(\gamma)|\,\mathcal{N}(\mathfrak{a}). \qquad \square$$

This provides a useful observation relating the norm of an ideal to the norms of its elements.

Lemma 2.8. *If $\mathfrak{a}$ is a fractional ideal of $\mathcal{O}_\Delta$ and $\gamma \in \mathfrak{a}$, then $\mathcal{N}(\mathfrak{a})$ divides $n(\gamma)$, i.e., $n(\gamma)$ is an integer multiple of $\mathcal{N}(\mathfrak{a})$.*

Proof. Consider the fractional ideal $\gamma^{-1}\mathfrak{a}$. This ideal contains 1, and therefore contains $\mathcal{O}_\Delta$, so

$$\mathcal{N}(\gamma^{-1}\mathfrak{a}) = \frac{[\gamma^{-1}\mathfrak{a} : \gamma^{-1}\mathfrak{a}]}{[\gamma^{-1}\mathfrak{a} : \mathcal{O}_\Delta]} = \frac{1}{[\gamma^{-1}\mathfrak{a} : \mathcal{O}_\Delta]},$$

which is the reciprocal of an integer. But $\mathcal{N}(\gamma^{-1}\mathfrak{a}) = |n(\gamma)|^{-1}\mathcal{N}(\mathfrak{a})$, which gives the desired result. $\square$

2.1.2 Ideal Multiplication

Definition 2.9. Given two fractional ideals $\mathfrak{a}$ and $\mathfrak{b}$ of $\mathcal{O}_\Delta$, their *product* $\mathfrak{ab}$ is the set of finite sums of elements $\alpha\beta$ for $\alpha \in \mathfrak{a}$ and $\beta \in \mathfrak{b}$.

Note that $\mathfrak{ab}$ is a fractional ideal of $\mathcal{O}_\Delta$ as well (the fact that it is closed under multiplication by $\frac{\Delta+\sqrt{\Delta}}{2}$ follows directly from the fact that $\mathfrak{a}$ and $\mathfrak{b}$ are).

Definition 2.10. A fractional ideal $\mathfrak{a}$ is *invertible* if there exists a fractional ideal $\mathfrak{b}$ such that $\mathfrak{ab} = \mathcal{O}_\Delta$; if so, we say that $\mathfrak{b}$ is an *inverse* of $\mathfrak{a}$.

It is shown in [3, Lemma 4.6.7] that if $\mathfrak{a}$ is invertible, then its inverse is unique; so we may refer to *the* inverse of $\mathfrak{a}$, which we denote $\mathfrak{a}^{-1}$.

We will make use of the following two results about invertible ideals.

Lemma 2.11 ([3, Proposition 4.6.8])**.** *If $\mathfrak{a}$ and $\mathfrak{b}$ are fractional ideals of $\mathcal{O}_\Delta$ such that at least one is invertible, then $\mathcal{N}(\mathfrak{ab}) = \mathcal{N}(\mathfrak{a})\mathcal{N}(\mathfrak{b})$.*

Lemma 2.12 ([3, Proposition 5.2.5])**.** *A fractional ideal $\mathfrak{a} = \langle \alpha, \beta \rangle$ is invertible if and only if $\mathcal{N}(\mathfrak{a}) = \gcd(\alpha\overline{\alpha}, \beta\overline{\beta}, \alpha\overline{\beta} + \overline{\alpha}\beta)$. In that case, $\mathfrak{a}^{-1} = \mathcal{N}(\mathfrak{a})^{-1}\overline{\mathfrak{a}}$.*

Remark 2.13. If Δ is a *fundamental* discriminant, meaning that Δ cannot be written as $d^2\Delta'$ where $d > 1$ is an integer and Δ' is also a valid discriminant (i.e., is 0 or 1 mod 4), then every fractional ideal in $\mathcal{O}_\Delta$ is invertible (a proof is given in [3, Chapter 4.6.2]), so the above results hold for all fractional ideals in $\mathcal{O}_\Delta$. However, when Δ is not a fundamental discriminant, there do exist non-invertible ideals; details can be found in [3, Chapter 4.6.1].

2.1.3 Equivalence of Ideals and the Narrow Class Group

Definition 2.14. Two fractional ideals $\mathfrak{a}$ and $\mathfrak{b}$ are *narrowly equivalent* if there exists $\gamma \in \mathbb{Q}(\sqrt{\Delta})$ with $n(\gamma) > 0$ such that $\mathfrak{a} = \gamma\mathfrak{b}$. We write $\mathfrak{a} \sim \mathfrak{b}$ to denote that $\mathfrak{a}$ is equivalent to $\mathfrak{b}$, and $[\mathfrak{a}]$ to denote the equivalence class of $\mathfrak{a}$.

Ideal multiplication is clearly a well-defined operation on narrow equivalence classes of ideals. Note also that if $\mathfrak{a}$ is invertible, then all ideals narrowly equivalent to $\mathfrak{a}$ are also invertible. Since ideal multiplication is clearly associative, it then defines a group structure on the set of narrow equivalence classes of *invertible* ideals; we will use $\mathrm{Cl}^+(\mathcal{O}_\Delta)$ to denote this group. The identity element of $\mathrm{Cl}^+(\mathcal{O}_\Delta)$ is $[\mathcal{O}_\Delta]$ (since $\mathfrak{a}\mathcal{O}_\Delta = \mathfrak{a}$ for any fractional ideal $\mathfrak{a}$), and by Lemma 2.12 the inverse of $[\mathfrak{a}]$ is $[\overline{\mathfrak{a}}]$.

2.2 Correspondence Between Quadratic Forms and Ideals

We begin by describing a way to associate fractional ideals of $\mathcal{O}_\Delta$ to quadratic forms in $\mathcal{F}_\Delta$ and vice versa. Neither direction of this construction is uniquely defined — an ideal may correspond to many quadratic forms, and a quadratic form to many ideals — but we will see in Subsection 2.3 that it produces a well-defined bijection between their *equivalence classes* (more precisely, between the narrow equivalence classes of fractional ideals of $\mathcal{O}_\Delta$ and the equivalence classes of quadratic forms in $\mathcal{F}_\Delta$).

Given a fractional ideal $\mathfrak{a}$ of $\mathcal{O}_\Delta$, choose a $\mathbb{Z}$-basis $\mathfrak{a} = \langle \alpha, \beta \rangle$ such that $\alpha\overline{\beta} - \overline{\alpha}\beta > 0$. We then define the associated quadratic form

$$f(x, y) = \frac{(\alpha x + \beta y)(\overline{\alpha}x + \overline{\beta}y)}{\mathcal{N}(\mathfrak{a})}.$$

Note that this construction depends not only on $\mathfrak{a}$ but also on the choice of $\mathbb{Z}$-basis.

To check that $f \in \mathcal{F}_\Delta$, first f has integer coefficients by Lemma 2.8 (note that $\alpha\overline{\beta}+\overline{\alpha}\beta = n(\alpha+\beta)-n(\alpha)-n(\beta)$, so since the lemma implies that $n(\alpha)$, $n(\beta)$, and $n(\alpha+\beta)$ are all divisible by $\mathcal{N}(\mathfrak{a})$, then so are all three coefficients). In fact, by Lemma 2.12, f is primitive if and only if $\mathfrak{a}$ is invertible.

The discriminant of f is

$$\frac{(\alpha\overline{\beta}+\overline{\alpha}\beta)^2 - 4\alpha\overline{\alpha}\beta\overline{\beta}}{\mathcal{N}(\mathfrak{a})^2} = \frac{(\alpha\overline{\beta}-\overline{\alpha}\beta)^2}{\mathcal{N}(\mathfrak{a})^2} = \Delta$$

by Corollary 2.6. Finally, if $\Delta < 0$ then $\alpha\overline{\alpha} > 0$ for all x and y, so f is positive definite. So f is indeed a binary quadratic form in $\mathcal{F}_\Delta$. Let $\mathcal{F}(\mathfrak{a})$ be the set of quadratic forms which can be obtained from $\mathfrak{a}$ in this way (over all choices of $\mathbb{Z}$-basis).

To reverse this construction, we will use the following lemma.

Lemma 2.15. *If f is a quadratic form of discriminant Δ and α and β are elements of $\mathbb{Q}(\sqrt{\Delta})$ such that $f(-\beta,\alpha) = 0$, then $\langle\alpha,\beta\rangle$ is a fractional ideal of $\mathcal{O}_\Delta$.*

Proof. It suffices to check that $\langle\alpha,\beta\rangle$ is closed under multiplication by elements of $\mathcal{O}_\Delta$, or equivalently that $\alpha\mathcal{O}_\Delta$ and $\beta\mathcal{O}_\Delta$ are subsets of $\langle\alpha,\beta\rangle$. To prove this for α, note that $-\frac{\beta}{\alpha}$ is a root of the polynomial $at^2+bt+c=0$, which means

$$-\frac{\beta}{\alpha} = \frac{-b\pm\sqrt{\Delta}}{2a}.$$

Since $\mathcal{O}_\Delta$ has $\mathbb{Z}$-basis $\langle 1, \frac{\Delta+\sqrt{\Delta}}{2}\rangle$ and $b \equiv \Delta \pmod 2$, then $\mathcal{O}_\Delta$ also has $\mathbb{Z}$-basis $\langle 1, -\frac{a\beta}{\alpha}\rangle$; but then it is clear that $\alpha\mathcal{O}_\Delta = \langle\alpha, -a\beta\rangle \subseteq \langle\alpha,\beta\rangle$. The proof that $\beta\mathcal{O}_\Delta \subseteq \langle\alpha,\beta\rangle$ is analogous. □

Now given a quadratic form $f(x,y) = ax^2+bxy+cy^2$ in $\mathcal{F}_\Delta$, we can find α and β in $\mathbb{Q}(\sqrt{\Delta})$ such that the following three conditions hold:

- $n(\alpha)$ has the same sign as a,
- $\alpha\overline{\beta}-\overline{\alpha}\beta > 0$, and
- $f(-\beta,\alpha) = 0$.

Call such a pair (α,β) a *factoring pair* of f. (One way of obtaining such a pair is as follows: first, choose α arbitrarily such that $n(\alpha)$ has the same sign as a — this is always possible because if $\Delta<0$ then $\mathcal{F}_\Delta$ only consists of quadratic forms with $a>0$, while if $\Delta>0$ then there exist $\alpha\in\mathbb{Q}(\sqrt{\Delta})$ with $n(\alpha)$ of either sign. Then since the roots of the polynomial $at^2+bt+c=0$ lie in $\mathbb{Q}(\sqrt{\Delta})$ and are conjugates (i.e., if r is a root then so is $\overline{r}$), we can find $\beta\in\mathbb{Q}(\sqrt{\Delta})$ such that $f(-\beta,\alpha) = f(-\overline{\beta},\overline{\alpha}) = 0$. Then exactly one of (α,β) and $(\overline{\alpha},\overline{\beta})$ satisfies the second condition, and this choice is a factoring pair.)

By Lemma 2.15, then $\mathfrak{a} = \langle\alpha,\beta\rangle$ is an ideal of $\mathcal{O}_\Delta$, which we define as the ideal associated to f. Note that this construction again depends on the choice of α and β; let $\mathcal{I}(f)$ be the set of fractional ideals which can be obtained from f in this way.

These two constructions are 'inverses' of each other — given a fractional ideal $\mathfrak{a}$, if the $\mathbb{Z}$-basis $\langle\alpha,\beta\rangle$ produces the quadratic form

$$f(x,y) = \frac{(\alpha x+\beta y)(\overline{\alpha}x+\overline{\beta}y)}{\mathcal{N}(\mathfrak{a})},$$

then it is clear that (α,β) is a factoring pair of f, which returns the fractional ideal $\mathfrak{a}$ (the sign condition on $n(\alpha)$ follows from $\mathcal{N}(\mathfrak{a})>0$). Meanwhile, given a form $f\in\mathcal{F}_\Delta$ and a factoring pair (α,β) producing the fractional ideal $\mathfrak{a}$, we know f must factor as

$$f(x,y) = \frac{(\alpha x+\beta y)(\overline{\alpha}x+\overline{\beta}y)}{\gamma}$$

for some $\gamma \in \mathbb{Q}$ (since if one root of $at^2 + bt + c$ is $-\frac{\beta}{\alpha}$, the other is its conjugate). Then since f has discriminant Δ, we must have

$$\Delta = \frac{(\alpha\overline{\beta} + \overline{\alpha}\beta)^2 - 4\alpha\overline{\alpha}\beta\overline{\beta}}{\gamma^2} = \frac{(\alpha\overline{\beta} - \overline{\alpha}\beta)^2}{\gamma^2} = \frac{\mathcal{N}(\mathfrak{a})^2 \cdot \Delta}{\gamma^2},$$

which implies that $\gamma = \pm\mathcal{N}(\mathfrak{a})$. Then the fact that $\alpha\overline{\alpha}$ has the same sign as the x^2–coefficient of f requires that $\gamma = \mathcal{N}(\mathfrak{a})$, so we in fact have

$$f(x, y) = \frac{(\alpha x + \beta y)(\overline{\alpha}x + \overline{\beta}y)}{\mathcal{N}(\mathfrak{a})},$$

which is the quadratic form produced from $\mathfrak{a}$ under the $\mathbb{Z}$-basis $\langle\alpha, \beta\rangle$.

2.3 Correspondence Between Equivalence Classes of Quadratic Forms and Ideals

We will now check that the correspondence given in Subsection 2.2 provides a bijection between equivalence classes of quadratic forms and narrow equivalence classes of fractional ideals.

Proposition 2.16. *For any quadratic form $f \in \mathcal{F}_\Delta$ and corresponding fractional ideal $\mathfrak{a} \in \mathcal{I}(f)$, we have $\mathfrak{a}' \in \mathcal{I}(f)$ if and only if $\mathfrak{a}'$ is narrowly equivalent to $\mathfrak{a}$.*

Proof. Let $\mathfrak{a} = \langle\alpha, \beta\rangle$ be produced from the factoring pair (α, β) of f. First, if $\mathfrak{a}'$ is narrowly equivalent to $\mathfrak{a}$, then by definition we can write $\mathfrak{a}' = \gamma\mathfrak{a} = \langle\gamma\alpha, \gamma\beta\rangle$ for some $\gamma \in \mathbb{Q}(\sqrt{\Delta})$ with $n(\gamma) > 0$. Then $(\gamma\alpha, \gamma\beta)$ is a factoring pair of f as well — multiplying (α, β) by γ multiplies both $\alpha\overline{\alpha}$ and $\alpha\overline{\beta} - \overline{\alpha}\beta$ by $n(\gamma) > 0$, so it preserves their signs. So $\mathfrak{a}' \in \mathcal{I}(f)$ as well.

To prove the converse, suppose that (α', β') is another factoring pair of f; we will show that $(\alpha', \beta') = (\gamma\alpha, \gamma\beta)$ for some γ with $n(\gamma) > 0$. First note that $-\frac{\beta}{\alpha}$ and $-\frac{\beta'}{\alpha'}$ are both roots of the integer-coefficient polynomial $at^2 + bt + c$, so they must be equal or conjugate.

First we claim that they cannot be conjugate. Suppose that they are, so $\beta = r\alpha$ and $\beta' = \overline{r}\alpha'$ for some $r \in \mathbb{Q}(\sqrt{\Delta}) \setminus \mathbb{Q}$. Then we have

$$\alpha\overline{\beta} - \overline{\alpha}\beta = \alpha\overline{r}\overline{\alpha} - \overline{\alpha}r\alpha = (\overline{r} - r)n(\alpha),$$

and similarly

$$\alpha'\overline{\beta'} - \overline{\alpha'}\beta' = (r - \overline{r})n(\alpha').$$

But $n(\alpha)$ and $n(\alpha')$ must have the same sign (as both have the same sign as the x^2–coefficient of f), so the right-hand sides of these two expressions have opposite sign; but the left-hand sides are both positive, contradiction.

So $-\frac{\beta}{\alpha}$ and $-\frac{\beta'}{\alpha'}$ are equal. Then we can let $\gamma = \frac{\alpha'}{\alpha} = \frac{\beta}{\beta'}$; since $n(\alpha)$ and $n(\alpha')$ must have the same sign as the x^2–coefficient of a, we have $n(\gamma) > 0$. So $\mathfrak{a}'$ is indeed narrowly equivalent to $\mathfrak{a}$. □

Proposition 2.17. *For any fractional ideal $\mathfrak{a}$ of $\mathcal{O}_\Delta$ and corresponding quadratic form $f \in \mathcal{F}(\mathfrak{a})$, we have $f' \in \mathcal{F}(\mathfrak{a})$ if and only if f' is equivalent to f.*

Proof. Let f be produced from the $\mathbb{Z}$-basis $\langle\alpha, \beta\rangle$ of $\mathfrak{a}$, so

$$f(x, y) = \frac{(\alpha x + \beta y)(\overline{\alpha}x + \overline{\beta}y)}{\mathcal{N}(\mathfrak{a})}.$$

First we will show that if f' is equivalent to f, then $f' \in \mathcal{F}(\mathfrak{a})$ as well. Since f' is equivalent to f, there exists a matrix $A \in \mathrm{SL}_2(\mathbb{Z})$ such that whenever $(x,y)^\intercal = A(x',y')^\intercal$ we have $f(x',y') = f(x,y)$. Now define α' and β' so that

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

Since $A \in \mathrm{SL}_2(\mathbb{Z})$, then (α', β') is a $\mathbb{Z}$-basis of $\mathfrak{a}$ as well, and $\alpha'\overline{\beta'} - \overline{\alpha'}\beta' = \alpha\overline{\beta} - \overline{\alpha}\beta > 0$. Meanwhile, for all x' and y', if we define (x,y) so that $(x,y)^\intercal = A(x',y')^\intercal$, we then have

$$\alpha'x' + \beta'y' = \begin{bmatrix}\alpha' & \beta'\end{bmatrix}\begin{bmatrix}x'\\y'\end{bmatrix} = \begin{bmatrix}\alpha & \beta\end{bmatrix} \cdot A \cdot \begin{bmatrix}x'\\y'\end{bmatrix} = \begin{bmatrix}\alpha & \beta\end{bmatrix}\begin{bmatrix}x\\y\end{bmatrix} = \alpha x + \beta y,$$

and taking conjugates gives $\overline{\alpha'}x' + \overline{\beta'}y' = \overline{\alpha}x + \overline{\beta}y$ as well, so we have

$$\frac{(\alpha'x' + \beta'y')(\overline{\alpha'}x' + \overline{\beta'}y')}{\mathcal{N}(\mathfrak{a})} = \frac{(\alpha x + \beta y)(\overline{\alpha}x + \overline{\beta}y)}{\mathcal{N}(\mathfrak{a})} = f(x,y) = f'(x',y').$$

Since this is true for all x' and y' (for the corresponding values of x and y), then f' must equal the above polynomial, so $\langle \alpha', \beta' \rangle$ is a $\mathbb{Z}$-basis of $\mathfrak{a}$ producing f'.

To prove the converse, we can essentially run the same argument in reverse — suppose that $f' \in \mathcal{F}(\mathfrak{a})$ is produced by the $\mathbb{Z}$-basis $\langle \alpha', \beta' \rangle$. Then there exists a change of basis matrix $A \in \mathrm{SL}_2(\mathbb{Z})$ such that

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

and A provides a transformation between f and f' in the same way as above. □

Propositions 2.16 and 2.17 together imply that the correspondence in Subsection 2.2 provides a bijection between the equivalence classes of quadratic forms in $\mathcal{F}_\Delta$ and narrow equivalence classes of fractional ideals of $\mathcal{O}_\Delta$. Furthermore, if this bijection links the classes $[f]$ and $[\mathfrak{a}]$, then every quadratic form in $[f]$ corresponds to every fractional ideal in $[\mathfrak{a}]$, and vice versa.

2.4 Gauss's Composition Law in Terms of Ideal Multiplication

We will now describe how to compose two forms in terms of multiplying their corresponding ideals.

Theorem 2.18. *Let f_1 and f_2 be quadratic forms in $\mathcal{F}_\Delta$ with* positive x^2*–coefficient, and let $\mathfrak{a}_1 \in \mathcal{I}(f_1)$ and $\mathfrak{a}_2 \in \mathcal{I}(f_2)$ be any two ideals corresponding to f_1 and f_2. Let $\mathfrak{a} = \mathfrak{a}_1\mathfrak{a}_2$. Then any quadratic form f for which*

$$f \cdot \frac{\mathcal{N}(\mathfrak{a}_1)\mathcal{N}(\mathfrak{a}_2)}{\mathcal{N}(\mathfrak{a})} \in \mathcal{F}(\mathfrak{a})$$

is a composition of f_1 and f_2.

Note that by one direction of Theorem 1.12 all compositions of f_1 and f_2 are equivalent; since $\mathcal{F}(\mathfrak{a})$ is an equivalence class of quadratic forms, then *all* compositions of f_1 and f_2 can be obtained in this way. This theorem actually proves the other direction of Theorem 1.12, since if f is in $\mathcal{F}(\mathfrak{a})$ then so is every quadratic form f' equivalent to f (by Proposition 2.17).

Proof. Let f_1, f_2, and $f \cdot \frac{\mathcal{N}(\mathfrak{a}_1)\mathcal{N}(\mathfrak{a}_2)}{\mathcal{N}(\mathfrak{a})}$ correspond to $\mathfrak{a}_1$, $\mathfrak{a}_2$, and $\mathfrak{a}$ through (α_1, β_1), (α_2, β_2), and (α, β) respectively (so these pairs are factoring pairs of their corresponding forms and $\mathbb{Z}$-bases of their corresponding

ideals), so that we have

$$f_1(x,y) = \frac{(\alpha_1 x + \beta_1 y)(\overline{\alpha_1} x + \overline{\beta_1} y)}{\mathcal{N}(\mathfrak{a}_1)}$$
$$f_2(x,y) = \frac{(\alpha_2 x + \beta_2 y)(\overline{\alpha_2} x + \overline{\beta_2} y)}{\mathcal{N}(\mathfrak{a}_2)}$$
$$f(x,y) = \frac{(\alpha x + \beta y)(\overline{\alpha} x + \overline{\beta} y)}{\mathcal{N}(\mathfrak{a}_1)\mathcal{N}(\mathfrak{a}_2)}.$$

Since $\mathfrak{a} = \mathfrak{a}_1\mathfrak{a}_2$ can be written as both $\langle \alpha, \beta \rangle$ and $\langle \alpha_1\alpha_2, \alpha_1\beta_2, \beta_1\alpha_2, \beta_1\beta_2 \rangle$, there exists a 2×4 integer matrix P such that

$$\begin{bmatrix} \alpha_1\alpha_2 & \alpha_1\beta_2 & \beta_1\alpha_2 & \beta_1\beta_2 \end{bmatrix} = \begin{bmatrix} \alpha & \beta \end{bmatrix} \cdot P$$

(obtained by writing each of $\alpha_1\alpha_2$, $\alpha_1\beta_2$, $\beta_1\alpha_2$, and $\beta_1\beta_2$ as a $\mathbb{Z}$-linear combination of α and β), as well as a 4×2 integer matrix Q such that

$$\begin{bmatrix} \alpha & \beta \end{bmatrix} = \begin{bmatrix} \alpha_1\alpha_2 & \alpha_1\beta_2 & \beta_1\alpha_2 & \beta_1\beta_2 \end{bmatrix} \cdot Q$$

(obtained by writing α and β as $\mathbb{Z}$-linear combinations of $\alpha_1\alpha_2$, $\alpha_1\beta_2$, $\beta_1\alpha_2$, and $\beta_1\beta_2$). Together, these imply that

$$\begin{bmatrix} \alpha & \beta \end{bmatrix} = \begin{bmatrix} \alpha & \beta \end{bmatrix} \cdot PQ,$$

and since α and β are linearly independent over $\mathbb{Z}$, then PQ must be the 2×2 identity matrix.

First we will check that if $(x,y)^\intercal = P(x_1x_2, x_1y_2, y_1x_2, y_1y_2)^\intercal$ then $f(x,y) = f_1(x_1,y_1) \cdot f_2(x_2,y_2)$ — in other words, that P provides a transformation between $f_1 \cdot f_2$ and f. To see this, for any such (x,y), (x_1,y_1), and (x_2,y_2), we can write

$$\begin{aligned}
\alpha x + \beta y &= \begin{bmatrix} \alpha & \beta \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \\
&= \begin{bmatrix} \alpha & \beta \end{bmatrix} \cdot P \cdot \begin{bmatrix} x_1x_2 \\ x_1y_2 \\ y_1x_2 \\ y_1y_2 \end{bmatrix} \\
&= \begin{bmatrix} \alpha_1\alpha_2 & \alpha_1\beta_2 & \beta_1\alpha_2 & \beta_1\beta_2 \end{bmatrix} \begin{bmatrix} x_1x_2 \\ x_1y_2 \\ y_1x_2 \\ y_1y_2 \end{bmatrix} \\
&= (\alpha_1x_1 + \beta_1y_1)(\alpha_2x_2 + \beta_2y_2).
\end{aligned}$$

Taking the conjugate of both sides gives

$$\overline{\alpha} x + \overline{\beta} y = (\overline{\alpha_1} x_1 + \overline{\beta_1} y_1)(\overline{\alpha_2} x_2 + \overline{\beta_2} y_2)$$

as well, and multiplying these equalities and dividing by $\mathcal{N}(\mathfrak{a}_1)\mathcal{N}(\mathfrak{a}_2)$ gives $f(x,y) = f_1(x_1,y_1)f_2(x_2,y_2)$.

It remains to check that P is a valid transformation matrix, i.e., that it satisfies the conditions in Definition 1.9. First to check that the greatest common divisor of its minors is 1, by the Cauchy–Binet formula we have

$$\det(PQ) = \sum \det(P_S)\det(Q_S)$$

where S ranges over all 2-element subsets of $\{1,2,3,4\}$, P_S denotes the 2×2 submatrix of P with column set S, and Q_S denotes the 2×2 submatrix of Q with row set S. But PQ is the identity matrix, so $\det(PQ) = 1$; this means the greatest common divisor of the minors $\det(P_S)$ must be 1 as well.

Meanwhile to check the sign condition $\det(P_{\{1,2\}}) > 0$, we have

$$\begin{bmatrix}\alpha_1\alpha_2 & \alpha_1\beta_2\end{bmatrix} = \begin{bmatrix}\alpha & \beta\end{bmatrix} \cdot P_{\{1,2\}},$$

which means by Lemma 2.5 that

$$\det(P_{\{1,2\}}) = \frac{\alpha_1\alpha_2\overline{\alpha_1\beta_2} - \overline{\alpha_1\alpha_2}\alpha_1\beta_2}{\alpha\overline{\beta} - \overline{\alpha}\beta} = \frac{n(\alpha_1)(\alpha_2\overline{\beta_2} - \overline{\alpha_2}\beta_2)}{(\alpha\overline{\beta} - \overline{\alpha}\beta)}.$$

We have $n(\alpha_1) > 0$ because we assumed that the x^2–coefficient of f_1 is positive, and $\alpha_2\overline{\beta_2} - \overline{\alpha_2}\beta_2$ and $\alpha\overline{\beta} - \overline{\alpha}\beta$ are required to be positive as well; this implies $\det(P_{\{1,2\}}) > 0$. We can similarly check that

$$\det(P_{\{1,3\}}) = \frac{n(\alpha_2)(\alpha_1\overline{\beta_1} - \overline{\alpha_1}\beta_1)}{(\alpha\overline{\beta} - \overline{\alpha}\beta)} > 0$$

as well. So P is indeed a valid transformation matrix, and therefore f is a composition of f_1 and f_2. □

Remark 2.19. It is also possible to compute the composition of forms with negative x^2–coefficient in this way — if f_1 instead has negative x^2–coefficient, then the theorem statement is true with $\mathfrak{a} = \mathfrak{a}_1\overline{\mathfrak{a}_2}$ instead. The proof is essentially the same, but with α_2 and β_2 replaced with $\overline{\alpha_2}$ and $\overline{\beta_2}$ in most places — the significance of this change is that then $n(\alpha_1)$ and $\overline{\alpha_2}\beta_2 - \alpha_2\overline{\beta_2}$ are both negative, so we still have

$$\det(P_{\{1,2\}}) = \frac{n(\alpha_1)(\overline{\alpha_2}\beta_2 - \alpha_2\overline{\beta_2})}{(\alpha\overline{\beta} - \overline{\alpha}\beta)} > 0.$$

Note that if $\mathcal{N}(\mathfrak{a}) = \mathcal{N}(\mathfrak{a}_1)\mathcal{N}(\mathfrak{a}_2)$, then Theorem 2.18 becomes the cleaner statement that the compositions of forms corresponding to $\mathfrak{a}_1$ and $\mathfrak{a}_2$ are simply the forms corresponding to $\mathfrak{a}_1\mathfrak{a}_2$; in particular, these compositions have discriminant Δ as well. Since primitive forms correspond to invertible ideals and vice versa, if at least one of f_1 and f_2 is primitive, then at least one of $\mathfrak{a}_1$ and $\mathfrak{a}_2$ is invertible, in which case by Lemma 2.11 we do have $\mathcal{N}(\mathfrak{a}) = \mathcal{N}(\mathfrak{a}_1)\mathcal{N}(\mathfrak{a}_2)$; so in particular, the composition of *primitive* forms of discriminant Δ always has discriminant Δ as well.

On the other hand, if $\mathcal{N}(\mathfrak{a}) \neq \mathcal{N}(\mathfrak{a}_1)\mathcal{N}(\mathfrak{a}_2)$, then the compositions are instead scaled multiples of the forms corresponding to $\mathfrak{a}_1\mathfrak{a}_2$, and do not have discriminant Δ.

2.5 The Class Group of Quadratic Forms

Theorem 2.18 has a few immediate consequences that allow us to place a *group structure* on the equivalence classes of quadratic forms.

Corollary 2.20. *If f_1 and f_1' are equivalent and f_2 and f_2' are equivalent, and all four forms have positive x^2–coefficient, then the set of compositions of f_1 and f_2 is the same as the set of compositions of f_1' and f_2'.*

Proof. This follows immediately from the fact that f_1 and f_1' correspond to the same ideal $\mathfrak{a}_1$, and the same is true for f_2 and f_2'. Then Theorem 2.18 (which applies as all four forms have positive x^2–coefficient) implies that the compositions of f_1 and f_2 and the compositions of f_1' and f_2' are both precisely the forms corresponding to the ideal $\mathfrak{a}_1\mathfrak{a}_2$. □

Then composition provides a binary operation on the equivalence classes of quadratic forms in $\mathcal{F}_\Delta$ — given two equivalence classes, choose representatives f_1 and f_2 with positive x^2–coefficient (such representatives always exist), and define their composition $[f_1] \cdot [f_2]$ as the equivalence class of all compositions of f_1 and f_2.

Theorem 2.21. *The set of equivalence classes of primitive forms in $\mathcal{F}_\Delta$ under composition forms a group, which is isomorphic to the narrow class group* $\mathrm{Cl}^+(\mathcal{O}_\Delta)$.

Proof. This follows immediately from the fact that composing two classes of forms corresponds exactly to multiplying the corresponding ideals, and that primitive forms correspond exactly to invertible ideals. □

In particular, note that Theorem 2.18 makes it immediate that composition is associative, since ideal multiplication is associative (this is true even if the forms are not primitive) — this is not obvious from the definition.

We use $\mathrm{Cl}(\mathcal{F}_\Delta)$ to denote this group of equivalence classes. The identity of $\mathrm{Cl}(\mathcal{F}_\Delta)$ is the quadratic form corresponding to the class of the unit ideal $(1) = \mathcal{O}_\Delta$. If $\Delta \equiv 0 \pmod 4$, then we can take the $\mathbb{Z}$-basis $\langle 1, -\frac{\sqrt{\Delta}}{2}\rangle$ to obtain that the identity is the class of the quadratic form

$$f(x,y) = \left(x - \frac{\sqrt{\Delta}}{2}y\right)\left(x + \frac{\sqrt{\Delta}}{2}y\right) = x^2 - \frac{\Delta}{4}y$$

(this in particular implies the original example of composition in Example 1.10). If $\Delta \equiv 1 \pmod 4$, then we can take the $\mathbb{Z}$-basis $\langle 1, \frac{1-\sqrt{\Delta}}{4}\rangle$, which gives that the identity is the class of

$$f(x,y) = \left(x + \frac{1-\sqrt{\Delta}}{2}y\right)\left(x + \frac{1+\sqrt{\Delta}}{2}y\right) = x^2 + xy + \frac{1-\Delta}{4}y^2.$$

We can similarly use $\mathrm{Cl}^+(\mathcal{O}_\Delta)$ to obtain inverses in $\mathrm{Cl}(\mathcal{F}_\Delta)$ — a form $f(x,y) = ax^2 + bxy + cy^2$ with $a > 0$ corresponds to the ideal $\mathfrak{a} = \langle a, \frac{b-\sqrt{\Delta}}{2}\rangle$, which has norm $\mathcal{N}(\mathfrak{a}) = a$. The inverse of the class of $\mathfrak{a}$ is the class of $\overline{\mathfrak{a}} = \langle -a, \frac{b+\sqrt{\Delta}}{2}\rangle$ (we change the sign of a to preserve the condition that $\alpha\overline{\beta} - \overline{\alpha}\beta$ should be positive in our $\mathbb{Z}$-basis), which has norm $\mathcal{N}(\overline{\mathfrak{a}}) = a$ as well, so the inverse of $[f]$ is the class of

$$f'(x,y) = \frac{\left(-ax - \frac{b+\sqrt{\Delta}}{2}\right)\left(-ax - \frac{b-\sqrt{\Delta}}{2}\right)}{a} = ax^2 - bxy + cy^2.$$

3 The Principal Genus Theorem

In this section, we will define the genus of a quadratic form and state and prove the principal genus theorem, using the group structure of $\mathrm{Cl}(\mathcal{F}_\Delta)$. We will follow [2, Chapter 4]. For simplicity, we will only work with the case where Δ is an odd fundamental discriminant — i.e., Δ is odd and not divisible by the square of any prime. These arguments can be adapted to even fundamental discriminants as well, and [2, Chapter 4] handles both cases, but the details are somewhat more messy. A generalization to nonfundamental discriminants is in [2, Chapter 7].

3.1 Definition of the Genus

We will define the genus of a quadratic form in terms of certain quadratic characters. We use $\left(\frac{a}{b}\right)$ to denote the Jacobi symbol of a mod b (if b is an odd prime, it is defined as 1 if a is a quadratic residue mod b, -1 if a is a quadratic nonresidue mod b, and 0 if $b \mid a$; it is then extended multiplicatively to all odd b). Note that the Jacobi symbol is multiplicative in both a and b.

Lemma 3.1. *For any primitive quadratic form f of discriminant Δ and any odd prime $p \mid \Delta$, all integers r relatively prime to p which are represented by f have the same value of* $\left(\frac{r}{p}\right)$.

Proof. Let $f(x,y) = ax^2 + bxy + cy^2$. First note that f cannot divide both a and c (if it did, then since p divides $\Delta = b^2 - 4ac$ it would also divide b, contradicting primitivity), so without loss of generality we may assume $p \nmid a$. Then if $f(x,y) = r$ for some integers x and y, by completing the square we have

$$4ar = (2ax + by)^2 - \Delta y^2 \equiv (2ax + by)^2 \pmod{p}.$$

This means $4ar$ is a square mod p, so $\left(\frac{4ar}{p}\right) = 1$, and therefore $\left(\frac{r}{p}\right) = \left(\frac{a}{p}\right)$, which means $\left(\frac{r}{p}\right)$ must be the same over all r relatively prime to p represented by f. □

Note also that by Lemma 1.5, any primitive quadratic form f represents some r relatively prime to each $p \mid \Delta$. This allows us to define a map $\chi_p \colon \mathrm{Cl}(\mathcal{F}_\Delta) \to \{\pm 1\}$ sending $[f]$ to the common value of $\left(\frac{r}{p}\right)$ over all r (relatively prime to p) which are represented by f — this is well-defined because equivalent forms represent the same set of integers, and therefore produce the same value of $\chi_p([f])$.

The key observation that will allow us to connect the group structure of $\mathrm{Cl}(\mathcal{F}_\Delta)$ to genera is the following.

Lemma 3.2. *For each prime $p \mid \Delta$, the map χ_p is a group homomorphism.*

Proof. Suppose that $[f] = [f_1] \cdot [f_2]$ where f_1 and f_2 have positive x^2-coefficient, so that f is a composition of f_1 and f_2. Let f_1 and f_2 represent integers r_1 and r_2 which are relatively prime to p. Then f represents $r_1 r_2$ by the definition of Gauss's composition law, so

$$\chi_p([f]) = \left(\frac{r_1 r_2}{p}\right) = \left(\frac{r_1}{p}\right)\left(\frac{r_2}{p}\right) = \chi_p([f_1])\chi_p([f_2]),$$

and therefore χ_p is a group homomorphism on $\mathrm{Cl}(\mathcal{F}_\Delta)$. □

We are now ready to define the genus of a quadratic form.

Definition 3.3. Let $\Delta = p_1 \cdots p_t$ for distinct odd primes $p_1, \ldots, p_t$, and let $\chi \colon \mathrm{Cl}(\mathcal{F}_\Delta) \to \{\pm 1\}^t$ be the homomorphism $[f] \mapsto (\chi_{p_1}([f]), \ldots, \chi_{p_t}([f]))$. For each vector $x \in \{\pm 1\}^t$, the *genus* corresponding to x is the set of forms $f \in \mathcal{F}_\Delta$ such that $\chi(f) = x$.

Since χ is a homomorphism, the genera are precisely the cosets of $\ker \chi$ (the set of forms mapped to the all-ones vector, which we denote by $\mathbf{1}$), which is known as the *principal genus*.

3.2 The Principal Genus Theorem

The principal genus theorem provides a complete classification of which forms are in the principal genus.

Theorem 3.4 (Principal Genus Theorem)**.** *A quadratic form f is in the principal genus if and only if $[f] = [f']^2$ for some form f'.*

In the remainder of this subsection, we will prove this theorem. One direction is fairly straightforward — if $[f] = [f']^2$ then $\chi([f]) = \chi([f'])^2 = \mathbf{1}$. However, the reverse direction is more difficult. In order to prove it, we will analyze two homomorphisms — the map $\chi \colon \mathrm{Cl}(\mathcal{F}_\Delta) \to \{\pm 1\}^t$ defined above, and the squaring map $\omega \colon \mathrm{Cl}(\mathcal{F}_\Delta) \to \mathrm{Cl}(\mathcal{F}_\Delta)$ sending $[f] \mapsto [f]^2$. We wish to prove that $\ker \chi = \operatorname{im} \omega$. Since the easy direction of the theorem implies that $\operatorname{im} \omega \subseteq \ker \chi$, it suffices to compare their sizes, and this can be done by instead comparing the sizes of $\operatorname{im} \chi$ and $\ker \omega$ — in other words, our goal is to prove that the set of genera is in bijection with the 2-torsion in $\mathrm{Cl}(\mathcal{F}_\Delta)$. It turns out that both of these sets are easier to understand. In Subsubsection 3.2.1 we will analyze $\operatorname{im} \chi$, the set of vectors $x \in \{\pm 1\}^t$ which actually correspond to genera. In Subsubsection 3.2.2 we will analyze $\ker \omega$, the set of classes of forms whose squares are the identity — or equivalently, which are equal to their own inverse. Such forms are called *ambiguous* forms.

3.2.1 Characterization of the Possible Genera

In this subsubsection, we will provide a full characterization of $\operatorname{im}\chi$ — we will prove that a vector $x = (x_1, \dots, x_t)$ is in $\operatorname{im}\chi$ if and only if $x_1 \cdots x_t = 1$, which will imply that there are 2^{t-1} genera.

In order to do this, we will need the following characterization of when some r is represented by *any* quadratic form of discriminant Δ.

Lemma 3.5. *If r is an odd positive integer relatively prime to Δ, then there exists a quadratic form of discriminant Δ which represents r if and only if for every prime q for which $\nu_q(r)$ is odd, Δ is a quadratic residue mod q.*

Proof. First we will show that this condition is necessary — we will show that if $\nu_q(f(x,y))$ is odd for some form f of discriminant Δ and integers x and y, then Δ is a quadratic residue mod q. First by dividing x and y by a power of q if necessary (which does not affect the parity of $\nu_q(f(x,y))$, and therefore preserves the fact that it is nonzero), we can ensure that at least one of x and y is not a multiple of q; without loss of generality suppose that $q \nmid y$. Then if $f(x,y) = ax^2 + bxy + cy^2$, completing the square gives that

$$(2ax + by)^2 - \Delta y^2 = 4af(x,y) \equiv 0 \pmod{q},$$

which since y is nonzero mod q implies that Δ must be a square mod q.

Conversely, suppose that Δ is a quadratic residue mod q for all primes q for which $\nu_q(r)$ is odd, and let $r = s^2 r'$ where r' is squarefree; then Δ is a quadratic residue mod r' as well. Since r' is odd and $\Delta \equiv 1 \pmod 4$ must be a quadratic residue mod 4, then Δ is a quadratic residue mod $4r'$ as well. This means there exist integers b and c such that

$$\Delta - b^2 = -4cr',$$

and therefore the form $f(x,y) = r'x^2 + bxy + cy^2$ has discriminant Δ. Then $f(s,0) = s^2 r' = r$, as desired. □

Lemma 3.6. *There exists a genus corresponding to $x = (x_1, \dots, x_t) \in \{\pm 1\}^t$ if and only if $x_1 \cdots x_t = 1$.*

Proof. First to show that this condition is necessary, suppose that there is a genus corresponding to x, so there is some quadratic form f such that the integers r represented by f satisfy $\left(\frac{r}{p_i}\right) = x_i$ for all i. Lemma 3.5 in particular implies that if a form of discriminant Δ represents r, then $\left(\frac{\Delta}{r}\right) = 1$. But by quadratic reciprocity, we have

$$\left(\frac{\Delta}{r}\right) = \left(\frac{r}{\Delta}\right) = \left(\frac{r}{p_1}\right) \cdots \left(\frac{r}{p_t}\right)$$

(note that $\Delta \equiv 1 \pmod 4$). So we must have $x_1 \cdots x_t = 1$.

To prove the converse, it suffices to construct some r such that $\left(\frac{r}{p_i}\right) = x_i$ for each i and r is represented by some form f; then we will have $\chi([f]) = x$. We will actually take r to be prime; in order to do this, we will need Dirichlet's theorem.

Theorem 3.7 (Dirichlet's theorem)**.** *Given any positive integer m and residue a relatively prime to m, there exist infinitely many primes $p \equiv a \pmod m$.*

By the Chinese Remainder Theorem, we can construct a residue $a \bmod p_1 \cdots p_t$ such that $\left(\frac{a}{p_i}\right) = x_i$ for each i; then by Dirichlet's theorem, there exists a prime $r \equiv a \pmod{p_1 \cdots p_t}$, which must also satisfy $\left(\frac{r}{p_i}\right) = x_i$ for each i. Then by quadratic reciprocity we have $\left(\frac{\Delta}{r}\right) = x_1 \cdots x_t = 1$, which since r is prime implies that Δ is a quadratic residue mod r; therefore by Lemma 3.5, there exists a quadratic form of discriminant Δ representing r, as desired. □

Corollary 3.8. *There are exactly 2^{t-1} genera. In other words, $|\operatorname{im}\chi| = 2^{t-1}$.*

3.2.2 Classes of Ambiguous Forms

We will now obtain an upper bound on the size of $\ker\omega$, i.e., the equivalence classes of ambiguous forms. We will only sketch the proof of this part, as it involves a fair amount of theory regarding the reduction of forms described in [2, Chapter 3]. This upper bound is actually an equality, as shown in [2, Proposition 4.17], but we will not need this for our purposes.

Lemma 3.9. *There are at most 2^{t-1} classes of ambiguous forms in $\mathcal{F}_\Delta$. In other words, $|\ker\omega| \le 2^{t-1}$.*

Proof Sketch. First we will show that any ambiguous form $f(x,y) = ax^2+bxy+cy^2$ is equivalent to the form $ax^2+axy+c'y^2$ for some c'. We may assume $a>0$ (by multiplying both by -1 otherwise); then the ideal $\mathfrak{a} = \langle a, \frac{b-\sqrt{\Delta}}{2}\rangle$ is associated to f by the construction in Subsection 2.2. Since $[f]$ is its own inverse in $\mathrm{Cl}(\mathcal{F}_\Delta)$, then $[\mathfrak{a}]$ must be its own inverse in $\mathrm{Cl}^+(\mathcal{O}_\Delta)$. Since the inverse of $[\mathfrak{a}]$ is $[\overline{\mathfrak{a}}]$ by Lemma 2.12, this means $\mathfrak{a} = \overline{\mathfrak{a}}$, and therefore $\langle a, \frac{b-\sqrt{\Delta}}{2}\rangle = \langle a, \frac{b+\sqrt{\Delta}}{2}\rangle$. This means $\mathfrak{a}$ must contain $\frac{b-\sqrt{\Delta}}{2} + \frac{b+\sqrt{\Delta}}{2} = b$, so $a \mid b$; then since b is odd, subtracting an appropriate multiple of a from $\frac{b-\sqrt{\Delta}}{2}$ gives that $\mathfrak{a} = \langle a, \frac{a-\sqrt{\Delta}}{2}\rangle$. Using this $\mathbb{Z}$-basis of $\mathfrak{a}$ in the construction in Subsection 2.2 gives a form $f'(x,y) = ax^2+axy+c'y^2$; since forms corresponding to the same ideal are equivalent, this means $f \sim f'$.

Then we must have $\Delta = a^2-4ac'$, so in particular a must divide Δ. This means any ambiguous form f is equivalent to the form $ax^2+axy+\frac{a+d}{4}y^2$ where $ad=-\Delta$.

It can be shown (see the proof of [2, Proposition 4.17]) that

$$ax^2+axy+\frac{a+d}{4}y^2 \sim dx^2+dy^2+\frac{a+d}{4}y^2.$$

In the case $\Delta<0$, this immediately finishes — there are 2^t ways to choose a to be a positive divisor of Δ (since Δ is a product of t primes), and each form produced in this way is equivalent to one other, so there are at most 2^{t-1} equivalence classes of ambiguous forms. (In fact, [2, Chapter 2] shows that these equivalence classes are all distinct, so there are exactly 2^{t-1} equivalence classes.)

In the case $\Delta>0$, this shows that every ambiguous form is equivalent to a form $ax^2+axy+\frac{a+d}{4}y^2$ with $ad=-\Delta$ and $|a|<\sqrt{\Delta}$ (since if $ad=-\Delta$, then this must be true of one of a and d). There are 2^t such forms (as we can choose the sign of a as well); however, the theory in [2, Chapter 3], and [2, Proposition 3.8] in particular, implies that each of these 2^t forms is equivalent to exactly one other, so we again have 2^{t-1} equivalence classes. □

3.2.3 Proof of the Principal Genus Theorem

We can now combine the results in Subsubsections 3.2.1 and 3.2.2 to prove the principal genus theorem.

Proof of Theorem 3.4. Consider the homomorphisms $\chi\colon \mathrm{Cl}(\mathcal{F}_\Delta) \to \{\pm1\}^t$ and $\omega\colon \mathrm{Cl}(\mathcal{F}_\Delta) \to \mathrm{Cl}(\mathcal{F}_\Delta)$ defined at the beginning of Subsection 3.2; as stated there, we wish to show that $\ker\chi = \mathrm{im}\,\omega$ (since $\ker\chi$ is by definition the principal genus, and $\mathrm{im}\,\omega$ is by definition the set of squares in $\mathrm{Cl}(\mathcal{F}_\Delta)$).

As stated in Subsection 3.2, it is clear that $\mathrm{im}\,\omega \subseteq \ker\chi$ — if $[f] \in \mathrm{im}\,\omega$ we can write $[f] = [f']^2$ for some f', and then $\chi([f]) = \chi([f'])^2 = \mathbf{1}$.

On the other hand, in Subsubsection 3.2.1 we showed that $|\mathrm{im}\,\chi| = 2^{t-1}$, and in Subsubsection 3.2.2 we showed that $|\ker\omega| \le 2^{t-1}$. Since we have

$$|\ker\chi|\,|\mathrm{im}\,\chi| = |\ker\omega|\,|\mathrm{im}\,\omega| = |\mathrm{Cl}(\mathcal{F}_\Delta)|\,,$$

this implies that $|\mathrm{im}\,\omega| \ge |\ker\chi|$. Since $\mathrm{im}\,\omega \subseteq \ker\chi$, this implies the two sets are in fact equal. □

References

[1] Mark Beintema and Azar Khosravani. The Origins of the Genus Concept in Quadratic Forms. *The Mathematics Enthusiast*, Volume 6, No. 1, Article 13, 2009 (https://doi.org/10.54870/1551-3440.1141).

[2] Duncan A. Buell. *Binary Quadratic Forms: Classical Theory and Modern Computations*. Springer, New York, 1989.

[3] Henri Cohen. *A Course in Computational Algebraic Number Theory*. Springer, Berlin, 1993.

[4] Harold M. Edwards. Composition of Binary Quadratic Forms and the Foundations of Mathematics. In *The Shaping of Arithmetic after C. F. Gauss's Disquisitiones Arithmeticae*, pages 129–144. Springer, Berlin, 2007.

[5] Franz Lemmermeyer. The Development of the Principal Genus Theorem. In *The Shaping of Arithmetic after C. F. Gauss's Disquisitiones Arithmeticae*, pages 529–561. Springer, Berlin, 2007.

[6] Franz Lemmermeyer. Binary Quadratic Forms and Counterexamples to Hasse's Local–Global Principle. 2011 (arXiv:1108.5687).

[7] Rick L. Shepherd. Binary Quadratic Forms and Genus Theory. Thesis, 2013.