Exploring Quadratic Form Composition on Conway's Topograph

Jenna M Allen

Department of Mathematics
University of Colorado
Boulder

Commitee

Advisor: Dr. Jonathan Wise, Department of Mathematics
Departmental Honors Director: Dr. Nathaniel Thiem, Department of Mathematics
Non-departmental representative: Dr. Benjamin Teitelbaum, Department of Musicology

Abstract:

In *Disquistones Arithmeticae,* Carl Friedrich Gauss constructs a composition law for binary quadratic forms [5]. Gauss's Composition law defines a group structure to the set of equivalence classes of primitive binary quadratic forms with the same discriminant. These group structures correspond to ideal classes of imaginary quadratic fields. In 1997, John Conway developed what is known as Conway's Topograph: a method for visualizing binary quadratic forms. Binary forms depicted on the topograph form "lakes," "wells", and "rivers" which are unique to each equivalence class of a primitive form. For example, a well found in the primitive form will be found in all quadratics in the same equivalence class as the primitive form. Since there exists a bijection between the ideal class groups and binary quadratic forms and a bijection between quadratic forms and Conway's Topograph, we wish to explore the bijection between the ideal class groups and Conway's Topograph.

Defense: November 3, 2020

Contents

1 An Introduction

Integral quadratic forms of two variables are given as,

$$f(x, y) = ax^2 + bxy + cy^2,$$

for a, b, c in the integers. The initial study of integral quadratic forms began with Lagrange who developed the ideas of discriminant, equivalence, and the reduced form [4]. Carl Friedrich Gauss later constructed a composition law for binary quadratic forms. In *Disquistones Arithmeticae*, Gauss implies there exists a group structure on the set of equivalence classes of primitive binary quadratic forms with same the discriminant[5]. Gauss demonstrated that for fixed discriminant, there are finitely many primitive binary quadratic forms. His method for composing quadratic forms is of some interest to us. Gauss was able to prove his composition results in an Abelian group; however, the theory is awkward and the proof is rather long and complicated. Instead, we will focus on Dirichlet's composition law, which uses a direct formula for the composition. It is possible to directly prove that for fixed discriminant, Dirichlet composition on the equivalence classes of primitive binary quadratic forms a finite Abelian group. However, the proof is made simpler by using ideal class groups.

Dedekind's Supplement XI builds the isomorphism between ideal class groups and quadratic forms. Using Dedekind's theory, an equivalence class of quadratic forms is equivalent to a fractional ideal in the ring of integers. The composition law also translates into the ideal class groups. Using the group structure, we are able to easily compose forms using simple multiplication of ideals.

There exists a more visual representation of quadratic forms known as Conway's Topograph, which was created by John H. Conway in his *The Sensual Quadratic Form*[3]. The topograph is an object that conveniently lays out the domain of a quadratic form along a tree structure where each vertex has three edges and every face has infinitely many edges. The result is that each edge is a basis of the domain and each face is a different input to a quadratic form.

Conway's Topograph provides an efficient method to explore the values of quadratics and to understand different forms. Furthermore, it provides an easy way to visualize the relationship between two equivalent quadratic forms. We will see how it only takes a gradual walk into the valley of the topograph to find a quadratic's "well," which gives us the associated reduced primitive form.

In this text, we will begin by exploring Conway's topograph. Section 2 will lay out the theory behind the construction of the topograph and how to plot a quadratic on it. Using this visual method, we will develop an understanding of primitive quadratic forms and how the members of the class group of quadratic forms relate to one another.

Section 3 develops the necessary machinery to demonstrate the Abelian group of classes of quadratic forms with fixed discriminant. We will begin with Dirichlet's composition before transitioning into defining quadratic fields and rings of integers. From here, we are able to build up to the ideal class group where we finally state and prove the bijection connecting ideals and quadratic forms.

Section 4 explores some methods attempted to view the composition law on the topograph. We find that we can build an ideal topograph where the norms of the ideals mimic the values of a quadratic form and each edge represents a basis of the ideal. By further examining Dirichlet's composition, we notice a connection between composing quadratic forms and finding matching edges on the related topographs. We end with a theorem from Trifković which gives us a direct computation for the composition when edges on two topographs match.

2 The Topograph

Conway's Topograph is a method for visualizing a particular class of quadratic polynomials over $\mathbb{Z}^2$. The topograph is outlined in a set of lectures given by John H. Conway, published in *The Sensual Quadratic*

Form [3]. We present its construction and use.

2.1 Construction

To begin, we find an *edge* on the topograph which is constructed from two *primitive vectors* that form a basis.

Definition 2.1. A **primitive vector** is an ordered pair (a, b) in $\mathbb{Z}^2$ such that $\gcd(a, b) = 1$. That is, (a, b) cannot be represented as $k \cdot (a', b')$ for some $k > 1$ and for some integers a' and b'.

For convenience, we choose $\pm(0, 1)$ and $\pm(1, 0)$ as the basis to begin construction. We split the plane into two with an edge denoted by a line. We then label the top of the plane with one basis vector and the bottom of the plane with the other as shown in Figure 1.

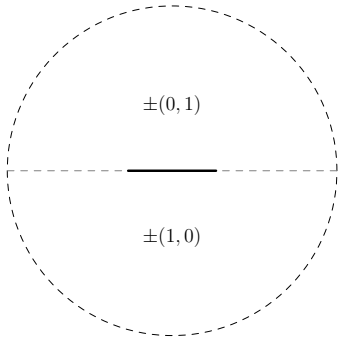

Figure 1: Starting edge of the topograph.

Definition 2.2. An **edge** on the topograph is uniquely defined by two primitive vectors (a, b) and (b, c) which form a basis such that, $\det\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \pm 1$. Each edge connects two *vertices* [8].

Definition 2.3. A **vertex** on the topograph is a point where three edges meet such that each vector has two edges separating it from the other two vectors. We define the vertex by the three primitive vectors surrounding it, which form a *superbase*.

Definition 2.4. A **superbase** is a set of three vectors, $\{\pm(a_1, b_1), \pm(a_2, b_2), \pm(a_3, b_3)\}$ such that

$$\pm(a_1, b_1) \pm (a_2, b_2) \pm (a_3, b_3) = 0$$

for some choice of signs. Any choice of two vectors forms a basis.

For example, consider the set of vectors, $\{\pm(0, 1), \pm(1, 0), \pm(1, 1)\}$. This is a superbase since $(0, 1) + (1, 0) - (1, 1) = 0$. We see that $\{\pm(1, 0), \pm(0, 1)\}$, $\{\pm(1, 0), \pm(1, 1)\}$, and $\{\pm(1, 1), \pm(0, 1)\}$ are all bases.

Theorem 2.5. *Suppose e_1 and e_2 form a basis in V. Then the sets $\{e_1, e_1 + e_2\}$, $\{e_2, e_1 + e_2\}$, $\{e_1, e_1 - e_2\}$, and $\{e_2, e_1 - e_2\}$ also form a basis.*

Proof. We will show that $\{e_1, e_1 + e_2\}$ form a basis. The other cases are similar.

Consider the vector equation for scalars n_1, n_2:

$$n_1 \cdot e_1 + n_2 \cdot (e_1 + e_2) = 0$$
$$(n_1 + n_2) \cdot e_1 + n_2 \cdot e_2 = 0.$$

Let $n_3 = n_1 + n_2$. Then,

$$n_3 \cdot e_1 + n_2 \cdot e_2 = 0.$$

Given that e_1 and e_2 form a basis, e_1 and e_2 are linearly independent. Then, the only solution to $n_3 \cdot e_1 + n_2 \cdot e_2 = 0$ is for $n_3, n_2 = 0$. Thus, the vectors e_1 and $e_1 + e_2$ are linearly independent.

For scalars $a \geq b$, let $x \in V$ where $x = a \cdot e_1 + b \cdot e_2$. We see that x may be written in terms of e_1 and $e_1 + e_2$ as follows:

$$x = (a - b) \cdot e_1 + b \cdot (e_1 + e_2).$$

Thus, e_1 and $e_1 + e_2$ span V and form a basis. □

Corollary 2.6. *The sets* $\{e_1, e_2, e_1 + e_2\}$ *and* $\{e_1, e_2, e_1 - e_2\}$ *each form a superbase.*

Given that a superbase defines each vertex and each pair of vectors in a superbase forms a basis, we can now add these edges to our topograph.

For a basis $\{\pm(a, b), \pm(c, d)\}$, Figure 2 demonstrates the addition of the superbases $\{\pm(a, b), \pm(c, d), \pm(a + c, b + d)\}$ and $\{\pm(a, b), \pm(c, d), \pm(a - c, b - d)\}$ to the topograph. We begin to see *faces* forming on the topograph.

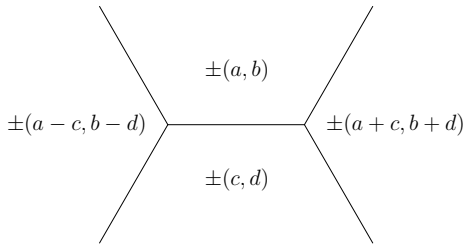

Figure 2: The two superbases.

Definition 2.7. A **face** on the topograph is defined by a primitive vector.

Figure 2 shows us how to construct the two vertices for a given edge by finding the neighboring faces. Applying this method to each face, we begin to construct a larger picture. Beginning with our basis of $\{\pm(0, 1), \pm(1, 0)\}$, we apply Theorem 2.5 repeatedly and achieve the picture shown in Figure 3.

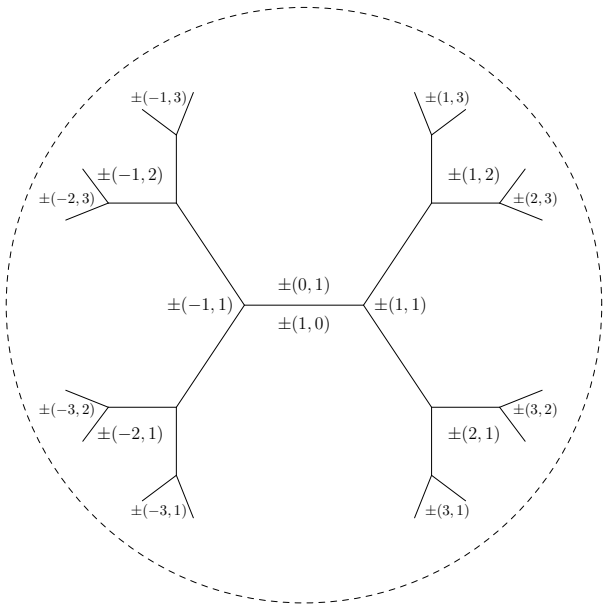

Figure 3: Conway's Topograph plotted within the Poincaré disk model.

By continually applying Theorem 2.5, we see that the topograph will continue to grow and is infinite. To view the entire topograph, one must visualize infinitely many n-gon faces. This image of the topograph is called the *domain topograph* [8].

Definition 2.8. The **domain topograph** is a method used to visualize the connections between infinitely many primitive vectors, bases, and superbases. Each primitive vector is shown on a face. Every basis is represented as an edge between the two faces representing the appropriate vectors.

Lemma 2.9. *Let $\{e_1, e_2\}$ be primitive vectors that form an edge on the topograph. Then, all the edges surrounding the face defined by e_1 are given by $\{n \cdot e_1, e_2\}$ for some integer n.*

Proof. This follows from Theorem 2.5 and Corollary 2.6. Proceed by induction. Let $k \in \mathbb{Z}$ and assume the edge $\{ke_1, e_2\}$ along the face e_1 is k edges away from $\{e_1, e_2\}$. Then, the next edge over is $\{e_1 + ke_1, e_2\} = \{(k+1)e_1, e_2\}$. □

Theorem 2.10. *All primitive vectors are contained in the domain topograph.*

Proof. This proof is similar to the proof given by Weissman[8]. Let $v_1 = (a, b)$ and $v_2 = (c, d)$ be primitive vectors that form a basis. Then $\{\pm v_1, \pm v_2\}$ form an edge on the topograph. Then $ad - bc = \pm 1$. Notice that $\gcd(a, c) = 1$ and $\gcd(d, b) = 1$. We may now apply the Euclidean algorithm.

$$(a, b) = q_0(c, d) + (e, f)$$

for some integer q_0 such that (c, d) and (e, f) share an edge on the topograph.

We see that each step of the Euclidean algorithm can be completed on the topograph by walking along q_0 edges surrounding the face $\pm v_2$ from the edge defined by $\{\pm v_1, \pm v_2\}$ by Lemma 2.9.

Repeating the Euclidean algorithm n, times we eventually find that

$$(p, q) = p(1, s) + (0, t).$$

The Euclidean algorithm applies row operations to our original matrix that do not modify the determinant. Thus,

$$\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \det \begin{pmatrix} 1 & s \\ 0 & t \end{pmatrix},$$

so $t = \pm 1$.

Now we have walked from $\{\pm v_1, \pm v_2\}$ to $\{\pm(1, s), \pm(0, 1)\}$. From here it is just a short walk as described by 2.9 to the edge $\{\pm(1, 0), \pm(0, 1)\}$.

Since we can walk from any edge to $\{\pm(1, 0), \pm(0, 1)\}$, the topograph is connected. □

2.2 Plotting a Quadratic

Up to this point, we have not considered how to visualize a quadratic form with the topograph. This is because domain topographs exist without the need of a quadratic form. The domain topograph simply outlines the structure and relationship to the values in the domain of a quadratic form. To view a quadratic form, we simply plug the values of the domain into the quadratic form and write the corresponding range value on the topograph instead of the domain vector. This constructs the *range topograph* [8].

Definition 2.11. A **two-variable homogeneous integral quadratic form** is a quadratic $ax^2 + bxy + cy^2$ with $a, b, c \in \mathbb{Z}$ where x,y are integer variables.

A single-variable quadratic function given by $g(x) = ax^2 + bx + c$ may be homogenized into an associated two-variable integral form found by

$$f(x, y) = y^2 \cdot g\left(\frac{x}{y}\right) = ax^2 + bxy + cy^2.$$

Conversely, a two-variable homogeneous integral quadratic $f(x, y) = ax^2 + bxy + cy^2$ is associated with the single-variable quadratic found by

$$g(x) = f(x, 1) = ax^2 + bx + c.$$

The single-variable quadratic function $g(x)$ has a root at $\frac{m}{n}$ if and only if $f(x, y)$ has a root at (m, n).

Two-variable homogeneous integral quadratic forms (indicated as quadratic forms unless otherwise indicated) have some very nice properties.

Lemma 2.12. *Given a quadratic form $f(x, y)$, for any scalar k we have $f(kx, ky) = k^2 f(x, y)$.*

Proof. Let $f(x, y) = ax^2 + bxy + cy^2$. Let $k \in \mathbb{R}$. Then we see that $f(kx, ky) = ak^2x^2 + bk^2xy + ck^2y^2 = k^2 f(x, y)$ □

Notice that 2.12 implies $f(-x, -y) = f(x, y)$ and $f(-x, y) = f(x, -y)$ for $k = -1$. This property is why we don't need to specify $+(a, b)$ or $-(a, b)$ when constructing the domain topograph.

Definition 2.13. The **range topograph** labels the regions of the domain topograph with the values of a given quadratic form. All possible values up to scaling are included on the topograph.

Figure 4 is the topograph for the quadratic form $14x^2 + 9xy + y^2$. The range topograph is in red while the domain topograph is in black.

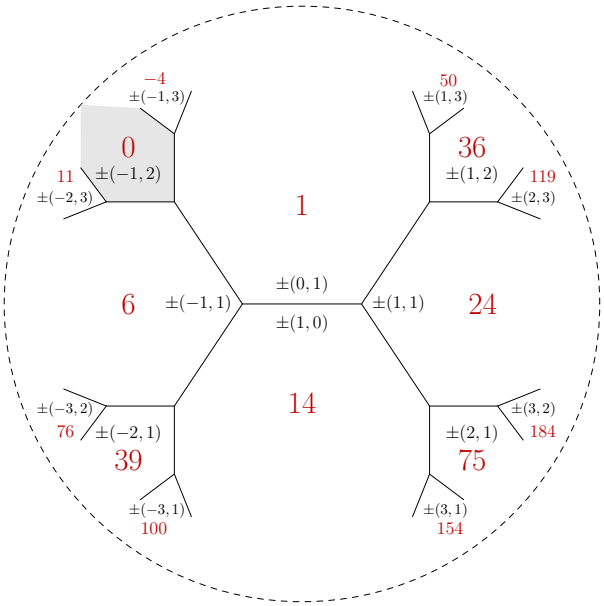

Figure 4: Graph of $14x^2 + 9xy + y^2$ on the topograph.

We now have a visual representation of the values of the quadratic. Notice the shaded face at $\pm(-1, 2)$ where the range topograph is zero. Faces in the range topograph that are zero are called *lakes*. Notice the superbase $\{\pm(-1, 2), \pm(0, 1), \pm(-1, 3)\}$. We call this basis a *well* since the absolute values of the range topograph increase as we move away from this feature. This phenomena is demonstrated by *the Climbing Lemma*. But first we prove *the Arithmetic Progression Rule* which allows the construction of the range topograph without the domain topograph.

Theorem 2.14 (The Arithmetic Progression Rule)**.** *Let $\{\pm e_1, \pm e_2, \pm e_3\}$ be a superbase where $e_3 = e_1 - e_2$. Given a quadratic form $f(x, y)$ with known values at the superbase, we may find the value of $f(x, y)$ at $e_1 + e_2$ as*

$$f(e_1 + e_2) = 2 \cdot f(e_1) + 2 \cdot f(e_2) - f(e_3).$$

Proof. This can be verified by directly comparing the values of $f(e_1 + e_2)$ to $2 \cdot f(e_1) + 2 \cdot f(e_2) - f(e_3)$ in a rather labor intensive, brute force fashion. For a more elegant proof, Conway compares this to Apollonius's theorem in geometry[3]. Weissman has an alternative method that proves this by demonstrating the presence of an arithmetic progression[8]. □

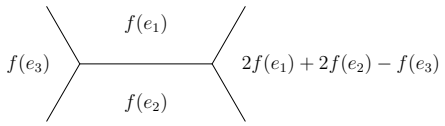

Figure 5: The Arithmetic Progression Rule.

The Arithmetic Progression Rule allows a complete construction of a range topograph given the values of the quadratic form at a superbase.

When drawing the topograph, it can be beneficial to label the direction in which the values are growing. Notice that the value of $f(e_1+e_2)$ is found by calculating $f(e_1)+f(e_2)$ and then adding $f(e_1)+f(e_2)-f(e_3)$. Let $h = f(e_1)+f(e_2)-f(e_3)$. Draw an arrow on the edge of $f(e_1)$ and $f(e_2)$ pointing toward $f(e_1+e_2)$ to indicate $f(e_1+e_2) = f(e_1)+f(e_2)+h$ (Figure 6). Should you choose to fill in the topograph in the opposite direction of the arrow, simply subtract h from $f(e_1)+f(e_2)$. Thus, in Figure 6, $f(e_3) = f(e_1)+f(e_2)-h$.

Theorem 2.15 (The Climbing Lemma)**.** *If $f(e_1)$, $f(e_2)$, and h are positive, then $f(e_1+e_2)$ is positive. Additionally, the edge between $f(e_1)$ and $f(e_1+e_2)$ has an arrow pointing away from the vertex representing the superbase at $\{e_1, e_2, e_1+e_2\}$. Likewise, the edge between $f(e_2)$ and $f(e_1+e_2)$ has an arrow pointing away from the vertex representing the superbase at $\{e_1, e_2, e_1+e_2\}$.*

Proof. Recall $h = f(e_1)+f(e_2)-f(e_3)$. Thus, $|h| < |f(e_1)+f(e_2)|$. So $f(e_1+e_2)$ must be positive for positive $f(e_1)$ and $f(e_2)$. The proof is similar for the other case. □

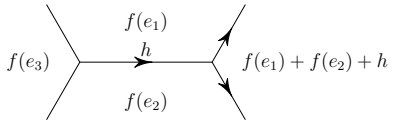

Figure 6: Progressing arithmetically with difference term h.

2.2.1 Quadratic forms on the Topograph

Conway classifies quadratics and their topographies based upon the signs at all nonzero primitive vectors and by objects that appear in the topograph. Conway names these objects after water features such as "lakes" and "wells." To classify quadratic forms we must first define these objects that occur on the topograph.

Definition 2.16. Given a two variable homogeneous integral quadratic form, $f(x,y)$, if for all $e_i \in \mathbb{Z}^2$, $f(e_i) > 0$ or $f(e_i) < 0$, then there exists a superbase $\{\pm(e_1), \pm(e_2), \pm(e_3)\}$ such that $f(e_1), f(e_2)$ and $f(e_3)$ satisfy the triangle equality. That is, $f(e_1)+f(e_2) \geq f(e_3)$ and $f(e_2)+f(e_3) \geq f(e_1)$ and $f(e_1)+f(e_3) \geq f(e_2)$. We call this superbase a **well**. A double well occurs when two wells are formed and are joined by an edge.

By applying Theorems 2.14 and 2.15, as we move away from the well, the absolute values of the faces increase. It is possible to have two wells sharing a single edge where the h value along the edge is zero. We call this a double well. Since the absolute values of the faces increase as we move away from the well(s), it is impossible to have two or more wells separated by more than one edge. Thus, there is only one well, or double well, which is analogous to a minima or maxima of the quadratic form.

Definition 2.17. A **river** is a sequence of connected edges that separate the positive and negative values. Rivers separate the topograph into a positive region and a negative region. A form, $f(x,y) = ax^2+hxy+cy^2$, has a river if $ab-2h$ is negative, but not the negative of a perfect square.

Definition 2.18. A **lake** is a region on the topograph where $f(x,y)$ is zero. The regions around a lake form an arithmetic progression unless the lake has a river connecting it to another lake, or is immediately adjacent to a second lake.

Now we may define the forms as follows:

- The + Forms: The smallest values surround a single or double well and increase as we move away from the well(s).
- The − Forms: The smallest values surround a single or double well and decrease as we move away from the well(s).
- The +− Forms: There is a periodic *river* of edges separating the positive and negative values. Values increase in absolute value as we move away from the river.
- The 0 Form: The only value is 0 and the topograph consists of infintely many *lakes* labeled 0.
- The 0+ Form: Values increase as we move away from a single lake.
- The 0− Form: Values decrease as we move away from a single lake.
- The 0 + − Form: There are two distinct lakes joined by a finite river. The river and lakes separate the positive and negative values of the topograph. There is a special case of this form where both lakes are adjacent and there is no river.

For the rest of this paper we are especially interested in in + Forms also known as positive definite forms. Positive definite forms have interesting properties which we explore more in the following sections.

2.3 Topographs of Positive Definite Forms

Given a quadratic form $f(x, y) = ax^2 + hxy + by^2$, we may begin the drawing of the topograph as shown in Figure 7. We define the maps from quadratic to topograph and topograph to quadratic as follows.

Definition 2.19. Given a quadratic form $f(x, y) = ax^2 + hxy + by^2$, we may begin the drawing of the topograph at the superbase $\{\pm(0, 1), \pm(1, 0), \pm(1, 1)\}$ as shown by the vertex in Figure 7.

Definition 2.20. Given a vertex of the topograph at the superbase $\{\pm(0, 1), \pm(1, 0), \pm(1, 1)\}$ as shown in Figure 7 we find the represented quadratic form to be,

$$f(x, y) = ax^2 + (c - a - b)xy + by^2.$$

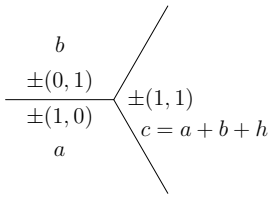

Figure 7: Superbase at $\{\pm(0, 1), \pm(1, 0) \pm (1, 1)\}$ of $ax^2 + hxy + by^2$.

It is easy to verify that these mappings are inverses of each other and by construction, the range topograph is isomorphic to the quadratic form it represents.

In general, the quadratic forms we will be examining on a topograph are *primitive*.

Definition 2.21. A **primitive quadratic form** is a form $f(x, y) = ax^2+bxy+cy^2$ such that $\gcd(a, b, c) = 1$.

Any form that is primitive can be made not primitive by scaling a, b, c by some value. Any not primitive form is easily made primitive by dividing by $\gcd(a, b, c)$.

Notice that the map in Definition 2.20 does not actually care about the domain topograph underneath. In fact, any vertex of a range topograph can be written as a quadratic form.

Definition 2.22. We say two forms f and g are equivalent if for $m, n, k, \ell \in \mathbb{Z}$, $f(x, y) = g(mx+ny, kx+\ell y)$ and $\begin{pmatrix} m & n \\ k & \ell \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$. That is, $m\ell - nk = 1$

The matrix $\begin{pmatrix} m & n \\ k & \ell \end{pmatrix}$ is a change-of-basis matrix. On the topograph, this describes how to move from one edge of the topograph to another. This transformation further defines the presence of equivalence classes of quadratic forms.

Definition 2.23. The **discriminant** of a quadratic form $f(x, y) = ax^2 + bxy + cy^2$ is $D = b^2 - 4ac$.

The discriminant is always either 0 mod 4 or 1 mod 4. It is worth noting that if $f(x, y) = ax^2 + bxy + cy^2$ is positive definite, then $g(x, y) = -(ax^2 + bxy + cy^2)$ is necessarily negative definite. In which case, f and g share the same discriminant.

For positive definite forms, $D < 0$.

Lemma 2.24. *For any quadratic form, there is an equivalent form such that $|b| \leq |a| \leq |c|$ and $b \geq 0$ if $|a| = |b|$ or $|a| = |c|$.*

Proof. For proof, one can view Legendre's reduction algorithm. It can be found in Trifković [7] on page 132. □

Using 2.24 we can enumerate out the quadratic forms that represent equivalence classes for a given discriminant.

Theorem 2.25. *There are finitely many equivalence classes of quadratic forms for given discriminant D.*

Proof. Pick $D < 0$. We now present an algorithm for finding quadratic forms as shown by Trifković [7]. Since D is negative, $b^2 - D$ is positive. By 2.24 we are looking for the form with $|b| \leq |a| \leq |c|$ so,

$$-D = 4ac - b^2 \geq 4b^2 - b^2 = 3b^2.$$

So $|b| < \sqrt{-D/3}$. We now have finitely many b's to check. Once again using the discriminant, $b^2 - 4ac = D$ we find that there are finitely many values for a and c.

All that remains is to check each possible form for equivalence to the others which is easily done by checking the range topograph for each form and identifying the well.

Since 2.24 shows us that every form is equivalent to the forms we have found, there must be finitely many equivalence classes of forms. □

3 Ideals

Gauss first proved that quadratic forms of a given discriminant can be separated into equivalence classes represented by a single primitive form as we explored in the previous chapter. In *Disquisitiones Arithmeticae*, Gauss develops a composition law which is rather tedious and difficult to read and prove. While not necessarily easy to do, it has been shown that it is possible to automate the composition [6]. Here, we find Dirichlet's composition from Supplement X is significantly easier to implement and understand [2].

Lemma 3.1. *Let $f(x, y) = ax^2 + bxy + cy^2$ and $g(x, y) = a'x^2 + b'xy + c'y^2$ be two binary quadratic forms of discriminant D. Let $gcd\left(a, a', \frac{b+b'}{2}\right) = e$. Then, there is a unique integer B modulo $\frac{2aa'}{e^2}$ such that,*

$$B \equiv b \ mod \ \frac{2a}{e},$$
$$B \equiv b' \ mod \ \frac{2a'}{e},$$
$$B^2 \equiv D \ mod \ \frac{4aa'}{e^2}.$$

Proof. For proof, see Boyer[2] page 6 or Cox[4] page 48. □

Definition 3.2. Let $f(x,y) = ax^2 + bxy + cy^2$ and $g(x,y) = a'x^2 + b'xy + c'y^2$ be two binary quadratic forms of discriminant D. The **Dirichlet composition** of $f(x,y)$ and $g(x,y)$ is the form,

$$F(x,y) = \frac{aa'}{e^2}x + Bxy + \frac{B^2 - D}{4aa'}y^2,$$

where B is the integer B of Lemma 2.

This composition allows us to build an *Abelian group* from classes of quadratic forms.

Definition 3.3. A **group** G is a set with a law of composition with the following properties:

(i) Composition is associative. That is, $(ab)c = a(bc)$ for all a, b, and c in G.

(ii) There exists an identity element 1 in G such that $1a = a$ and $a1 = a$ for all a in G.

(iii) For every element a in G there exists an inverse b in G such that $ab = 1$ and $ba = 1$.

We call a group **Abelian** if the law of composition is commutative. That is, $a \times b = b \times a$ for a, b in G [1].

The proof that classes of quadratic forms form a group can be done using the composition directly with quadratic forms, but it is tricky. The proof is significantly easier if done using ideal class groups, which have a bijection to classes of quadratic forms. Here, we will build up the basic ring theory necessary to understand the bijection, prove it is a bijection, and then show that classes of quadratic forms form an Abelian group.

3.1 Ring of Integers

We suggest having a basic understanding of group theory. However, we will recall some basic definitions here[1].

Definition 3.4. A **ring** R is a set closed under two binary operations $+$ and $\times$ with the following properties:

(i) Under $+$, R is an abelian group with identity 0.

(ii) The operation $\times$ is associative with identity 1.

(iii) The distributive law holds. That is, for all a, b, and c in R, $(a + b)c = ac + bc$.

Definition 3.5. A **field** F is a set closed under two binary operations $+$ and $\times$ with the following properties:

(i) Under $+$, F is an abelian group with identity 0.

(ii) Under $\times$, $F - 0$ is an abelian group with identity 1.

(iii) The distributive law holds. That is, for all a, b, and c in R, $(a + b)c = ac + bc$.

Definition 3.6. A **quadratic field** is a field of the form,

$$\mathbb{Q}\left[\sqrt{D}\right] = \left\{a + b\sqrt{D} \ : \ a, b \in \mathbb{Q}\right\},$$

Where $D \in \mathbb{Z}$ is square-free. We say the field $\mathbb{Q}\left[\sqrt{D}\right]$ is **imaginary** for $D < 0$ and **real** for $D > 0$

We can already see a connection from quadratic fields to our quadratic forms. An element $\alpha \in \mathbb{Q}\left[\sqrt{D}\right]$ where $\alpha = a + b\sqrt{D}$ is precisely the root located in the upper half-plane of a quadratic polynomial, $f(x) = x^2 - 2ax + a^2 - b^2D$. Further, the *conjugate* of α, given as $a - b\sqrt{D}$, is the root located in the lower half plane.

[1]The following definitions are taken from Artin[1]

Definition 3.7. Let $\alpha \in \mathbb{Q}\left[\sqrt{D}\right]$. Then $\alpha = a + b\sqrt{D}$. We define the **conjugate** of α as $\bar{\alpha} = a - b\sqrt{D}$. Then the **norm** of α is,

$$N(\alpha) = \alpha\bar{\alpha} = a^2 - b^2 D.$$

The **trace** of α is,

$$Tr(\alpha) = \alpha + \bar{\alpha} = 2a.$$

The basic properties of the norm are given in the following theorem.

Lemma 3.8. *For all $\alpha, \beta \in \mathbb{Q}\left[\sqrt{D}\right]$, $N(\alpha\beta) = N(\alpha)N(\beta)$. Additionally, $N(\alpha) = 0$ if and only if $\alpha = 0$.*

Proof. Let $\alpha = a + b\sqrt{D}$ and $\beta = c + e\sqrt{D}$. Consider the following,

$$\begin{aligned}
N(\alpha\beta) &= N\left[(a + b\sqrt{D})(c + e\sqrt{D})\right] \\
&= N(ac + beD + (bc + ae)\sqrt{D}) \\
&= (ac + beD + (bc + ae)\sqrt{D})(ac + beD - (bc + ae)\sqrt{D}) \\
&= (ac + beD)^2 - (bc + ae)^2 D \\
&= a^2c^2 + 2abceD + b^2e^2D^2 - b^2c^2D - 2abceD - a^2e^2D \\
&= a^2c^2 - a^2e^2D - b^2c^2D + b^2e^2D^2 \\
&= (a^2 - b^2D)(c^2 - e^2D) \\
&= N(a + b\sqrt{D})N(c + e\sqrt{D}) \\
&= N(\alpha)N(\beta).
\end{aligned}$$

By applying definition 3.7, if $\alpha = 0$, $N(\alpha) = 0$. Now assume $N(\alpha) = 0$. Then $\alpha\bar{\alpha} = a^2 - b^2D = 0$ and $a^2 = b^2D$. Thus $a = b$ and $D = 1$, $D = a^2$ and $b = 1$, or $a = b = 0$. But D is defined to be square-free and $D \neq 1$ or a^2. Therefore $a = b = 0$ and $\alpha = 0$. □

The basic properties of the trace are similar to the norm.

Lemma 3.9. *For all $\alpha, \beta \in \mathbb{Q}\left[\sqrt{D}\right]$, $Tr(\alpha + \beta) = Tr(\alpha) + Tr(\beta)$. Further if $\alpha = a + b\sqrt{D}$, $Tr(\alpha) = 0$ if and only if $\alpha = b\sqrt{D}$.*

Proof. Let $\alpha = a + b\sqrt{D}$ and $\beta = c + e\sqrt{D}$. Consider the following,

$$\begin{aligned}
Tr(\alpha + \beta) &= Tr\left[a + b\sqrt{D} + c + e\sqrt{D}\right] \\
&= Tr\left[(a + c) + (b + e)\sqrt{D}\right] \\
&= (a + c) + (b + e)\sqrt{D} + (a + c) - (b + e)\sqrt{D} \\
&= (a + b\sqrt{D} + a - b\sqrt{D}) + (c + e\sqrt{D} + c - e\sqrt{D}) \\
&= Tr(\alpha) + Tr(\beta).
\end{aligned}$$

By Definition 3.7, if $\alpha = b\sqrt{D}$ then $Tr(\alpha) = 0$. Assume $Tr(\alpha = 0)$. Then $2a = 0$ so $a = 0$. Thus $\alpha = 0 + b\sqrt{D} = b\sqrt{D}$. □

Notice that in our original quadratic polynomial, $f(x) = x^2 - 2ax + a^2 - b^2D$. By substituting the trace and norm, we get

$$f(x) = x^2 - Tr(\alpha)x + N(\alpha).$$

We are particularly interested in $\alpha \in \mathbb{Q}\left[\sqrt{D}\right]$ such that $Tr(\alpha)$ and $N(\alpha)$ are integers.

Definition 3.10. The **ring of integers** of $\mathbb{Q}\left[\sqrt{D}\right]$ is the set

$$\mathcal{O} = \left\{\alpha \in \mathbb{Q}\left[\sqrt{D}\right] \ : \ Tr(\alpha), N(\alpha) \in \mathbb{Z}\right\}.$$

Here we have defined the ring of integers as a set. However it does form a ring.

Lemma 3.11. *The ring of integers is a ring under addition and multiplication in the reals.*

Proof. Addition and multiplication are associative and multiplication is commutative since $\mathcal{O}$ is a subgroup of $\mathbb{R}$.

Let $\alpha, \beta \in \mathcal{O}$. Then $Tr(\alpha+\beta) = Tr(\alpha) + Tr(\beta)$ by Lemma 3.9, which is an integer. Let $\alpha = a + b\sqrt{D}$ and $\beta = c + d\sqrt{D}$. Then,

$$\begin{aligned} Tr(\alpha\beta) &= Tr(ac - bdD + (ad+bc)\sqrt{D}) \\ &= 2ac - 2bdD, \end{aligned}$$

which is an integer. Now consider the norm. We have $N(\alpha\beta) = N(\alpha)N(\beta)$ by Lemma 3.8. Then,

$$\begin{aligned} N(\alpha+\beta) &= N(a+c+(b+d)\sqrt{D}) \\ &= (a+c)^2 - (b+d)^2 D, \end{aligned}$$

which is an integer.

We see that $0 \in \mathcal{O}$ such that for $\alpha \in \mathcal{O}$, $\alpha + 0 = 0 + \alpha = \alpha$ and for every α there is an inverse $-\alpha$ such that $\alpha + (-\alpha) = 0$ □

We can define the values of $\mathcal{O}$ more precisely by considering the values of D mod 4.

Theorem 3.12. *Let $D \in \mathbb{Z}$ and square-free. Then the ring of integers of $\mathbb{Q}\left[\sqrt{D}\right]$ is given by $\mathcal{O} = \mathbb{Z} + \mathbb{Z}\delta = \mathbb{Z}[\delta]$ where*

$$\delta = \begin{cases} \sqrt{D} & \text{for } D \equiv 2,3 \text{ (mod 4)} \\ \frac{1+\sqrt{D}}{2} & \text{for } D \equiv 1 \text{ (mod 4)} \end{cases}.$$

Proof. This is a reproduction of the proof in Trifković [7]. First we show that $\sqrt{D}$ and $\frac{1+\sqrt{D}}{2}$ are in $\mathcal{O}$. We see that $Tr(\sqrt{D}) = 0$ by 3.9 and $N\left(\sqrt{D}\right) = D$ by 3.7. We calculate the norm and trace of $\frac{1+\sqrt{D}}{2}$:

$$\begin{aligned} N\left(\frac{1+\sqrt{D}}{2}\right) &= \frac{1}{4} - \frac{1}{4}D \\ &= \frac{1-D}{4}, \\ Tr\left(\frac{1+\sqrt{D}}{2}\right) &= \frac{1+\sqrt{D}}{2} + \frac{1-\sqrt{D}}{2} \\ &= 1. \end{aligned}$$

We see that $N\left(\frac{1+\sqrt{D}}{2}\right) \in \mathbb{Z}$ only if $D \equiv 1 \bmod 4$. Thus $\mathbb{Z}[\delta] \subseteq \mathcal{O}$.

We now wish to show $\mathcal{O} \subseteq \mathbb{Z}[\delta]$ Pick $\alpha \in \mathcal{O}$ such that $\alpha = a + b\sqrt{D}$. Then, by definition the trace and norm of α are integers. For integers r, m, n, let $a = \frac{r}{2}$ and $b = \frac{m}{n}$ such that $\gcd(m,n) = 1$. Then $N(\alpha) = \frac{r^2}{4} - \frac{m^2}{n^2}D$. With some reorganizing, $4m^2D = n^2(r^2 - 4N(\alpha))$. Since n and m are relatively prime, n^2 cannot divide m^2. So, n^2 must divide $4D$. If there was a prime p that divides n, then p^2 must divide D, but D is square-free. So, $n = 2^\ell$ for integer ℓ. Note that 2 is prime, so 2^2 does not divide D. So, $2\ell \leq 3$. Thus, $n = 1$ or $n = 2$. So, $b = \frac{2m}{2}$ or $b = \frac{m}{2}$. We pick $s \in \mathbb{Z}$ such that $b = \frac{s}{2}$ Reconsider the norm, $N(\alpha) = \frac{r^2}{4} - \frac{s^2}{4}D$ which we may rearrange to be $r^2 - s^2D = 4N(\alpha)$. That is, $r^2 \equiv s^2 D \bmod 4$. We see that only squares modulo 4 are 1 and 0, so $r^2, s^2 \equiv 0$ or $1 \bmod 4$.

(i) Assume $D \not\equiv 1 \bmod 4$. Then r^2 and $s^2 \equiv 0 \bmod 4$, and r and s are even. Thus, a and b are integers so we have $\mathbb{Z} + \mathbb{Z}\sqrt{D}$.

(ii) Assume $D \equiv 1 \bmod 4$. Then r^2 and $s^2 \equiv 0 \bmod 4$, and r and s are odd. So, for some $k \in \mathbb{Z}$ we may write $r = s + 2k$ and we have

$$\frac{s+2k}{2} + \frac{s\sqrt{D}}{2} = k + s\frac{1+\sqrt{D}}{2}$$

as desired.

Thus $\mathcal{O} \subseteq \mathbb{Z}[\delta]$, so $\mathcal{O} = \mathbb{Z}[\delta]$. □

Definition 3.13. The discriminant of the ring $\mathbb{Q}[\sqrt{D}]$ is given by D.

It turns out that rings of integers with discriminant D correspond to quadratic forms of discriminant D. We are particularly interested in the ideals of the ring $\mathcal{O}$.

3.2 Ideal

Recall the definition of an ideal:

Definition 3.14. An **ideal** I of a ring R is a nonempty subset of R such that

(i) I is closed under addition. That is, for a, b in I, $a + b$ is in I.

(ii) If a is in I and r is in R, then rs is in I.

We wish to consider the ideals in a quadratic ring. These are given by $\mathbb{Z}\alpha + \mathbb{Z}\beta = \{m\alpha + n\beta \ : \ m, n \in \mathbb{Z}\}$ for $\alpha, \beta \in \mathcal{O}$.

Lemma 3.15. *Every ideal in a quadratic ring has the form $\mathbb{Z}\alpha + \mathbb{Z}\beta$ for $\alpha, \beta \in \mathcal{O}$.*

Proof. This is a result of the Elementary Divisor Theorem. Let α be an element of the ideal. Then α is also in $\mathcal{O} = \mathbb{Z}[\delta]$ so for a and b in the integers we may write it as, $\alpha = a + b\delta$. This form cannot be isomorphic to the set $\{0\}$. It is also not isomorphic to $\mathbb{Z}$ since there is a second, imaginary term given by δ. Therefore it is isomorphic to $\mathbb{Z}^2$, namely $\alpha = a + b\delta \simeq (a, b)$ where $(a, b) \in \mathbb{Z}^2$. □

Definition 3.16. The **norm** of an ideal $I \neq 0$ of $\mathcal{O}$ is $N(I) = |\mathcal{O}/I|$ [7].

Definition 3.17. Recall δ from 3.12. A **fractional ideal** in a quadratic field, $\mathbb{Q}\left[\sqrt{D}\right]$, is an additive subgroup $\mathscr{I}$ of $\mathbb{Q}\left[\sqrt{D}\right]$ that satisfies the following:

(i) $\mathscr{I} = \mathbb{Z}\alpha + \mathbb{Z}\beta$, for $\alpha, \beta \in \mathbb{Q}\left[\sqrt{D}\right]$ are linearly independent over $\mathbb{Z}$.

(ii) $\delta\mathscr{I} \subseteq \mathscr{I}$

One way we can think of α and β as is a lattice over $\mathbb{Q}\left[\sqrt{D}\right]$. For an ideal I, we call (α, β) an oriented basis of I.

Definition 3.18. We say a basis (α, β) of an ideal I is properly oriented if,

$$\frac{\bar{\alpha}\beta - \alpha\bar{\beta}}{\sqrt{D}} \geq 0$$

Definition 3.19. For an ideal I, we call I a **principal ideal** in the ring R if $I = Ra$ for some $a \in R$. We call a a **generator** of I

We can translate the principal ideals to fractional ideals as well.

Definition 3.20. Fractional ideals in the form

$$\mathcal{O}_\alpha = \left\{\beta\alpha \ : \ \beta \in \mathbb{Q}\left[\sqrt{D}\right]\right\} = \mathbb{Z}\alpha + \mathbb{Z}\delta\alpha,$$

for any $\alpha \in \mathbb{Q}\left[\sqrt{D}\right] \setminus 0$ are called **principal fractional ideals.**

We may now define the ideal class group.

Definition 3.21. If H is a subgroup of G and if a is an element of G, the subset

$$aH = \{ah \ : \ h \in H\}$$

is the **left coset** [1].

Definition 3.22. The set of all cosets of a subgroup H of a group G denoted G/H is called a **quotient group**.[1]

Definition 3.23. Let $\mathbb{I}_{\mathcal{O}}$ be the group of fractional ideals in $\mathcal{O}$. Let $\mathbb{P}_{\mathcal{O}}$ be the subgroup of $\mathbb{I}_{\mathcal{O}}$ consisting of all principal fractional ideals. The **ideal class group** is the quotient

$$Cl(\mathcal{O}) = \mathbb{I}_{\mathcal{O}}/\mathbb{P}_{\mathcal{O}}.$$

Our interest is in a fractional ideal $(\alpha, \beta) = \mathbb{Z}\alpha + \mathbb{Z}\beta$, where $\alpha, \beta \in \mathcal{O}$.

Definition 3.24. Every ideal class is represented by an integral ideal, I. Namely for fractional ideals $\mathscr{I}$ and $\mathscr{J}$ and $k \in \mathcal{O}$,

$$\mathscr{J} = k\mathscr{J} = I.$$

Definition 3.25. Let I and J be ideals. The product, IJ is

$$IJ = \left\{ \sum_{i=1}^{m} x_i y_i \ : \ x_i \in I, y_i \in J \right\}.$$

That is, the product IJ is the smallest ideal containing all products xy.

Given two ideals, I_1 generated by (a, b) and I_2 generated by (c, d), we may find the product of two ideals as,

$$\begin{aligned} I_1 I_2 &= (a, b)(c, d) \\ &= (ac, ad, bc, bd). \end{aligned}$$

By Lemma 3.15 we know the smallest ideal containing all these products must be generated by two elements. Thus, by linear combinations of ac, ad, bc, and bd we may find (α, β), which generate the ideal I_3.

3.3 Proof of the Bijection

For fixed discriminant D there is a bijection between classes of binary quadratic forms of discriminant D and the ideal class group. Using this correspondence we can calculate the class number of an ideal class group, and use this correspondence to preform Gauss's composition law.

Definition 3.26. Let $\mathscr{I}$ be a fractional ideal of $\mathcal{O}$ and let (α, β) be an ordered basis of $\mathscr{I}$. Then $f_{\mathscr{I}(\alpha,\beta)}$ is a quadratic form given by,

$$f_{\mathscr{I}(\alpha,\beta)} = \frac{N(\alpha x + \beta y)}{N(\mathscr{I})}.$$

(As given by Trifković [7])

Definition 3.27. Let $f(x, y) = ax^2 + bxy + cy^2$ be a quadratic form with discriminant D. Then $\left(a, \frac{b+\sqrt{D}}{2}\right)$ is a proper ideal of $\mathcal{O}$ [4]. Note that the right generator is exactly the quadratic form's root in the lower half plane multiplied by $-a$.

Lemma 3.28. *If M is a 2×2 matrix with real entries and let $\alpha \in \mathbb{C}$ and $M(\alpha, 1) = (x, y)$ then* $\operatorname{sign} \operatorname{Im} \frac{x}{y} = \operatorname{sign}(\det(M) \operatorname{Im} \alpha)$.

Proof. Let $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with $a, b, c, d \in \mathbb{R}$. Let $\alpha = n - mi$. We see that α is in the lower half plane. Consider:

$$M \begin{pmatrix} \alpha \\ 1 \end{pmatrix} = \begin{pmatrix} a\alpha + b \\ c\alpha + d \end{pmatrix}.$$

Consider the fraction $\frac{a\alpha+b}{c\alpha+d}$. If we subtract a complex number by its conjugate, we are left with twice the imaginary part. Proceeding,

$$\begin{aligned} \frac{a\alpha + b}{c\alpha + d} - \frac{a\bar{\alpha} + b}{c\bar{\alpha} + d} &= \frac{(a^2N(A) + bc\bar{\alpha} + ad\alpha + bd) - (a^2N(A) + bc\alpha + ad\bar{\alpha} + bd)}{c^2N(\alpha) + cdTr(\alpha) + d^2} \\ &= \frac{ad(\alpha - \bar{\alpha}) - bc(\alpha - \bar{\alpha})}{c^2N(\alpha) + cdTr(\alpha) + d^2} \\ &= \frac{\det(M)(\alpha - \bar{\alpha})}{c^2N(\alpha) + cdTr(\alpha) + d^2}. \end{aligned}$$

The denominator is precisely $N(c\alpha + d)$ so we only need consider the numerator. We know that $\alpha - \bar{\alpha}$ is in the lower half plane, so $\det(M)(\alpha - \bar{\alpha})$ is in the lower half plane only if $\det(M) > 0$. □

Theorem 3.29. *Definitions 3.26 and 3.27 define maps that form inverse bijections between ideal classes and classes of quadratic forms.*

Proof. We wish to show that the maps preserve the relationship of equivalence classes of quadratic forms. Let $f(x, y)$ and $g(z, w)$ be equivalent quadratic forms of discriminant D. Without loss of generality, assume $f(x, y)$ is reduced and primitive. Let $\alpha \in \mathbb{C}$ such that $f(\alpha, 1) = 0$. Assume α is in the lower half plane. Then, the associated ideal class to $f(x, y)$ is $(a, -a\alpha) = a(1, -\alpha) = (1, \alpha)$.

Since f and g are equivalent there is a matrix,

$$M = \begin{pmatrix} m & n \\ k & \ell \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}).$$

Then $m\ell - nk = 1$, and $f(x, y) = g(mx + ny, kx + \ell y)$ where $z = mx + ny$ and $w = kx + \ell y$. So,

$$0 = f(\alpha, 1) = g(m\alpha + n, k\alpha + \ell).$$

Notice that $k\alpha + \ell$ and $m\alpha + n$ are in $\mathbb{C}$. By Lemma 2.12 we have

$$\begin{aligned} 0 &= g(m\alpha + n, k\alpha + \ell) \\ 0 &= (k\alpha + \ell)^2 g\left(\frac{m\alpha + n}{k\alpha + \ell}, 1\right) \\ 0 &= g\left(\frac{m\alpha + n}{k\alpha + \ell}, 1\right). \end{aligned}$$

That is, $\frac{m\alpha+n}{k\alpha+\ell} = \frac{b+\sqrt{b^2-4ac}}{2a}$ for $a, b, c \in \mathbb{Z}$ where $g(z, w) = az^2 + bzw + cw^2$. Thus, the basis of the ideal in the ideal class associated to equivalent forms of $g(z, w)$ is

$$\left(1, \frac{m\alpha + n}{k\alpha + \ell}\right) = (k\alpha + \ell, m\alpha + n).$$

Lemma 3.28 tells us that $\frac{m\alpha+n}{k\alpha+\ell}$ is in the lower half plane since α is in the lower half plane. Notice that $k\alpha+\ell$ and $m\alpha + n$ are in the ideal generated by $(1, \alpha)$. Thus $(k\alpha + \ell, m\alpha + n) \subseteq (1, \alpha)$, because M is invertible. Further, $(k\alpha + \ell, m\alpha + n) = \frac{1}{k\alpha+\ell}\left(1, \frac{m\alpha+n}{k\alpha+\ell}\right) = \left(1, \frac{m\alpha+n}{k\alpha+\ell}\right)$ by scaling the ideal. Thus $\left(1, \frac{m\alpha+n}{k\alpha+\ell}\right) = (1, \alpha)$.

Now, let (α, β) be oriented generators of an ideal, $\mathscr{I}$. If (α', β') are oriented generators, by Lemma 3.28 we can find a linear transform that sends (α', β') to (α, β). Then, for an ideal, $\mathscr{J}$ in the same ideal class as

(α, β), there must be some λ such that $\lambda\mathscr{I} = \mathscr{J}$ Then, $(\lambda\alpha, \lambda\beta)$ generates $\mathscr{J}$. The associated quadratic form to $\mathscr{I}$ is

$$\frac{N(\alpha x + \beta y)}{N(\mathscr{I})},$$

and the associated quadratic form to $\mathscr{J}$ is

$$\frac{N(\lambda\alpha x + \lambda\beta y)}{N(\mathscr{J})} = \frac{N(\lambda(\alpha x + \beta y))}{N(\mathscr{J})}.$$

By Lemma 3.8 we write this as

$$\frac{N(\lambda)}{N(\mathscr{J})} N(\alpha x + \beta y).$$

We see that $\frac{N(\lambda)}{N(\mathscr{J})}$ and $\frac{1}{N(\mathscr{I})}$ are just scalars so the generated quadratic forms must be equivalent.

Let $f(x, y) = ax^2 + bxy + cy^2$. Then by Definition 3.27, $f(x, y)$ is mapped to the ideal $\left(a, \frac{b+\sqrt{D}}{2}\right)$. By Definition 3.26 the ideal $\left(a, \frac{b+\sqrt{D}}{2}\right)$ maps to the quadratic form given by

$$\begin{aligned}
\frac{N\left(ax + \frac{b+\sqrt{D}}{2}y\right)}{N(\mathscr{I})} &= \frac{1}{N(\mathscr{I})}\left(ax + \frac{b+\sqrt{D}}{2}y\right)\left(ax + \frac{b-\sqrt{D}}{2}y\right) \\
&= \frac{1}{N(\mathscr{I})}(a^2x^2 + abxy + acy^2) \\
&= \frac{a}{N(\mathscr{I})}(ax^2 + bxy + cy^2).
\end{aligned}$$

The forms $\frac{a}{N(\mathscr{I})}(ax^2 + bxy + cy^2)$ and $ax^2 + bxy + cy^2$ are identical except one has a scaling factor. Thus, they are equivalent forms. So, the map that sends quadratic form to ideal class back to quadratic form, is the identity map on quadratic forms. Going one step further, $\frac{-b-\sqrt{D}}{2a}$ is also a root of $\frac{a}{N(\mathscr{I})}(ax^2+bxy+cy^2)$ when $y = 1$. Thus the ideal generated by $\left(a, \frac{b+\sqrt{D}}{2}\right)$ is associated with the quadratic form $\frac{a}{N(\mathscr{I})}(ax^2+bxy+cy^2)$. So, the mapping from ideal to quadratic back to ideal is the identity map on ideal classes.

Therefore, there is a bijection between the ideal class groups of discriminant D and classes of quadratic forms. □

Now that we have built a bijection between ideal class groups and classes of quadratic forms, it is surprisingly simple to prove the group structure.

Theorem 3.30. *Classes of quadratic forms of discriminant D form an Abelian group under Dirichlet composition.*

Proof. By 3.29 we see there is a bijection between ideal classes and classes of quadratic forms. Ideal class groups form Abelian groups, thus classes of quadratic forms must form Abelian groups. □

Definition 3.31. The identity element of a set of classes of primitive quadratic forms of discriminant D is,

$$\begin{aligned}
f(x, y) &= x^2 - \frac{D}{4}y^2 \qquad \text{for } D \equiv 0 \bmod 4, \text{ or} \\
f(x, y) &= x^2 + xy - \frac{1-D}{4}y^2 \qquad \text{for } D \equiv 1 \bmod 4.
\end{aligned}$$

We call this form the **principal** form.

Lemma 3.32. *Given a quadratic form $f(x, y) = ax^2 + bxy + cy^2$, the inverse under composition is $ax^2 - bxy + cy^2$.*

Proof. Consider the Dirichlet composition. Let $f(x,y) = ax^2 + bxy + cy^2$ be a primitive quadratic form with discriminant D. Then $g(x,y) = ax^2 - bxy + cy^2$ is also a primitive form since by definition of a primitive quadratic form, $\gcd(a,b,c) = 1$. We cannot compose $f(x,y)$ with $g(x,y)$ since $\gcd(a,a) = a$ and a need not be 1. Consider the equivalent form $h(x,y) = cx^2 + bxy + ay^2 = g(y,-x)$. Then we have $\gcd\left(a, c, \frac{b+b}{2}\right) = \gcd(a,c,b) = 1$. That is $e = 1$ from Lemma 3.1. We may find B from Lemma 3.1 to be $B = b$ if we take Legendre's reduction of a primitive quadratic form $|b| < a < c$ and $b^2 = D + 4ac$ (see Lemma 2.24). So, the composition of $f(x,y)$ with $h(x,y)$ is

$$F(x,y) = acx^2 + bxy + \frac{b^2 - D}{4ac}y^2 = acx^2 + bxy + y^2.$$

Recall that the principal form can be written primitively as

$$f(x,y) = x^2 - \frac{D}{4}y^2 \qquad \text{for } D \equiv 0 \bmod 4, \text{ or}$$
$$f(x,y) = x^2 + xy - \frac{1-D}{4}y^2 \qquad \text{for } D \equiv 1 \bmod 4,$$

by Definition 3.31. Using the equivalent form of $F_0(x,y) = F(y,-x) = x^2 - bxy + acy^2$ notice that $\gcd(1,b,ac) = 1$. Thus F_0 is a primitive form. Again using Lagrange's reduction, assume this form reduces such that $|b| \leq a = 1$. If $b = 0$ we see we have $D = -4ac$ so $F_0(x,y) = x^2 - \frac{D}{4}y^2$ as desired. If $b = 1$ then $D = 1 - 4ac$ and satisfies $F_0(x,y) = x^2 - xy + \frac{1-D}{4}y^2$. The identity is it's own inverse, so the $-xy$ term presents no issue. If $b = -1$ then $D = 1 - 4ac$ and satisfies $F_0(x,y) = x^2 + xy + \frac{1-D}{4}y^2$ as desired. □

3.4 Example and the Composition Law

To make the previous section clearer, here we will work through an example and generate the unique quadratic forms associated with the ring of integers $\mathbb{Z}\left[\sqrt{-14}\right]$. Since $-14 \equiv 3 \pmod 4$ the ring $\mathbb{Z}\left[\sqrt{-14}\right]$ has discriminant $4 \cdot -14 = -56$. Therefore we are looking for all forms of the discriminant -56. We will search for these forms using theorem 2.25. Recall $|b| \leq a \leq c$ by lemma 2.24. Now consider the discriminant,

$$\begin{aligned} -56 &= b^2 - 4ac \\ 56 &= 4ac - b^2 \\ &=\geq 4b^2 - b^2 \\ &= 3b^2 \\ \sqrt{56/3} &\geq |b| \\ |b| &\leq 4.3, \end{aligned}$$

where the inequality on the third line is true since $|b| \leq a \leq c$. There are finitely many possibilities of b to check. Recall the discriminant, $56 = 4ac - b^2$, rearranged to $56 + b^2 = 4ac$. The right hand side is even, so the left hand side must be even as well. Therefore b is even and $b = -4, -2, 0, 2, 4$. Now we consider each of these cases.

(i) If $b = -4$ then $18 = ac$. So $ac = 2 \cdot 9$ or $ac = 3 \cdot 6$. However none of these are valid for $|b| \leq a \leq c$.

(ii) If $b = -2$ then $15 = ac$. So $ac = 3 \cdot 5$. Thus our quadratic form is $3x^2 - 2xy + 5y^2$.

(iii) If $b = 0$ we have $14 = ac$. So $ac = 2 \cdot 7$ or $ac = 1 \cdot 14$. Thus the quadratic forms are $2x^2 + 7y^2$ and $x^2 + 14y^2$.

(iv) If $b = 2$ then $15 = ac$. So $ac = 3 \cdot 5$. Thus our quadratic form is $3x^2 + 2xy + 5y^2$.

(v) If $b = 4$ then $18 = ac$. So $ac = 2 \cdot 9$ or $ac = 3 \cdot 6$. However none of these are valid for $|b| \leq a \leq c$.

We have found four distinct quadratic forms and we can quickly plot these on the topograph to check that no two of them are properly equivalent.

This implies that there are 4 ideal classes in $Cl\left(\mathbb{Q}\left[\sqrt{-14}\right]\right)$.

The ideals associated with each form are:

Quadratic Form	Ideal Generators
x^2+14y^2	$(1,\sqrt{-14})$
$2x^2+7y^2$	$(2,\sqrt{-14})$
$3x^2+2xy+5y^2$	$(3,1+\sqrt{-14})$
$3x^2-2xy+5y^2$	$(3,-1+\sqrt{-14})$

Now all that remains is to multiply the ideals to find the group structure. We see that x^2+14y^2 is the principal form. That is it is the identity element of the group. We see this is true since one of the ideal generators is 1, so every ideal multiplied by it will remain unchanged. By lemma 3.32, $3x^2+2xy+5y^2$ and $3x^2-2xy+5y^2$ are inverses. So we only need check what happens when composing $2x^2+7y^2$. First consider this form composed with itself:

$$\begin{aligned}(2,\sqrt{-14})(2,\sqrt{-14}) &= (4,2\sqrt{-14},-14)\\ &= (4,2\sqrt{-14},-14,4\cdot 4-14)\\ &= (2,2\sqrt{-14})\\ &= 2(1,\sqrt{-14}).\end{aligned}$$

So this form is also a self inverse. Now consider $2x^2+7y^2$ composed with $3x^2+2xy+5y^2$:

$$\begin{aligned}(2,\sqrt{-14})(3,1+\sqrt{-14}) &= (6,2+2\sqrt{-14},3\sqrt{-14},-14+\sqrt{-14})\\ &= (6,2+2\sqrt{-14},3\sqrt{-14},-14+\sqrt{-14},2+2\sqrt{-14}-3\sqrt{-14})\\ &= (6,2+2\sqrt{-14},3\sqrt{-14},-14+\sqrt{-14},-2+\sqrt{-14})\\ &= (6,2+2\sqrt{-14},3\sqrt{-14},-2+\sqrt{-14})\\ &= (6,3(2+2\sqrt{-14})-2\cdot 3\sqrt{-14},2+2\sqrt{-14},3\sqrt{-14},-2+\sqrt{-14})\\ &= (2+2\sqrt{-14},3\sqrt{-14},-2+\sqrt{-14})\\ &= (2+2\sqrt{-14},3\sqrt{-14},-2+\sqrt{-14},-1(2+2\sqrt{-14})+3\sqrt{-14})\\ &= (2+2\sqrt{-14},3\sqrt{-14}).\end{aligned}$$

We cannot immediately see the corresponding quadratic form, so we map this to the corresponding quadratic.

$$\frac{1}{N((2+2\sqrt{-14},3\sqrt{-14}))}N((2+2\sqrt{-14})x+(3\sqrt{-14})y)=10x^2+28xy+21y^2.$$

We reduce this form using the topograph. Traveling down to a well we get $5x^2+2xy+3y^2$ or $3x^2-2xy+5y^2$.

By a similar calculation we see that $3x^2-2xy+5y^2$ composed with $2x^2+7y^2$ results in $3x^2+2xy+5y^2$.

The final compositions we have to check are $3x^2+2xy+5y^2$ with itself and $3x^2-2xy+5y^2$ with itself. Consider,

$$\begin{aligned}(3,1+\sqrt{-14})(3,1+\sqrt{-14}) &= (9,3+3\sqrt{-14},-13+2\sqrt{-14})\\ &= (9,3+3\sqrt{-14},-13+2\sqrt{-14},5+2\sqrt{-14})\\ &= (3+3\sqrt{-14},-13+2\sqrt{-14},5+2\sqrt{-14})\\ &= (3+3\sqrt{-14},5+2\sqrt{-14}).\end{aligned}$$

Again, we do not immediately see the corresponding quadratic form, so we map it to the corresponding quadratic.

$$\frac{1}{N((3+3\sqrt{-14},5+2\sqrt{-14}))}N((3+3\sqrt{-14})x+(5+2\sqrt{-14})y)=15x^2+22xy+9y^2.$$

Reducing this form on the topograph by travelling down to a well, we find $2x^2+7y^2$. Similarly we find that $3x^2-2xy+5y^2$ composed with itself also gives us $2x^2+7y^2$.

We are ready to build a table of the group structure.

	x^2+14y^2	$2x^2+7y^2$	$3x^2+2xy+5y^2$	$3x^2-2xy+5y^2$
x^2+14y^2	x^2+14y^2	$2x^2+7y^2$	$3x^2+2xy+5y^2$	$3x^2-2xy+5y^2$
$2x^2+7y^2$	$2x^2+7y^2$	x^2+14y^2	$3x^2-2xy+5y^2$	$3x^2+2xy+5y^2$
$3x^2+2xy+5y^2$	$3x^2+2xy+5y^2$	$3x^2-2xy+5y^2$	$2x^2+7y^2$	x^2+14y^2
$3x^2-2xy+5y^2$	$3x^2-2xy+5y^2$	$3x^2+2xy+5y^2$	x^2+14y^2	$2x^2+7y^2$

This group structure is identical to the group structure of $\mathbb{Z}/4\mathbb{Z}$.

4 The Composition Law on the Topograph

Gauss was the first to outline a composition law on quadratic forms. The quadratics of a discriminant form a group. Given two quadratics of the same discriminant, we can compose them and achieve a third quadratic form. By multiplying the generators of the ideal representing each quadratic, the resulting product will contain the generators of the ideal representing the composed quadratic.

In the previous two sections, we have established bijections between quadratic forms and the topograph, and between quadratic forms and the ideals of the quadratic field. Therefore, there must be some bijection between the ideals of the quadratic field and the topograph. Furthermore, there should be a way to view the composition law and perform it directly on the topograph.

4.1 The Ideal Topograph

One method explored was the creation of an ideal topopgraph.

Given an ideal generated by $(1, q)$ where q is the root of the associated quadratic, we can build a similar topograph to the domain and range topographs constructed in Section 2.

Definition 4.1. The **ideal topograph** labels the faces with a generator of the ideal. For each edge on the topograph, the two generators generate the ideal.

Given an edge with two faces, we can generate a third and fourth face by adding and subtracting the generators as we might for the domain topograph.

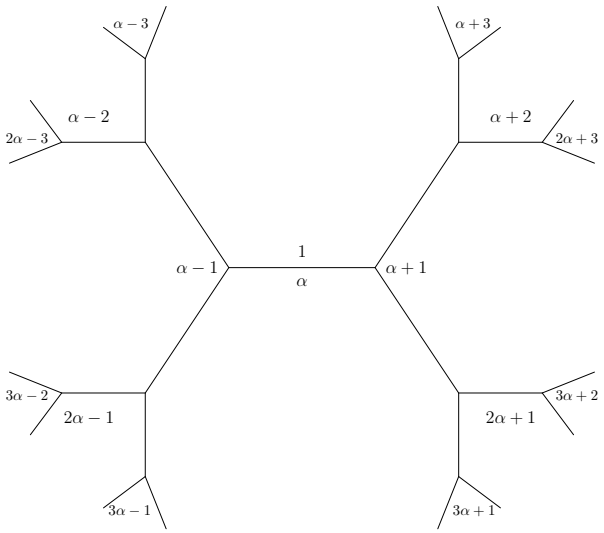

Figure 8: The Ideal Topograph

We can further add to this image by considering the norms of each ideal, similar to the range topograph we constructed in Section 2.

We wish to see which faces we would get by multiplying generators of ideals. Consider the ideals in $\mathbb{Z}\left[\sqrt{-5}\right]$. The discriminant is -20 and the class number is 2. So, there are two classes of quadratic forms represented by x^2+5y^2 and $2x^2+2xy+3y^2$, with associated ideal classes given by $(1,\sqrt{-5})$ and $\left(1,\frac{1+\sqrt{-5}}{2}\right)=\left(2,1+\sqrt{-5}\right)$ respectively.

We can build the multiplication table of this group structure very easily.

	x^2+5y^2	$2x^2+2xy+3y^2$
x^2+5y^2	x^2+5y^2	$2x^2+2xy+3y^2$
$2x^2+2xy+3y^2$	$2x^2+2xy+3y^2$	x^2+5y^2

The ideal topograph of $(1,\sqrt{-5})$ is exactly Figure 8 with $\alpha=\sqrt{-5}$. Let us examine the ideal topograph given by $\left(2,1+\sqrt{-5}\right)$ shown in Figure 9.

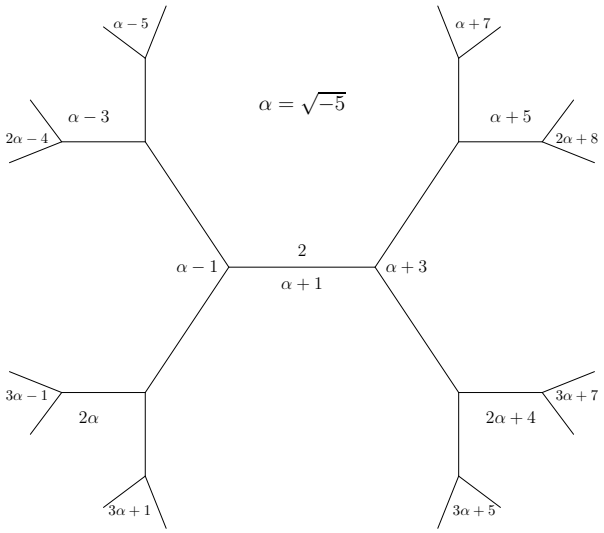

Figure 9: The Ideal Topograph of $(2,1+\alpha)$ with $\alpha=\sqrt{-5}$

The non trivial composition in this group is $2x^2+2xy+3y^2$ with itself. Let $\alpha=\sqrt{-5}$ and consider multiplying the ideals,

$$(2,1+\sqrt{\alpha})(2,1+\sqrt{\alpha})=(4,2,2\alpha+2,2\alpha-4)$$

We see that 2 and $2+2\alpha$ generate an ideal. We draw the ideal topograph generated by $(2,2+2\alpha)$ in Figure 10.

Every generator we found in calculating the composition can be found directly on the topograph in Figure 10. We selected 2 and $2\alpha+2$ as a starting basis for the topograph so both naturally occur in the center of our image. The other two also appear; 6 is a multiple of 2 and $2\alpha-4$ is found in the upper left branch of our image. Any two generators on the topograph in Figure 9 that share an edge generate the ideal and can be multiplied with any other edge in the same topograph to get a similar composition. So, would we find more faces in Figure 10 if we used any of the other infinitely many compositions?

After computing a couple hundred products of generators, we find every face shown in Figure 10. It would seem that every face in Figure 10 can be found by composing edges of Figure 9.

Proposition 4.1. *Given two ideal topographs, the compositions of every edge between both topographs of four generators draw every face on the composed ideal topograph.*

With the product of $(2,2+2\alpha)$ with itself, it seems that it was extremely lucky 2 and $2\alpha+2$ were immediately found to generate the ideal. Some pairs of generators immediately give a generator of the new ideal. Most pairs seem to provide a random scatter of faces across the composed topograph. We hope that there is a "correct" selection of two edges, however we were unable to determine this.

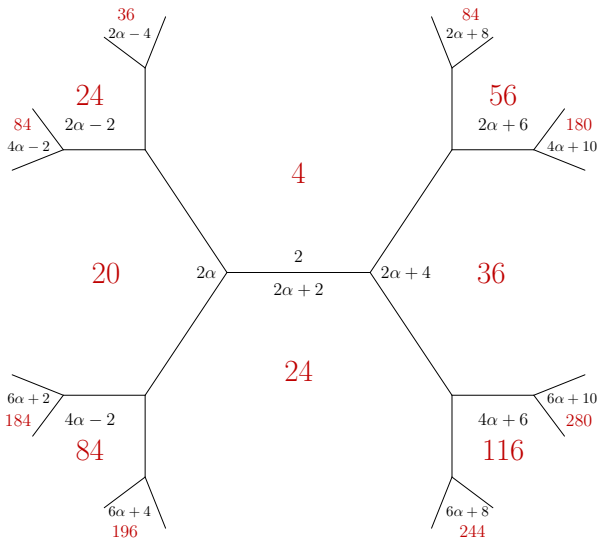

Figure 10: The Ideal Topograph of $(2, 2+2\alpha)$ with $\alpha = \sqrt{-5}$ with the norm topograph drawn on top in red.

4.2 Dirchelt and Trifkovic on Topograph

It is perhaps more promising if we consider performing a composition directly on the range topograph by attempting to understand Dirichlet's composition.

Recall 3.1 which defines a value B. Remember that given a form $ax^2 + bxy + cy^2$, b is found on the topograph as the h value described in 2.15.

Lemma 4.2. *If $f(x, y) = ax^2 + bxy + cy^2$ and $g(x, y) = a'x^2 + b'xy + c'y^2$ be primitive quadratic forms with discriminant D and $b = b'$ then $b \equiv B \mod \frac{4aa'}{e^2}$.*

Proof. Given that f and g are primitive, we have $e = \gcd(a, a', b) = 1$. It is necessarily true that $b \equiv b \mod 2a$ and $b \equiv b' \mod 2a'$. So all we need to show is $b^2 \equiv D \mod 4aa'$. By definition $D = b^2 - 4ac$. Therefore $b^2 = D + 4ac$. So, if $b^2 \equiv D = b^2 - 4ac \mod 4aa'$ then $a'b^2 \equiv a'b^2 - 4aa'c \mod 4aa'$ and we see $a'b^2 \equiv a'b^2 \mod 4aa'$. □

It seems that if we can find two faces a and a' on the topograph such that $\gcd(a, a') = 1$ and find two edges along those faces that have a shared value h, we can then preform a composition at that edge.

Recalling the form that the Dirichlet composition gives us,

$$F(x, y) = \frac{aa'}{e}x^2 + Bxy + \frac{B^2 - D}{4aa'}y^2,$$

finding $B = h = h'$, a, and a' is intuitive to do on the topograph. We see that with $B = h = h'$, e is 1, so the composed form will be,

$$F(x, y) = aa'x^2 + Bxy + \frac{B^2 - D}{4aa'}y^2.$$

The values for the coefficient on x^2 and xy are easy and "nice" to see on the topograph, however $\frac{B^2-D}{4aa'}$ is not something we can easily see.

We have a possible composition interpretated on the topograph, but the last coefficient is not intuitive and is a rather dissatisfying solution.

Proposition 7.11.5 in Trifković [7] gives a new potential avenue:

Theorem 4.3. *[7] Any two $SL_2(\mathbb{Z})$-equivalence classes of quadratic forms of discriminant D_F have representatives $a_1x^2 + bxy + cy^2$ and $a_2x^2 + bxy + c_2y^2$, with $gcd(a_1, a_2) = 1$. We say that two such quadratic*

forms are ***united****. Put* $c = gcd(c_1, c_2)$*. Then* $c_1 = ca_2$*,* $c_2 = ca_1$*, and the composition of the classes is given by*

$$\left[a_1x^2 + bxy + (ca_2)y^2\right]\left[a_2x^2 + bxy + ca_1y^2\right] = \left[(a_1a_2)x^2 + bxy + cy^2\right].$$

This is a modification of the Dirichlet composition. We have similar conditions as above with finding $B = h = h'$ and $\gcd(a, a') = 1$. However we have a new way of calculating the final coefficient as $c = \gcd(c_1, c_2)$ with $c_1 = ca_2$, $c_2 = ca_1$. Then our composed form is

$$F(x, y) = a_1a_2x^2 + h_1xy + cy^2.$$

This is not quite as convoluted as the final term when interpreting Dirichlet composition and is slightly easier to notice as a relationship on topographs. But it still is not the satisfying solution we were hoping for.

Acknowledgements

Many thanks to my advisor Professor Jonathan Wise for his patience, discussions, and encouragement. He has taught me so much about algebra, number theory, and just general mathematics. This project has been a unique and wonderful part of my undergraduate experience.

5 References

[1] Michael Artin. *Algebra*. 2nd. Pearson India Education Services Pvt.Ltd, 2015. ISBN: 9789332549838.

[2] Florian Bouyer. *Composition and Bhargava's Cubes*. URL: https://warwick.ac.uk/fac/sci/maths/people/staff/fbouyer/gauss_composition.pdf.

[3] John H. Conway. *The Sensual Quadratic Form*. Vol. 26. Carus Mathematical Monographs. The Mathematical Association of America, 1997. URL: https://www.maths.ed.ac.uk/~v1ranick/papers/conwaysens.pdf.

[4] David A. Cox. *Primes of the Form* $x^2 + ny^2$*: Fermat, Class Field Theory, and Complex Multiplication*. John Wiley & Sons, Inc., Hoboken, New Jersey, 2013. ISBN: 9781118390184.

[5] Carl Friedrich Gauss. *Disquisitiones Arithmeticae*. Springer-Verlag New York Berlin Heidelberg Tokyo, 1966. ISBN: 0387962549.

[6] Jeremy Gray. *A History of Abstract Algebra*. Springer Nature Switzerland AG., 2018. ISBN: 9783319947730.

[7] Mak Trifković. *Algebraic Theory of Quadratic Numbers*. Springer Scienc+Business Media New York, 2013. ISBN: 9781461477174.

[8] Martin H. Weissman. *An Illustrated Theory of Numbers*. American Mathematical Society, Providence, Rhode Island, 2017. ISBN: 9781470434939.

[9] Melanie Matchett Woods. "Gauss composition over an arbitrary base". In: *Adances in Mathematics* 226.2 (2011), pp. 1756–1771. DOI: https://doi.org/10.1016/j.aim.2010.08.018.