5-2009

Binary Quadratic Forms over F[T] and Principal Ideal Domains

Jeff Beyerl
Clemson University, J_Beyerl@hotmail.com

Binary Quadratic Forms over $\mathbb{F}[T]$ and Principal Ideal Domains

---

A Masters Thesis
Presented to
the Graduate School of
Clemson University

In Partial Fulfillment
of the Requirements for the Degree
Masters of Science
Mathematics

---

by
Jeffrey J. Beyerl
May 2009

Accepted by:
Drs. Kevin James, Hui Xue, Committee Chairs
Hiren Maharaj

Abstract

This paper concerns binary quadratic forms over $\mathbb{F}[T]$. It develops theory analogous to the theory of binary quadratic forms over $\mathbb{Z}$. Most although not all of the results are almost identical, while some of the proofs require different techniques.

In particular, the form class group is determined when the form takes values in a principal ideal domain, and the ideal class group (and class group isomorphism) is determined when the form takes values in $\mathbb{F}[T]$.

Table of Contents

Chapter 1

Introduction

Polynomial functions, such as $\sum_{i_1,i_2,\ldots,i_n \geq 0} a_{i_1,i_2,\ldots,i_n} x_1^{i_1} \cdots x_n^{i_n}$, have been studied since long ago. Quadratic forms are a particular kind of polynomial equation of particular interest. A quadratic form is a polynomial in which the total degree of each term ($i_1 + i_2 + \cdots + i_n$ above) is two. Quadratic forms have been studied in various dimensions (number of different independent variables) and over various settings (the ring the variables take values from). In particular there is an extensive theory for quadratic forms over $\mathbb{Q}, \mathbb{Q}_p$ as well as over arbitrary fields. Cassels text [1] provides an in depth treatment of forms over $\mathbb{Q}$ and $\mathbb{Q}_p$. Chapter 15 of [5] also provide a classification of equivalent forms and genera over $\mathbb{Z}$ and $\mathbb{Z}_p$. O'Meara's text [7] provides a treatment of forms over fields, as well as some theory over more general rings. Springer's Online Reference Works [6] gives a short summary of many of the general results.

The primary direction for this work is analogous to the material on binary quadratic forms over $\mathbb{Z}$ found in [2]. Many of the theorems hold true over an arbitrary PID or more specifically $\mathbb{F}[T]$, although some of the proof methods require more attention.

Chapter 2

Definitions and Notation

2.1 Quadratic Forms

Let A be any Principal Ideal Domain in which $2 \in A$ is a unit. A binary quadratic form, or just form for short, is a function of the form

$$f(x,y) = ax^2 + bxy + cy^2 = \begin{bmatrix} x & y \end{bmatrix} \begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} =: [a,b,c] \in A[x,y].$$

Above, a will occasionally be referred to as the "first coefficient" and similarly b and c as the "second" and "third" coefficients respectively. f is said to be primitive when $\langle a,b,c \rangle_A := \{\alpha a + \beta b + \gamma c | \alpha, \beta, \gamma \in A\} = A = \langle 1 \rangle_A$. The discriminant of f is $Disc(f) = b^2 - 4ac$. Given $a, b, D = Disc(f)$, c is uniquely determined, and so f will occasionally be denoted by $f = [a,b,*]_D$.

An element $m \in A$ is said to be represented by f if there exists $x, y \in A$ such that $f(x,y) = m$. Such m is said to be properly represented by f when we also have $\langle x,y \rangle_A = \langle 1 \rangle_A$.

The set of all primitive forms will be denoted $Q(*) := \{f | f \text{ is a primitive form}\}$, and those with a given discriminant $Q(D) := \{f | f \text{ is a primitive form, } Disc(f) = D\}$. Further, the group $GL_2(A)$ acts on $Q(*)$ and $SL_2(A)$ acts on $Q(D)$, the set of all primitive forms of fixed discriminant,

(see [A.1]) via the group action with operation denoted by juxtaposition and defined by

$$\begin{aligned}
\gamma f = \begin{bmatrix} p & q \\ r & s \end{bmatrix} f &\mapsto f(px+qy, rx+sy) \\
&= \begin{bmatrix} x & y \end{bmatrix} \gamma^{\mathrm{T}} \begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix} \gamma \begin{bmatrix} x \\ y \end{bmatrix} \\
&= \begin{bmatrix} x & y \end{bmatrix} \begin{bmatrix} p & q \\ r & s \end{bmatrix}^{\mathrm{T}} \begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix} \begin{bmatrix} p & q \\ r & s \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}.
\end{aligned}$$

We obtain an equivalence relation: $f \backsim g$ iff there exist $\gamma \in GL_2(A)$ such that $\gamma f = g$ (see [A.2]). We say that f is <u>properly equivalent</u> with g if $\gamma \in SL_2(A)$, and write $f \backsim g$, which is also the equivalence relation induced by the subgroup $SL_2(A)$ acting on $Q(*)$ (see [A.3]). Define

$$Q(D)/\backsim := \{[f] \in Q(*)/\backsim \, | Disc(f) = D, \, f \text{ is primitive}\}.$$

Two forms f_1, f_2 with the same discriminant are said to be <u>concordant</u> if they can be written as $f_1 = [a_1, B, a_2C]$ and $f_2 = [a_2, B, a_1C]$ where $a_1, a_2, B, C \in A$. We also define a binary operation on concordant forms, defined by $f * g := [a_1a_2, B, C]$, and call it the <u>composition of f and g</u>.

Chapter 3

Preliminaries

3.1 Introduction

In this chapter we lay the technical foundation and present results required for the next chapter. All these results should hold in any principal ideal domain. In fact most will hold true more generally, with the limiting factor being Lemma 3.2.4.

3.2 Some Lemmas On Quadratic Forms

Lemma 3.2.1 *With* $f = [a, b, c] \in Q(*)$, *and* $p, q, r, s \in A$, *then* $\begin{bmatrix} p & q \\ r & s \end{bmatrix} f = [f(p, r), 2apq + bqr + bps + 2crs, f(q, s)]$. *(Regardless of whether or not* $\begin{bmatrix} p & q \\ r & s \end{bmatrix}$ *is in* $GL_2(A)$, *or* $SL_2(A)$ *or not).*

Proof:

$$\begin{aligned}
\begin{bmatrix} p & q \\ r & s \end{bmatrix} f &= \begin{bmatrix} x & y \end{bmatrix} \begin{bmatrix} p & r \\ q & s \end{bmatrix} \begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix} \begin{bmatrix} p & q \\ r & s \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \\
&= \begin{bmatrix} x & y \end{bmatrix} \begin{bmatrix} pa + br/2 & pb/2 + rc \\ qa + bs/2 & qb/2 + sc \end{bmatrix} \begin{bmatrix} p & q \\ r & s \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \\
&= \begin{bmatrix} x & y \end{bmatrix} \begin{bmatrix} p^2a + bpr/2 + pbr/2 + r^2c & pqa + bqr/2 + pbs/2 + rcs \\ pqa + pbs/2 + qbr/2 + scr & q^2a + bqs/2 + qbs/2 + s^2c \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \\
&= \begin{bmatrix} x & y \end{bmatrix} \begin{bmatrix} ap^2 + bpr + cr^2 & apq + bqr/2 + bps/2 + crs \\ apq + bqr/2 + bps/2 + crs & aq^2 + bqs + cs^2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \\
&= \begin{bmatrix} x & y \end{bmatrix} \begin{bmatrix} f(p,r) & b'/2 \\ b'/2 & f(q,s) \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \\
&= [f(p,r), 2apq + bqr + bps + 2crs, f(q,s)].
\end{aligned}$$

■

Lemma 3.2.2 *$m \in A$ is properly represented by $f(x,y) = [a,b,c] \in Q(*)$ if and only if there exists $b', c' \in A$ such that $f \backsim [m, b', c']$. That is, f is properly equivalent to a form with m as the first coefficient.*

Proof: ($\Rightarrow$) Suppose $f(p,r) = m$ with $\langle p, r \rangle_A = \langle 1 \rangle_A$. Then there exists $q, s \in A$ such that $ps - qr = 1$. So

$$\begin{bmatrix} p & q \\ r & s \end{bmatrix} f = [f(p,r), b', f(r,s)] = [m, b', c'],$$

(see [3.2.1]) so that indeed $f \backsim [m, b', c']$.

($\Leftarrow$) Clearly $[m, b', c']$ properly represents m. Write $\gamma f = f(px + qy, rx + sy) = [m, b', c']$, where $\gamma = \begin{bmatrix} p & q \\ r & s \end{bmatrix} \in SL_2(A)$. Then $m = f(p \cdot 1 + q \cdot 0, r \cdot 1 + s \cdot 0) = f(p,r)$ Now $\langle p, r \rangle_A = \langle 1 \rangle_A$ because $ps - qr = 1$. Thus f also properly represents m. ■

Lemma 3.2.3 *Equivalent forms represent the same things. Likewise if $f \backsim g$ then f and g properly represent the same elements of A.*

Proof: Suppose f and g are equivalent. Then write $\gamma f = g$, $\gamma \in GL_2(A)$. If g represents m via $g(b_1, b_2) = m$, then f represents m via $\begin{bmatrix} x' & y' \end{bmatrix} = \begin{bmatrix} b_1 & b_2 \end{bmatrix} \gamma$, so we have $f(x', y') = m$.

For the second part, suppose $f \backsim g$, and suppose f properly represents $m \in A$. Then by Lemma 3.2.2, we know that $[m, b', c'] \backsim f \backsim g$ for some $b', c' \in A$. Hence $[m, b', c'] \backsim g$, and so again by Lemma 3.2.2 g properly represents m. ■

The next lemma is tricky. It is necessary for our construction of certain forms later, yet requires a setting in which $a, b \in A$ not sharing a common factor implies that $\langle a, b \rangle_A = \langle 1 \rangle_A$.

Lemma 3.2.4 *Let $M \in A \smallsetminus \{0\}$, and $f \in Q(*)$. Then there exists $r, s \in A, \langle r, s \rangle_A = \langle 1 \rangle_A$ such that $\langle f(r, s), M \rangle_A = \langle 1 \rangle_A$.*

Proof: We shall find $r, s \in A$ with $\langle r, s \rangle_A = \langle 1 \rangle_A$ so that $\langle f(r, s), M \rangle_A = \langle 1 \rangle_A$. Write $M = \prod_i m_i \prod_j p_j \prod_k q_k$ where m_i, p_i, q_k are all irreducible, and

$$m_i \nmid a,$$

$$p_j | a, \quad p_j \nmid c,$$

$$q_k | a, \quad q_k | c, \quad q_k \nmid b.$$

There are no other possible irreducible divisors, because f is primitive. Setting $r = \prod_j p_j$ and $s = \prod_i m_i$ we are done after a little bit of work (see [A.6]). ■

Lemma 3.2.5 *Fix $M \in A \smallsetminus \{0\}$. Let $f = [a, b, c] \in Q(*)$. Then f is properly equivalent to a form $[a', b', c']$ where $\langle a', M \rangle_A = \langle 1 \rangle_A$.*

Proof: Apply 3.2.4 to obtain a properly represented a' with $\langle a', M \rangle_A = \langle 1 \rangle_A$. Then apply Lemma 3.2.2 to place a' as the first coefficient of f. ■

Lemma 3.2.6 *Let $D \in A, M \in A \smallsetminus \{0\}, \mathcal{C}_1, \mathcal{C}_2 \in Q(D)/\backsim$. Then there is an $f_1 = [a, b, c] \in \mathcal{C}_1$ and $f_2 = [a', b', c'] \in \mathcal{C}_2$ such that $\langle a, a' \rangle_A = \langle 1 \rangle_A$, $\langle aa', N \rangle_A = \langle 1 \rangle_A$ and $aa' \neq 0$.*

Proof: Let $f_1 = [a, b, c] \in \mathcal{C}_1$ and $g = [\alpha, \beta, \gamma] \in \mathcal{C}_2$. If $a = 0$, replace f by a properly equivalent form with nonzero x^2 coefficient via Lemma 3.2.2. Apply Lemma 3.2.5 to f so that we may assume $\langle a, M \rangle_A = \langle 1 \rangle_A$. Now apply Lemma 3.2.5 to g to find $g_2 = [a', b', c'] \backsim g$ with $\langle a', aM \rangle_A = \langle 1 \rangle_A$. We are now done because $\langle a', aM \rangle_A = \langle 1 \rangle_A$ implies $\langle a, a' \rangle_A = \langle 1 \rangle_A$, and both $\langle a, M \rangle_A = \langle 1 \rangle_A$ & $\langle a', aM \rangle_A = \langle 1 \rangle_A$ together imply that $\langle aa', M \rangle_A = \langle 1 \rangle_A$. ■

Lemma 3.2.7 *If two forms $f_1 = [a_1, b, c_1], f_2 = [a_2, b, c_2]$ have the same discriminant, $a_1 a_2 \neq 0$, $\langle a_1, a_2 \rangle_A = \langle 1 \rangle_A$, and $a_1 | c_2, a_2 | c_1$, then f and g are concordant.*

Proof: Write $c_2 = a_1 n_1$ and $c_1 = a_2 n_2$. Then $D = b^2 - 4a_1 a_2 n_1 = b^2 - 4a_1 a_2 n_2$. Hence $a_1 a_2 n_1 = a_1 a_2 n_2$ and so $n_1 = n_2$. Define $c := n_1 = n_2$. Thus we have that $f_1 = [a_1, b, a_2 c], f_2 = [a_2, b, a_1 c]$ and so f_1 and f_2 are concordant. ■

We now have enough to prove the next result, which will eventually allow us to define an operation on $Q(D)/\backsim$.

Proposition 3.2.8 *Let $D \in A$, $M \in A \smallsetminus \{0\}, \mathcal{C}_1, \mathcal{C}_2 \in Q(D)/\backsim$. Then there are $f_1 \in \mathcal{C}_1$ and $f_2 \in \mathcal{C}_2$ such that*

$$f_1 = [a_1, B, a_2 C], \quad f_2 = [a_2, B, a_1 C]$$

where $a_i, B, C \in A$ $a_1 a_2 \neq 0$, $\langle a_1, a_2 \rangle_A = \langle 1 \rangle_A$, and $\langle a_1 a_2, M \rangle_A = \langle 1 \rangle_A$. That is, there are two concordant forms with $\langle a_1, a_2 \rangle_A = \langle 1 \rangle_A$ and $\langle a_1 a_2, M \rangle_A = \langle 1 \rangle_A$.

Proof: As in Lemma 3.2.6, choose $f_1 = [a, b, c] \in \mathcal{C}_1, f_2 = [a', b', c'] \in \mathcal{C}_2$ so that $\langle a, a' \rangle_A = \langle 1 \rangle_A$ and $\langle aa', M \rangle_A = \langle 1 \rangle_A$. Choose $n, n' \in A$ so that $an - a'n' = \frac{b'-b}{2}$. Then write $B := 2an + b = 2a'n' + b'$ so $\frac{B}{2} = an + \frac{b}{2} = a'n' + \frac{b'}{2}$, and $C = \frac{B^2 - D}{4aa'} \in A$ (see [A.4]). Then we compute

$$\begin{bmatrix} 1 & 0 \\ n & 1 \end{bmatrix} f_1 = [a, B, a'C], \text{ and}$$

$$\begin{bmatrix} 1 & 0 \\ n & 1 \end{bmatrix} f_2 = [a', B, aC]$$

(see [A.5]). Denote $a_1 = a$ and $a_2 = a'$ and we are done. ■

Definition 3.2.9 *We shall now define an operation on $Q(D)/\backsim$, represented by juxtaposition, and defined by*

$$\mathcal{C}_1 \mathcal{C}_2 := \mathcal{C}$$

where $[f * g] \in \mathcal{C}$ with the notation from above. That is, if $f_1 \in \mathcal{C}_1, f_2 \in \mathcal{C}_2$ are two concordant forms, then $[f_1][f_2] = [f_1 * f_2]$.

We will prove (4.2.2) that this operation is well defined.

Chapter 4

Main Results

4.1 Introduction

This chapter contains the main results of this paper. In the second section will determine the Form Class Group $Q(D)/\backsim$. That is, the group of proper equivalence classes in $Q(*)$. We prove that it is a group, using a method analogous to that over $\mathbb{Z}$ by Flath in chapter 5 of [3]. In the third section we will specialize to $\mathbb{F}[T]$ and discuss some developments new to the introduction of an independent variable to our coefficients. In the fourth section we discuss orders and define the ideal class group. In the fifth section we show that the two class groups are isomorphic: $Q(D)/\backsim \cong I(\mathcal{O})/P(\mathcal{O})$ in a manner analogous to Cox in section 7 of [2].

4.2 The Form Class Group

Lemma 4.2.1 *If $f_1, f_2 \in \mathcal{C} \in Q(D)/\backsim$ are concordant, then $f_1 * f_2 = f_2 * f_1$.*

Proof: This is trivial: Denote $f_1 = [a_1, b, a_2c], f_2 = [a_2, b, a_1c]$. Then $f_1 * f_2 = [a_1a_2, b, c] = [a_2a_1, b, c] = f_2 * f_1$. ■

Theorem 4.2.2 *Composition of classes via concordant forms defined by $[a_1, B, a_2C] * [a_2, B, a_1C] = [a_1a_2, B, C]$ gives a well defined operation on $S(D)$.*

Proof: Let $\mathcal{C}_1, \mathcal{C}_2 \in Q(D)/\backsim$. Then by Proposition 3.2.8 we may choose two concordant forms $f_1 \in \mathcal{C}_1, f_2 \in \mathcal{C}_2$, and define $\mathcal{C}_1\mathcal{C}_2 = [f_1 * f_2]$. To be well defined means precisely that if $g_1 \in \mathcal{C}_1, g_2 \in$

$\mathcal{C}_2$ is another pair of concordant forms, that $[g_1 * g_2] = [f_1 * f_2]$. We shall prove this by considering a series of sequentially more general cases.

Denote $f_1 = [a_1, b, a_2c], f_2 = [a_2, b, a_1c]$ and $g_1 = [a_1', b', a_2'c'], g_2 = [a_2', b', a_1'c']$. (We know that $f_1 \backsim g_1$ and $f_2 \backsim g_2$).

Case $1, f_1 = g_1$**,** $\langle a_1, a_2' \rangle_A = \langle 1 \rangle_A$**:** Because $f_1 = g_1$, we know that $b = b'$. Let $\gamma \in SL_2(A)$ such that $\gamma f_2 = g_2$, and write $\gamma = \begin{bmatrix} r & t \\ s & u \end{bmatrix}$. Then we know $\gamma^{\mathrm{T}} \begin{bmatrix} a_2 & b/2 \\ b/2 & a_1c \end{bmatrix} \gamma = \begin{bmatrix} a_2' & b/2 \\ b/2 & a_1'c' \end{bmatrix}$, which gives that $ta_2' = -sa_1c$ as well as some other useful equalities (see [A.7]).

Now because $\langle a_1, a_2' \rangle_A = \langle 1 \rangle_A$, we know that $a_1 | t$, and thus $\gamma' := \begin{bmatrix} r & t/a_1 \\ sa_1 & u \end{bmatrix} \in SL_2(A)$ (see [A.8]).

Then we after a little work have that $[g_1 * g_2] = [f_1 * f_2]$ because $g_1 * g_2 \backsim f_1 * f_2$ via γ' (see [A.9]).

Case $2, b = b', \langle a_1, a_2' \rangle_A = \langle 1 \rangle_A$**:** We have $f_1 = [a_1, b, a_2c], f_2 = [a_2, b, a_1c], g_1 = [a_1', b, a_2'c'], g_2 = [a_2', b, a_1'c']$. Then because the discriminants are equal, we have $b^2 - 4a_1a_2c = b^2 - 4a_1'a_2'c'$ so that $a_1a_2c = a_1'a_2'c'$. Thus $a_1 | a_1'c', a_2' | a_2c$, and so by Lemma 3.2.7 f_1 and g_2 are concordant. Thus we may write

$$f_1 = [a_1, b, a_2'c_0], \text{ and}$$

$$g_2 = [a_2', b, a_1c_0].$$

Thus by applying case 1 to the two pairs of concordant forms (f_1, f_2) and (f_1, g_2) we obtain $[f_1 * f_2] = [f_1 * g_2]$, and similarly $[g_2 * g_1] = [g_2 * f_1]$ (see [A.10]). Then using the fact that $*$ is Abelian (see [4.2.1]), and case 1

$$[f_1 * f_2] = [f_1 * g_2] = [g_2 * f_1] = [g_2 * g_1] = [g_1 * g_2]$$

which finishes case 2.

Case 3, $\langle a_1a_2, a_1'a_2' \rangle_A = \langle 1 \rangle_A$**:** If $b = b'$ we are done by applying case 2. Otherwise choose $n, n' \in A$ so that $a_1a_2n - a_1'a_2'n' = \frac{b'-b}{2}$. Rearranging this, we have $B := b + 2a_1a_2n = b' + 2a_1a_2n'$. Set

$$F_1 := \begin{bmatrix} 1 & a_2n \\ 0 & 1 \end{bmatrix} f_1 = [a_1, B/2, a_2(a_1a_2n^2 + bn + c)] \backsim f_1,$$

$$F_2 := \begin{bmatrix} 1 & a_1 n \\ 0 & 1 \end{bmatrix} f_2 = [a_2, B/2, a_1(a_1 a_2 n^2 + bn + c)] \backsim f_2,$$

$$G_1 := \begin{bmatrix} 1 & a_2' n' \\ 0 & 1 \end{bmatrix} g_1 = [a_1', B/2, a_2'(a_1' a_2' n'^2 + b' n' + c')] \backsim g_1,$$

$$G_2 := \begin{bmatrix} 1 & a_1' n' \\ 0 & 1 \end{bmatrix} g_2 = [a_2', B/2, a_1'(a_1' a_2' n'^2 + b' n' + c')] \backsim g_2,$$

$$H_1 := \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} f_1 * f_2 = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} [a_1 a_2, b/2, c] = [a_1 a_2, B/2, a_1 a_2 n^2 + bn + c] \backsim f_1 * f_2, \text{ and}$$

$$H_2 := \begin{bmatrix} 1 & n' \\ 0 & 1 \end{bmatrix} g_1 * g_2 = \begin{bmatrix} 1 & n' \\ 0 & 1 \end{bmatrix} [a_1' a_2', b'/2, c'] = [a_1' a_2', B/2, a_1' a_2' n'^2 + b' n' + c'] \backsim g_1 * g_2$$

where the equalities are proven in $(A.11)$, and the proper equivalence is by construction. We then have that F_1 and F_2 are concordant, and $F_1 * F_2 = H_1$ (see [A.12]). Likewise G_1 and G_2 are concordant and $G_1 * G_2 = H_2$.

Now because $\langle a_1 a_2, a_1' a_2' \rangle_A = \langle 1 \rangle_A$, it is certainly true that $\langle a_1, a_2' \rangle_A = \langle 1 \rangle_A$. Thus we may apply case 2 to F_1, F_2, G_1, G_2. In doing so we obtain that $F_1 * F_2 \backsim G_1 * G_2$. Thus,

$$[f_1 * f_2] = [H_1] = [F_1 * F_2] = [G_1 * G_2] = [H_2] = [g_1 * g_2]$$

using the fact that $H_1 = F_1 * F_2$ and $H_2 = G_1 * G_2$.

Case 4, no additional assumptions: Given $f_1 = [a_1, b, a_2 c]$, $f_2 = [a_2, b, a_1 c]$ and $g_1 = [a_1', b', a_2' c']$, $g_2 = [a_2', b', a_1' c']$, set $M := a_1 a_2 a_1' a_2'$. Then via Proposition 3.2.8 Choose α_1, α_2 with $\langle \alpha_1, \alpha_2 \rangle_A = \langle 1 \rangle_A$, $\langle \alpha_1 \alpha_2, M \rangle_A = \langle 1 \rangle_A$, and concordant forms g_1', g_2' so that

$$f_1 \backsim g_1' = [\alpha_1, \beta, \alpha_2 \eta]$$

$$f_2 \backsim g_2' = [\alpha_2, \beta, \alpha_1 \eta]$$

Now by the fact that $\langle \alpha_1 \alpha_2, a_1 a_2 a_1' a_2' \rangle_A = \langle 1 \rangle_A$, we know both $\langle a_1 a_2, \alpha_1 \alpha_2 \rangle_A = \langle 1 \rangle_A$ and $\langle \alpha_1 \alpha_2, a_1' a_2' \rangle_A = \langle 1 \rangle_A$. Hence f_1, f_2, g_1', g_2' satisfy the premesis for case 3, and so $f_1 * f_2 \backsim g_1' * g_2'$.

Likewise g_1', g_2', g_1, g_2 satisfy the premesis for case 3, and so $g_1' * g_2' \backsim g_1 * g_2$. Thus

$$[f_1 * f_2] = [g_1' * g_2'] = [g_1 * g_2].$$

And therefore to summarize our argument, given any representatives $f_1, g_1 \in \mathcal{C}_1$ and $f_2, g_2 \in \mathcal{C}_2$ with f_1 concordant with f_2 and g_1 concordant with g_2, we have

$$\mathcal{C}_1\mathcal{C}_2 = [f_1][f_2] = [g_1][g_2].$$

That is, $\mathcal{C}_1\mathcal{C}_2$ is well defined.

■

Lemma 4.2.3 *Composition of forms, and thus multiplication of elements of $Q(D)/\backsim$ is associative.*

Proof: By associativity in A and well definedness, we need only construct forms $f_1 \in \mathcal{C}_1, f_2 \in \mathcal{C}_2, f_3 \in \mathcal{C}_3$ in which we can compose. By Proposition 3.2.8 choose $f_1 = [a_1, b_1, a_2c_1] \in \mathcal{C}_1, f_2 = [a_2, b_1, a_1c_1] \in \mathcal{C}_2$. Then by Lemma 3.2.5 choose $f_3 = [a_3, b_3, c_3] \in \mathcal{C}_3$ with $\langle a_3, a_1a_2\rangle_A = \langle 1\rangle_A$.

By the fact that $\langle a_3, a_1a_2\rangle_A = \langle 1\rangle_A$ choose $m, n_3 \in A$ so that $a_1a_2m - a_3n_3 = \frac{b_3-b_1}{2}$. We then have that $a_1a_2m + \frac{b_1}{2} = a_3n_3 + \frac{b_3}{2}$. This gives us, labeling $n_1 := a_2m, n_2 := a_1m$, that

$$a_1n_1 + \frac{b_1}{2} = a_2n_2 + \frac{b_1}{2} = a_3n_3 + \frac{b_3}{2} =: B.$$

Now we find $g_1 \in \mathcal{C}_1, g_2 \in \mathcal{C}_2, g_3 \in \mathcal{C}_3$ by

$$g_1 := \begin{bmatrix} 1 & n_1 \\ 0 & 1 \end{bmatrix} f_1 = [a_1, B, \delta_1],$$

$$g_2 := \begin{bmatrix} 1 & n_2 \\ 0 & 1 \end{bmatrix} f_2 = [a_2, B, \delta_2],$$

$$g_3 := \begin{bmatrix} 1 & n_3 \\ 0 & 1 \end{bmatrix} f_3 = [a_3, B, \delta_3].$$

for appropriate (albeit messy) $\delta_1, \delta_2, \delta_3 \in A$ where the latter equalities are derived in A.15. The result now follows from associativity of A and the well definedness of $*$ (for more detail, see

A.16). ■

Lemma 4.2.4 *$[f_0] \in Q(D)/\backsim$ is an identity element, where $f_0 = [1, 0, -\frac{D}{4}]$.*

Proof: Let $f = [a, b, c] \in \mathcal{C} \in Q(D)/\backsim$. Then $f_0 \backsim \begin{bmatrix} 1 & b/2 \\ 0 & 1 \end{bmatrix} f_0 = [1, b, ac]$ (see [A.13]). Denote $f_0' := [1, b, ac]$, and we have that $f_0 * f = [a, b, c] = f$, so that indeed $[f_0]\mathcal{C} = \mathcal{C}$. ■

Lemma 4.2.5 *Inverses exist in $Q(D)/\backsim$.*

Proof: Let $[a, b, c] \in \mathcal{C}$ such that $ac \neq 0$ (there always exist such forms, see A.14). Then $[c, b, a]$ and $[a, b, c]$ are concordant. Further, $[c, b, a] \notin \mathcal{C}$ because $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} [a, b, c] = [c, b, a]$, but $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \in GL_2(A) - SL_2(A)$. Thus denote $\mathcal{C}^{-1}$ as the class with $[c, b, a] \in \mathcal{C}^{-1}$. Then we know that $f_0 \backsim [1, b, ac]$, and that $[a, b, c]$, $[c, b, a]$ are concordant. Hence

$$[a, b, c] * [c, b, a] = [ac, b, 1] \backsim [1, b, ac] \backsim f_0$$

and we are done. ■

Theorem 4.2.6 *$Q(D)/\backsim$ is an Abelian group.*

Proof: Multiplication of classes is well defined by 4.2.2. The previous lemmas give us that that multiplication is associative, that there is an identity, and that each element has an inverse. Thus indeed $Q(D)/\backsim$ is a group. It is Abelian by 4.2.1. ■

4.3 The Polynomial Ring $\mathbb{F}[T]$

We will now specialize to the polynomial ring $\mathbb{F}[T]$, although several results here should hold true in any specialization in which the induced (from being an Euclidean Domain) size function is discrete. A form $[a, b, c]$ will be called nearly reduced when $\deg(b') < \deg(a') \leq \deg(c')$ (note that we will use the convention that $\deg(0) = -\infty$. The following lemma guarantees the existence of nearly reduced forms in each class $\mathcal{C} \in Q(D)/\backsim$.

Lemma 4.3.1 *Denote $f = [a, b, c] \in Q(*)$. Then $f \backsim f' = [a', b', c']$ where $\deg(b') < \deg(a') \leq \deg(c')$.*

Proof: If $b = 0$ and $\deg(a) > \deg(c)$, then take $f' = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} f$. Note that we cannot have two of a, b, c zero lest f not be primitive unless if one of a, b, c is a unit and the other two are zero. In this case however, $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} f$ has two nonzero entries (see [B.1]). If $a = 0$ or $c = 0$, without loss of generality $a = 0$, then $f \backsim \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} f \backsim \begin{bmatrix} 3 & 1 \\ 2 & 1 \end{bmatrix} f \backsim \begin{bmatrix} 3 & 2 \\ 1 & 1 \end{bmatrix} f$, at least one of which has nonzero entries (see [B.2]).

So we have reduced the simple cases to the case that $b \neq 0$. Then if $\deg(a) > b$ and $\deg(c) > b$, then we are done with $f' = f$ or $f' = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} f$. If $\deg(a) \leq \deg(b)$, then write $b = qa + r$ where $q, r \in \mathbb{F}[T]$. Then choose $m := -q/2$, so that for $\gamma := \begin{bmatrix} 1 & m \\ 0 & 1 \end{bmatrix}$, we have that $f \backsim \gamma f = [a, b_2, c_2]$ has $\deg(b_2) < \deg(a)$ (see [B.4]). Note that $a_2 = a$ so that $a_2 \neq 0$. If $c = 0$, use the above to reduce the form to a form with all nonzero coefficients. (Note that this does not increase the minimum degree of the nonzero coefficients). If $\deg(c) < \deg(a)$, apply $\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$. Otherwise repeat this process at most $\min(\deg(a), \deg(b), \deg(c)) + 1$ times until $\deg(b)$ is less than both $\deg(a)$ and $\deg(c)$. Note that in the case that $\deg(a) = 0$, this will yield a form with $b = 0$. Note that the quantity $\min(\deg(a), \deg(b), \deg(c))$ comes from the fact that we reduce the degree of b each iteration, and $\min(\deg(a), \deg(c))$ does not increase. ■

Proposition 4.3.2 *Denote $f = [a, b, c]$. Let D be the discriminant of f. If $\deg(D) = 0$, then $f \backsim [a', 0, c']$ where $\deg(a') = \deg(c') = 0$.*

Proof: Reduce f to $f' = [a', b', c']$ so that $\deg(b') < \deg(a') \leq \deg(c')$ by 4.3.1. Then $0 = \deg(D) = \deg(b'^2 - 4a'c') = \deg(a'c') = \deg(a') + \deg(c')$. Thus $\deg(a') = \deg(c') = 0$. So we must have $b = 0$, because only 0 has degree less than 0. ■

Theorem 4.3.3 *$Q(D)/\backsim$ is a finite Abelian group.*

Proof: Let $\mathcal{C} \in Q(D)/\backsim$, and choose $f \in \mathcal{C}$ to be a nearly reduced form. Then $D = b^2 - 4ac$. However, $\deg(b^2) < \deg(4ac)$ because f is reduced, so $\deg(D) = \deg(ac)$. Hence $\deg(c)$ is bounded by $\deg(c) \leq \deg(D)$, and so $\deg(a), \deg(b), \deg(c) \leq \deg(D)$. Hence for a not very sharp upper bound,

$$|Q(D)/\backsim| \leq |\mathbb{F}|^{3\deg(D)}.$$

The Abelian group part was proven in 4.2.6. ■

4.4 Orders And the Ideal Class Group In $\mathbb{F}[T]$

We will continue to specialize to $\mathbb{F}[T]$, whose field of fractions is $\mathbb{F}(T)$. Let $D \in \mathbb{F}[T]$ be an irreducible polynomial. Denote $\mathfrak{d} := \sqrt{D}$. The field of fractions of $\mathbb{F}[T][\mathfrak{d}]$ is $\mathbb{F}(T)(\mathfrak{d}) = \mathbb{F}(T)[\mathfrak{d}]$. We then know that the integral closure of $\mathbb{F}[T]$ in $\mathbb{F}(T)[\mathfrak{d}]$ is $\mathcal{O}_K = \mathbb{F}[T][\mathfrak{d}] = \mathbb{F}[T] \oplus \mathbb{F}[T]\mathfrak{d}$ (see [8]). For clarity's sake we shall avoid using anything for K other than $\mathbb{F}(T)[\mathfrak{d}]$, although we shall still use the notation $\mathcal{O}_K$ instead of $\mathcal{O}_{\mathbb{F}_{(T)}[\mathfrak{d}]}$. Note that we will use $\mathfrak{d}$ or $\sqrt{D}$ depending on which seems more appropriate for intuition purposes at the time interchangeably.

Definition 4.4.1 *A subring $\{1\} \subseteq \mathcal{O} \subseteq \mathbb{F}(T)[\mathfrak{d}]$ is said to be an <u>order</u> in $\mathbb{F}(T)[\mathfrak{d}]$ when $\mathcal{O}$ is a finitely generated $\mathbb{F}[T]$-module, and contains a basis of $\mathbb{F}(T)[\mathfrak{d}]$ as a $\mathbb{F}(T)$-vector space.*

Lemma 4.4.2 *Let $\mathcal{O}$ be an order in $\mathbb{F}(T)[\mathfrak{d}]$. Then $\mathcal{O}$ is of rank 2 as a $\mathbb{F}[T]$ module.*

Proof: $\mathcal{O}$ is has no torsion because $\mathbb{F}(T)[\mathfrak{d}]$ has no zero divisors. By the structure theorem of modules over principal ideal domains it is free. It is of rank at least two because it contains a basis for $\mathbb{F}(T)[\mathfrak{d}]$ as an $\mathbb{F}(T)$ vector space.

To show that it is of rank less than 3, Let $g_1, g_2, g_3 \in \mathcal{O} \subseteq \mathbb{F}(T)[\mathfrak{d}]$. We know that $\mathbb{F}(T)[\mathfrak{d}]$ is of rank 2 as an $\mathbb{F}(T)$ vector space, so that there are $a_1, a_2, a_3 \in \mathbb{F}(T)$ not all zero so that

$$a_1 g_1 + a_2 g_2 + a_3 g_3 = 0.$$

Then clearing denominators we get

$$a_1' g_1 + a_2' g_2 + a_3' g_3 = 0$$

where $a_1', a_2', a_3' \in \mathbb{F}[T]$ and not all are zero. Thus g_1, g_2, g_3 are dependent over $\mathbb{F}[T]$ as well. Therefore $\mathcal{O}$ is of rank less than 3, and thus exactly 2. ■

Lemma 4.4.3 *Let a ring R with unity be a finitely generated $\mathbb{F}[T]$-submodule of $\mathbb{F}(T)[\mathfrak{d}]$. Then $R \cap \mathbb{F}(T) = \mathbb{F}[T]$.*

Proof: Let $\frac{p}{q} \in R \cap \mathbb{F}(T), p, q \in \mathbb{F}[T]$. Each element of $R \cap \mathbb{F}(T)$ may be represented as this, with p and q having no common factors. Indeed assume that p and q have no common factors.

Then we have $\cup_{i=1}^{\infty} \left\langle \frac{p^n}{q^n} \right\rangle_{\mathbb{F}[T]} \subseteq R \cap \mathbb{F}(T)$. Now R is a free $\mathbb{F}[T]$ module and finitely generated. Thus any $\mathbb{F}[T]$ submodule is also finitely generated. In particular $\cup_{i=1}^{\infty} \left\langle \frac{p^n}{q^n} \right\rangle_{\mathbb{F}[T]}$ is which implies $\deg(q) = 0$.

Thus we have that $R \cap \mathbb{F}(T) \subseteq \mathbb{F}[T]$. Further, $\mathbb{F}[T] \subseteq R$ because $1 \in R$, and R is a $\mathbb{F}[T]$ module. Trivially $\mathbb{F}[T] \subseteq \mathbb{F}(T)$ Therefore we have our result $R \cap \mathbb{F}(T) = \mathbb{F}[T]$. ■

Lemma 4.4.4 *Let $\mathcal{O}$ be an order in $\mathbb{F}(T)[\mathfrak{d}]$. Then $\mathcal{O} \subseteq \mathcal{O}_K$.*

Proof: Write $\mathcal{O} = \langle g_1, g_2 \rangle_{\mathbb{F}[T]}$ by 4.4.2. Thus we may write $1 = pg_1 + qg_2$ where $p, q \in \mathbb{F}[T]$. Write $\langle p, q \rangle_{\mathbb{F}[T]} = \langle g \rangle_{\mathbb{F}[T]}$ by the fact that $\mathbb{F}[T]$ is a principle ideal domain. Then $g^{-1} = \frac{p}{g} g_1 + \frac{q}{g} g_2 \in \mathcal{O} \cap \mathbb{F}(T) = \mathbb{F}[T]$. Hence $g \in \mathbb{F}$ by Lemma 4.4.3. Thus without loss of generality we may choose p, q so that $g = 1$. Then we may choose $r, s, \in F[T]$ so that $ps - qr = 1$. Hence $\begin{bmatrix} p & q \\ r & s \end{bmatrix} \in SL_2(\mathbb{F}[T])$, and so we may choose $\lambda := rg_1 + sg_2$ so that $\langle 1, \lambda \rangle_{\mathbb{F}[T]} = \mathcal{O}$.

Now $\mathcal{O}$ is a ring, and so $\lambda^2 \in \mathcal{O}$ because $\lambda \in \mathcal{O}$. Thus there are some $a_0, a_1 \in \mathbb{F}[T]$ such that $\lambda^2 = -a_0 - a_1\lambda$. Hence $\lambda^2 + a_1\lambda + a_0 = 0$, and so λ is integral over $\mathbb{F}[T]$. Hence $\mathcal{O}$ is contained in the integral closure of $\mathbb{F}[T]$, that is, $\mathcal{O} \subseteq \mathcal{O}_K$. ■

Lemma 4.4.5 *Let $\mathcal{O}$ be a subring $1 \in \mathcal{O} \subseteq \mathbb{F}(T)[\mathfrak{d}]$ of rank 2 as an $\mathbb{F}[T]$-submodule. Then $\mathcal{O}$ is an order and can be written as $\langle 1, f\mathfrak{d} \rangle_{\mathbb{F}[T]}$ for some $f \in \mathbb{F}[T]$.*

Proof: As in the proof of Lemma 4.4.4 we know that $\mathcal{O} = \langle 1, b \rangle_{\mathbb{F}[T]}$ where $b \in \mathcal{O} \subseteq \mathcal{O}_K$. Write $b = a + f\mathfrak{d}$ where $a, f \in \mathbb{F}[T]$. Then we have $\mathcal{O} = \langle 1, b \rangle_{\mathbb{F}[T]} = \langle 1, f\mathfrak{d} \rangle_{\mathbb{F}[T]}$. Then because $f\mathfrak{d}$ is $\mathbb{F}(T)$ independent of 1, we know that $\langle 1, f\mathfrak{d} \rangle_{\mathbb{F}(T)} = \mathbb{F}(T)[\mathfrak{d}]$. Hence $\mathcal{O}$ is an order. ■

Definition 4.4.6 *Let $\mathfrak{a}$ be an ideal of $\mathcal{O}$. A <u>fractional ideal</u> of $\mathcal{O}$ is a nonzero $\mathcal{O}$-submodule $\mathfrak{a}$ of $\mathbb{F}(T)[\mathfrak{d}]$ such that there is an $a \in \mathcal{O}$ such that $a\mathfrak{a} \subseteq \mathcal{O}$. A fractional ideal $\mathfrak{a}$ of $\mathcal{O}$ is said to be a <u>proper fractional ideal</u> if $\mathcal{O} = \{b \in \mathbb{F}(T)[\mathfrak{d}] | b\mathfrak{a} \subseteq \mathfrak{a}\}$.*

Note that any nonzero finitely generated $\mathcal{O}$-submodule of $\mathbb{F}(T)[\mathfrak{d}]$ is a fractional ideal (See page 401 in [4]).

Proposition 4.4.7 *If $\mathfrak{a}$ is a fractional ideal of an order $\mathcal{O}$, then $\mathfrak{a}$ is an $\mathbb{F}[T]$ module of rank 2.*

Proof: Select $a \in \mathcal{O}$ so that $a\mathfrak{a} \subseteq \mathcal{O}$. Then $a\mathfrak{a} = \langle \gamma, \lambda \rangle_{\mathbb{F}[T]}$ for some $\lambda, \gamma \in \mathcal{O}$ because $a\mathfrak{a}$ is a $\mathbb{F}[T]$-submodule of $\mathcal{O}_K$. Then $\mathfrak{a} = a^{-1}a\mathfrak{a} = \left\langle \frac{\gamma}{a}, \frac{\lambda}{a} \right\rangle_{\mathbb{F}[T]}$ ■

Lemma 4.4.8 *Let $ax^2+bx+c \subseteq \mathbb{F}[T][x]$ be the minimal polynomial for some $\tau \in \mathbb{F}(T)[\mathfrak{d}] \setminus \mathbb{F}[T]$. Then $\mathcal{O} := \langle 1, a\tau\rangle_{\mathbb{F}[T]}$ is an order of $\mathbb{F}(T)[\mathfrak{d}]$, and $\langle 1,\tau\rangle_{\mathbb{F}[T]}$ is a a proper fractional ideal of $\mathcal{O}$.*

Proof: First note that $\langle 1, a\tau\rangle_{\mathbb{F}[T]} = \left\langle 1, -b+\sqrt{D}\right\rangle_{\mathbb{F}[T]} = \left\langle 1, \sqrt{D}\right\rangle_{\mathbb{F}[T]}$. Then because $D \in \mathbb{F}[T]$ we find that $\langle 1, a\tau\rangle_{\mathbb{F}[T]}$ is a free $\mathbb{F}[T]$ module of rank 2 and is closed under multiplication. Hence it is a ring containing 1 and of rank 2 as an $\mathbb{F}[T]$ module and so is an order by 4.4.5.

$\langle 1,\tau\rangle_{\mathbb{F}[T]}$ is a fractional ideal because $\mathbb{F}[T] \subseteq \mathcal{O}$ so that $\langle 1,\tau\rangle_{\mathbb{F}[T]}$ is a finitely generated $\mathcal{O}$ module:

$$\left(\langle 1,\tau\rangle_{\mathbb{F}[T]}\right)\mathcal{O} = \langle 1,\tau\rangle_{\mathbb{F}[T]}\mathcal{O} = \langle 1,\tau\rangle_{\mathcal{O}}\,.$$

Now we shall prove that $\langle 1,\tau\rangle_{\mathbb{F}[T]}$ is proper. To do this we must prove that $\mathcal{O} = \{b \in \mathbb{F}(T)[\mathfrak{d}] : b\langle 1,\tau\rangle_{\mathbb{F}[T]} \subseteq \langle 1,\tau\rangle_{\mathbb{F}[T]}\}$. Because $\langle 1,\tau\rangle_{\mathbb{F}[T]}$ is an $\mathcal{O}$-module, "$\subseteq$" is trivial. We must prove "$\supseteq$". Note that $\beta\langle 1,\tau\rangle_{\mathbb{F}[T]} \subseteq \langle 1,\tau\rangle_{\mathbb{F}[T]}$ if and only if both $\beta \in \langle 1,\tau\rangle_{\mathbb{F}[T]}$ and $\beta\tau \in \langle 1,\tau\rangle_{\mathbb{F}[T]}$ if and only if there are $n,m \in \mathbb{F}[T]$ so that $\beta = m+n\tau$ and $a|n$. This is because if $\beta = m+n\tau$, then $\beta\tau = m\tau + n\tau^2 = m\tau - n\frac{b\tau+c}{a} = \frac{-cn}{a} + \left(\frac{-bn}{a}+m\right)\tau$. Thus $\beta\tau \in \langle 1,\tau\rangle_{\mathbb{F}[T]}$ if and only if both $\frac{cn}{a} \in \mathbb{F}[T]$ and $\frac{bn}{a} \in \mathbb{F}[T]$ if and only if $a|n$. ($\Leftarrow$ is trivial, $\Rightarrow$ is because with $\frac{cn}{a}+\frac{bn}{a} = d$ we have would $n(c+b) = da$, so that $a|n$). The converse is trivial.

Further there are $n,m \in \mathbb{F}[T]$ so that $\beta = m+n\tau$ and $a|n$ if and only if $\beta \in \langle 1, a\tau\rangle_{\mathbb{F}[T]}$. This is actually quite easy once one thinks about it. For the forward implication, write $\beta = m+n'a\tau$. For the converse write $\beta = m+n'a\tau$, and then define $n := n'a$.

Hence $\langle 1,\tau\rangle_{\mathbb{F}[T]}$ is also proper. ∎

The set of all fractional ideals of an order $\mathcal{O}$ is a monoid with the standard multiplication of fractional ideals, and identity $\mathcal{O}$. Thus we use the following standard definition.

Definition 4.4.9 *A fractional ideal $\mathfrak{a}$ of $\mathcal{O}$ is said to be <u>invertible</u> if there is another fractional ideal $\mathfrak{b}$ such that $\mathfrak{ab} = \mathcal{O}$.*

Because multiplication of fractional ideals is associative, inverses are unique. We shall denote the inverse of $\mathfrak{a}$ as $\mathfrak{a}^{-1}$.

Proposition 4.4.10 *Suppose $\mathcal{O}$ is an order of $\mathbb{F}(T)[\mathfrak{d}]$. Let $\mathfrak{a}$ be a fractional $\mathcal{O}$-ideal. Then $\mathfrak{a}$ is a proper if and only if $\mathfrak{a}$ is invertible.*

Proof: ($\Leftarrow$) Write $\mathfrak{ab} = \mathcal{O}$. We must prove that $\mathcal{O} = \{b \in \mathbb{F}(T)[\mathfrak{d}] | b\mathfrak{a} \subseteq \mathfrak{a}\}$. Because $\mathfrak{a}$ is an $\mathcal{O}$-module, "$\subseteq$" is trivial. We must prove "$\supseteq$". Let $b \in \mathbb{F}(T)[\mathfrak{d}]$ such that $b\mathfrak{a} \subseteq \mathfrak{a}$. Then

$b\mathcal{O} = b(\mathfrak{ab}) = (b\mathfrak{a})\mathfrak{b} \subseteq \mathfrak{ab} = \mathcal{O}$. Thus $b\mathcal{O} \subseteq \mathcal{O}$. In particular, $b = b \cdot 1 \in b\mathcal{O} \subseteq \mathcal{O}$. Hence $\mathfrak{a}$ is proper.

($\Rightarrow$) Let $\mathfrak{a}$ be a proper fractional ideal. Then by 4.4.7 we may write $\mathfrak{a} = \langle \alpha, \beta \rangle_{\mathbb{F}[T]}$ for some $\alpha, \beta \in \mathbb{F}(T)[\mathfrak{d}]$. Then denoting $\tau := \frac{\beta}{\alpha}$ we have

$$\mathfrak{a} = \alpha \langle 1, \tau \rangle_{\mathbb{F}(T)}.$$

Now let $ax^2 + bx + c$ be the minimal polynomial of τ. (Note that τ must be of degree two over $\mathbb{F}[T]$, because 1 and τ generate a free module of rank 2 that contains $\mathbb{F}[T]$)

Denote τ' to be the other root of $ax^2 + bx + c$.

Now because $\mathfrak{a}$ is proper, we know that $\mathcal{O} = \{\beta \in \mathbb{F}(T)[\mathfrak{d}] | \beta\mathfrak{a} \subseteq \mathfrak{a}\}$. Hence by 4.4.8 we know that $\mathcal{O} = \langle 1, a\tau \rangle_{\mathbb{F}[T]}$, and that the order $\langle 1, a\tau' \rangle_{\mathbb{F}[T]}$ has proper fractional ideal $\mathfrak{a}' := \langle 1, \tau' \rangle_{\mathbb{F}[T]}$. We see that these orders are actually the same, as $\langle 1, a\tau \rangle_{\mathbb{F}[T]} = \left\langle 1, \frac{-b+\sqrt{D}}{2} \right\rangle_{\mathbb{F}[T]} = \left\langle 1, -b + \sqrt{D} \right\rangle_{\mathbb{F}[T]} = \left\langle 1, b - \sqrt{D} \right\rangle_{\mathbb{F}[T]} = \left\langle 1, -b - \sqrt{D} \right\rangle_{\mathbb{F}[T]} = \langle 1, a\tau' \rangle_{\mathbb{F}[T]}$.

We can now obtain that $\mathfrak{a}^{-1} = \frac{a}{\alpha}\mathfrak{a}'$. This is because

$$\begin{aligned}
\left(\frac{a}{\alpha}\mathfrak{a}'\right)\mathfrak{a} &= \left(\frac{a}{\alpha}\langle 1, \tau \rangle_{\mathbb{F}[T]}\right)\left(\alpha \langle 1, \tau' \rangle_{\mathbb{F}[T]}\right) \\
&= \frac{a\alpha \langle 1, \tau \rangle_{\mathbb{F}[T]} \langle 1, \tau' \rangle_{\mathbb{F}[T]}}{\alpha} \\
&= \langle a, a\tau, a\tau', a\tau\tau' \rangle_{\mathbb{F}[T]} \\
&= \langle a, a\tau, a(\tau + \tau'), a\tau\tau' \rangle_{\mathbb{F}[T]} \\
&= \langle a, a\tau, -b, c \rangle_{\mathbb{F}[T]} \\
&= \langle (a, b, c), a\tau \rangle_{\mathbb{F}[T]} \\
&= \langle 1, a\tau \rangle_{\mathbb{F}[T]} \\
&= \mathcal{O}.
\end{aligned}$$

For the fourth equality consider that we know that $a\tau^2 + b\tau + c$ is the minimal polynomial of τ and τ'. Thus τ' is the only conjugate of τ, and so $\tau\tau' = N(\tau) = (-1)^{\deg(m_\tau(x))}[\tau]m_\tau(x) = -b$ as well as $\tau + \tau' = Tr(\tau) = [\tau^0]m_\tau(x) = c$.

■

Now to move toward the ideal class group, let $I(\mathcal{O})$ denote the set of all proper fractional ideals of $\mathcal{O}$, and $P(\mathcal{O})$ denote the subset of all principal proper fractional ideals. Clearly $\mathcal{O}$ is an

identity element of $I(\mathcal{O})$ under multiplication. By 4.4.10 we have inverses for each element of $I(\mathcal{O})$. (In fact we have constructed $I(\mathcal{O})$ by taking precisely those elements with inverses!). Thus $I(\mathcal{O})$ is a group if we can only show closure.

Proposition 4.4.11 *$I(\mathcal{O})$ is an Abelian group under multiplication.*

Proof: By the above comments we need only show that if $\mathfrak{a}, \mathfrak{b} \in I(\mathcal{O})$ then $\mathfrak{ab} \in I(\mathcal{O})$. As in page 402 of [4] we know that $\mathfrak{ab}$ is a fractional ideal. Thus we need only show that it is proper. Indeed by 4.4.10 we know that $\mathfrak{ab}$ is proper if and only if it has an inverse. Such an inverse is $\mathfrak{b}^{-1}\mathfrak{a}^{-1}$, as $\mathfrak{ab}\mathfrak{b}^{-1}a^{-1} = \mathfrak{a}\mathcal{O}\mathfrak{a}^{-1} = \mathfrak{a}\mathfrak{a}^{-1} = \mathcal{O}$. (Note that this concurrently proves that $\mathfrak{b}^{-1}\mathfrak{a}^{-1}$ must also be proper because $\mathfrak{b}^{-1}$ and $\mathfrak{a}^{-1}$ are). The fact that $I(\mathcal{O})$ is Abelian follows from the fact that multiplication in $\mathbb{F}(T)[\mathfrak{d}]$ is commutative. ■

Proposition 4.4.12 *$P(\mathcal{O})$ is a normal subgroup under multiplication.*

Proof: The fact that $P(\mathcal{O})$ is a group is trivial, as $(a)(b) = (ab)$ and $(a)^{-1} = (a^{-1})$. (Note that a^{-1} may not be in $\mathbb{F}[T]$, but that is fine because it may be a fractional ideal). The fact that $P(\mathcal{O})$ is normal follows from the fact that $I(\mathcal{O})$ is Abelian. ■

Definition 4.4.13 *We can then define the ideal class group of $\mathcal{O}$, $I(\mathcal{O})/P(\mathcal{O}) := I(\mathcal{O})/P(\mathcal{O})$.*

Corollary 4.4.14 *$I(\mathcal{O})/P(\mathcal{O})$ is a group.*

Proof: Trivial. ■

4.5 The Class Group Isomorphism

Assume that D is not a square in $\mathbb{F}[T]$.

There is an isomorphism between the form class group constructed in 4.2.6 and the ideal class group mentioned in 4.4.14.

To prove this we shall construct a map from the set of primitive forms of a given discriminant, $Q(D)$, to the ideals of an order $I(\mathcal{O})$. The order involved is $\langle 1, a\tau\rangle_{\mathbb{F}[T]} = \left\langle 1, \frac{-b+\sqrt{D}}{2}\right\rangle_{\mathbb{F}[T]} = \left\langle 1, \sqrt{D}\right\rangle_{\mathbb{F}[T]}$, where $[a,b,c] \in Q(D)$ and $\tau := \frac{-b+\sqrt{D}}{2a}$. The latter equality above is mostly obvious (see [C.1]), although slightly surprising. This is an order by 4.4.8. Denote this order as $\mathcal{O}$.

In figure 4.1, φ' is the map we shall construct, which induces the isomorphism φ between the two groups we are interested in. Define $\varphi'(f) := \langle a, \tau\rangle_{\mathbb{F}[T]}$, so $\varphi([f]) = \left[\langle a, \tau\rangle_{\mathbb{F}[T]}\right]$

Lemma 4.5.1 *Let $[a,b,c] \in Q(D)/\backsim$. Then $\left\langle a, \frac{-b+\sqrt{D}}{2}\right\rangle_{\mathbb{F}[T]} \left(= a\left\langle 1, -b+\sqrt{D}\right\rangle_{\mathbb{F}[T]}\right)$ is a proper ideal of $\mathcal{O}$.*

Proof: Let τ be a root of ax^2+bx+c. In the future we will specify which root, but for this lemma it does not matter. Because D is not a square, ax^2+bx+c is irreducible, and thus the minimal polynomial of τ. Hence by 4.4.8 we have that $\langle 1, \tau\rangle_{\mathbb{F}[T]}$ is a proper fractional ideal of $\mathcal{O} = \langle 1, a\tau\rangle_{\mathbb{F}[T]}$.

Now $a\langle 1, \tau\rangle_{\mathbb{F}[T]} \subseteq \langle 1, a\tau\rangle_{\mathbb{F}[T]}$ and thus $a\langle 1, \tau\rangle_{\mathbb{F}[T]}$ is a ordinary ideal. (by ordinary ideal we merely mean an ideal of $\mathcal{O}$).

That is, we found that $\langle 1, \tau\rangle_{\mathbb{F}[T]}$ and thus $a\langle 1, \tau\rangle_{\mathbb{F}[T]}$ is a proper fractional ideal of $\mathcal{O}$. But because it is contained in $\mathcal{O}$ it is in fact a ordinary ideal. ■

Lemma 4.5.2 *φ is well defined.*

Both our domain and codomain are equivalence classes, and so we must verify well definedness in both regards. So let $\mathcal{C} \in Q(D)/\backsim$ with representatives $f, g \in \mathcal{C}$.

$$\begin{array}{ccc} Q(D) & \xrightarrow{\quad\varphi'\quad} & I(\mathcal{O}) \\ \Big\downarrow{\scriptstyle [\cdot]} & & \Big\downarrow{\scriptstyle [\cdot]} \\ Q(D)/\backsim & \xrightarrow{\quad\varphi\quad} & I(\mathcal{O})/P(\mathcal{O}) \end{array}$$

Figure 4.1: The constructed mapping

Denote $f = f(x,y) = [a,b,c] = ax^2+bxy+cy^2, g = a'x^2+b'xy+c'y^2$. Let $\tau = \frac{-b+\sqrt{D}}{2a}, \tau' = \frac{-b'+\sqrt{D}}{2a'}$. Thus $\varphi([f]) = [\langle a,\tau\rangle_{\mathbb{F}[T]}], \varphi([g]) = [\langle a',\tau'\rangle_{\mathbb{F}[T]}]$. To show well definedness and one-to-one we will prove that f is properly equivalent to g if and only if $\langle a,\tau\rangle_{\mathbb{F}[T]}$ is equivalent to $\langle a',\tau'\rangle_{\mathbb{F}[T]}$.

That is to say that there is a $\gamma \in SL_2(\mathbb{F}[T])$ such that $\gamma g = f$ if and only if there is a $\lambda \in \mathbb{F}(T)[\mathfrak{d}]$ such that $\langle a,\tau\rangle_{\mathbb{F}[T]} = \lambda \langle a',\tau'\rangle_{\mathbb{F}[T]}$.

We shall do this in the next four claims, of which 4.5.2 will follow as a corollary.

Claim 4.5.3 *If* $f \backsim g$ *via* $\begin{bmatrix} p & q \\ r & s \end{bmatrix} g = f$, *then* $\tau' = \begin{bmatrix} p & q \\ r & s \end{bmatrix} \cdot \tau \left(= \frac{p\tau+q}{r\tau+s}\right)$.

Proof:

We shall prove that $\frac{p\tau+q}{r\tau+s}$ is actually τ'. We have $\begin{bmatrix} p & q \\ r & s \end{bmatrix} g = f$, $\begin{bmatrix} p & q \\ r & s \end{bmatrix} \in SL_2(\mathbb{F}[T])$, and we will need the fact that $\begin{bmatrix} p & q \\ r & s \end{bmatrix}^{-1} f = \begin{bmatrix} s & -q \\ -r & p \end{bmatrix} f = g$. This yields $a' = f(s,-r), b' = -2aqs + bpr + bps - 2cpr$, and $c' = f(-q,p)$ (see 3.2.1, with different constants plugged in.

Now expanding $\frac{p\tau+q}{r\tau+s}$ out we get that

$$\frac{p\tau+q}{r\tau+s} = \frac{2aqs - bps - bqr + 2cpr + \sqrt{D}(ps-qr)}{2(as^2 - bsr + cr^2)}$$

$$= \frac{-b' + \sqrt{D}}{2a'} = \tau'$$

where we removed the $ps-qr$ because $ps-qr = 1$ because $\begin{bmatrix} p & q \\ r & s \end{bmatrix} \in SL_2(\mathbb{F}[T])$.

This proves the result, although it may be noted that the first equality above is is because

$$\begin{aligned}
\frac{p\tau+q}{r\tau+s} &= \frac{p\frac{-b+\sqrt{D}}{2a}+q}{r\frac{-b+\sqrt{D}}{2a}+s} \\
&= \frac{p(-b+\sqrt{D})+2aq}{r(-b+\sqrt{D})+2as} \\
&= \frac{2aq-bp+p\sqrt{D}}{2as-br+r\sqrt{D}} \\
&= \frac{2aq-bp+p\sqrt{D}}{2as-br+r\sqrt{D}}\left(\frac{2as-br-r\sqrt{D}}{2as-br-r\sqrt{D}}\right) \\
&= \frac{(2aq-bp)(2as-br)-rpD+(-r(2aq-bp)+p(2as-br))\sqrt{D}}{(2as-br)^2-r^2D)} \\
&= \frac{4a^2qs-2abqr-2abps+b^2pr-rp(b^2-4ac)+(-2aqr+2bpr+2aps-bpr)\sqrt{D}}{4a^2s^2-4abrs+b^2r^2-r^2(b^2-4ac)} \\
&= \frac{4a^2qs-2abqr-2abps+b^2pr-b^2pr-4acpr+(-2aqr+2aps)\sqrt{D}}{4a^2s^2-4abrs+b^2r^2-b^2r^2+4ar^2c} \\
&= \frac{4a^2qs-2abqr-2abps-4acpr+(-2aqr+2aps)\sqrt{D}}{4a^2s^2-4abrs+4ar^2c} \\
&= \frac{2a\left(2aqs-bqr-bps-2cpr+(-qr+ps)\sqrt{D}\right)}{2a\left(2as^2-2brs+2r^2c\right)} \\
&= \frac{2aqs-bqr-bps-2cpr+(ps-qr)\sqrt{D}}{2as^2-2brs+2r^2c} \\
&= \frac{2aqs-bqr-bps-2cpr+(ps-qr)\sqrt{D}}{2\left(as^2-brs+cr^2\right)} \\
&= \frac{2aqs-bqr-bps-2cpr+(ps-qr)\sqrt{D}}{2\left(as^2-brs+cr^2\right)}.
\end{aligned}$$

■

Claim 4.5.4 *If* $\begin{bmatrix} p & q \\ r & s \end{bmatrix}\tau = \tau'$, *then* $f = \begin{bmatrix} p & q \\ r & s \end{bmatrix} g$. *(Note that this implies that if* $\begin{bmatrix} p & q \\ r & s \end{bmatrix} \in SL_2(\mathbb{F}[T])$, *then* $f \backsim g$, *while if* $\begin{bmatrix} p & q \\ r & s \end{bmatrix} \in GL_2(\mathbb{F}[T])$, *then* $f \backsimeq g$.*)*

Proof: Consider that

$$a'\tau'^2 + b'\tau' + c = 0$$

$$\Rightarrow a'\left(\frac{p\tau+q}{r\tau+s}\right)^2 + b'\frac{p\tau+q}{r\tau+s} + c = 0$$

$$\Rightarrow a'(p\tau+q)^2 + b'(p\tau+q)(r\tau+s) + c'(r\tau+s)^2 = 0$$

$$\Rightarrow a'(p^2\tau^2 + 2pq\tau + q^2) + b'(pr\tau^2 + (ps+qr)\tau + qs) + c'(r^2\tau^2 + 2rs\tau + s^2) = 0$$

$$\Rightarrow (a'p^2 + b'pr + c'r^2)\tau^2 + (2a'pq + bqr + bps + 2c'rs)\tau + (a'q^2 + b'qs + c's^2) = 0$$

$$\Rightarrow g(p,r)\tau^2 + (2a'pq + bqr + bps + 2c'rs)\tau + g(q,s) = 0.$$

So that we have that τ is a root of the polynomial $g(p,r)x^2 + (2a'pq + bqr + bps + 2c'rs)x + g(q,s)$. Hence because $ax^2 + bx + c$ is the minimal polynoimal of τ, $[a,b,c]$ divides $g(p,r)x^2 + (2a'pq + bqr + bps + 2c'rs)x + g(q,s)$. Because both of these polynomials are of degree two, we thus have that there is a $u \in \mathbb{F}^\star$ so that

$$au = g(p,r),$$

$$bu = 2a'pq + bqr + bps + 2c'rs, \text{ and}$$

$$cu = g(q,s).$$

Now note that we have by applying $\det\left(\begin{bmatrix} p & q \\ r & s \end{bmatrix}\right)\begin{bmatrix} p & q \\ r & s \end{bmatrix}^{-1}$ to $\begin{bmatrix} p & q \\ r & s \end{bmatrix}\tau = \tau'$,

$$(ps-qr)\tau = \begin{bmatrix} s & -q \\ -r & p \end{bmatrix}\tau'$$

which gives

$$(ps-qr)\left(\frac{-b+\sqrt{D}}{2a}\right) = \frac{-2a'pq - b'qr - b'ps - 2c'rs + (ps-qr)\sqrt{D}}{2\left(a'p^2 + b'pr + c'r^2\right)}.$$

because

$$\begin{aligned}
\frac{s\tau' - q}{-r\tau' + p} &= \frac{s\frac{-b'+\sqrt{D}}{2a'} - q}{-r\frac{-b'+\sqrt{D}}{2a'} + p} \\
&= \frac{s(-b'+\sqrt{D}) - 2a'q}{-r(-b'+\sqrt{D}) + 2a'p} \\
&= \frac{-2a'q - b's + s\sqrt{D}}{2a'p + b'r - r\sqrt{D}} \\
&= \frac{-2a'q - b's + s\sqrt{D}}{2a'p + b'r - r\sqrt{D}} \left(\frac{2a'p + b'r + r\sqrt{D}}{2a'p + b'r + r\sqrt{D}}\right) \\
&= \frac{(-2a'q - b's)(2a'p + b'r) + rsD + (r(-2a'q - b's) + s(2a'p + b'r))\sqrt{D}}{(2a'p + b'r)^2 - r^2D} \\
&= \frac{-4a'^2qp - 2a'b'qr - 2a'b'sp - b'^2sr + rs(b'^2 - 4a'c') + (-2a'qr + 2a'sp)\sqrt{D}}{4a'^2p^2 + 4a'b'rp + b'^2r^2 - r^2(b'^2 - 4a'c')} \\
&= \frac{-4a'^2qp - 2a'b'qr - 2a'b'sp - b'^2sr + b'^2sr - 4a'c'sr + (-2a'qr + 2a'sp)\sqrt{D}}{4a'^2p^2 + 4a'b'rp + b'^2r^2 - b'^2r^2 + 4a'r^2c'} \\
&= \frac{-4a'^2qp - 2a'b'qr - 2a'b'sp - 4a'c'sr + (-2a'qr + 2a'sp)\sqrt{D}}{4a'^2p^2 + 4a'b'rp + 4a'r^2c'} \\
&= \frac{2a'\left(-2a'qp - b'qr - b'sp - 2c'sr + (-qr + sp)\sqrt{D}\right)}{2a'\left(2a'p^{+}2b'rp + 2r^2c'\right)} \\
&= \frac{-2a'qp - b'qr - b'sp - 2c'sr + (sp - qr)\sqrt{D}}{2a'p^2 + 2b'rp + 2r^2c'} \\
&= \frac{-2a'qp - b'qr - b'sp - 2c'sr + (sp - qr)\sqrt{D}}{2\left(a'p^2 + b'rp + c'r^2\right)} \\
&= \frac{-2a'qp - b'qr - b'sp - 2c'sr + (sp - qr)\sqrt{D}}{2\left(a'p^2 + b'rp + c'r^2\right)} \\
&= \frac{-2a'pq - b'qr - b'ps - 2c'rs + (ps - qr)\sqrt{D}}{2\left(a'p^2 + b'pr + c'r^2\right)}.
\end{aligned}$$

Then by comparing the $\sqrt{D}$ parts we get

$$\frac{ps - qr}{2a} = \frac{ps - qr}{2\left(a'p^2 + b'pr + c'r^2\right)} = \frac{ps - qr}{2g(p, r)}$$

which gives

$$a = g(p, r).$$

And hence we have that $u = 1$.

Whence $\begin{bmatrix} p & q \\ r & s \end{bmatrix} g = f$ by 3.2.1. ■

Claim 4.5.5 *If* $\begin{bmatrix} p & q \\ r & s \end{bmatrix} \tau = \tau'$ *and* $\begin{bmatrix} p & q \\ r & s \end{bmatrix} \in SL_2(\mathbb{F}[T])$*, then there is a* $\lambda \in \mathbb{F}(T)[\mathfrak{d}]$ *so that* $\langle 1, \tau \rangle_{\mathbb{F}[T]} = \lambda \langle 1, \tau' \rangle_{\mathbb{F}[T]}$.

Proof: Let $\lambda = r\tau + s$, and then we have

$$\lambda \langle 1, \tau' \rangle_{\mathbb{F}[T]} = \lambda \left\langle 1, \frac{p\tau + q}{r\tau + s} \right\rangle_{\mathbb{F}[T]} = \langle r\tau + s, p\tau + q \rangle_{\mathbb{F}[T]} = \langle 1, \tau \rangle_{\mathbb{F}[T]} .$$

This is because for "$\supseteq$" We find that $1, \tau \in \langle r\tau + s, p\tau + q \rangle_{\mathbb{F}[T]}$ because

$$\tau = (ps - qr)\tau = s(p\tau + q) - q(r\tau + s)$$

$$1 = ps - qr = p(r\tau + s) - r(p\tau + q).$$

And that "$\subseteq$" is clear because $r\tau + s = s \cdot 1 + r \cdot \tau$, and likewise for $p\tau + q$. ■

Claim 4.5.6 *If there is a* $\lambda \in \mathbb{F}(T)[\mathfrak{d}]$ *so that* $\langle 1, \tau \rangle_{\mathbb{F}[T]} = \lambda \langle 1, \tau' \rangle_{\mathbb{F}[T]}$*, then there is a* $\begin{bmatrix} p & q \\ r & s \end{bmatrix} \in SL_2(\mathbb{F}[T])$ *so that* $\begin{bmatrix} p & q \\ r & s \end{bmatrix} \tau = \tau'$.

Proof: With the fact that $\lambda, \lambda\tau' \in \langle 1, \tau \rangle_{\mathbb{F}[T]}$ choose p, q, r, s so that $\lambda\tau' = p\tau + q$ and $\lambda = r\tau + s$. Then

$$\tau' = \frac{p\tau + q}{r\tau + s} = \begin{bmatrix} p & q \\ r & s \end{bmatrix} \tau.$$

Now $\begin{bmatrix} p & q \\ r & s \end{bmatrix}$ must be invertible because we could likewise write $\tau = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \tau'$, in which case we have $\tau = \begin{bmatrix} p & q \\ r & s \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} \tau'$ so that $\begin{bmatrix} p & q \\ r & s \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = I_2$. Thus because $\begin{bmatrix} p & q \\ r & s \end{bmatrix}$ is invertible, we have $\begin{bmatrix} p & q \\ r & s \end{bmatrix} \in GL_2(\mathbb{F}[T])$ and so by 4.5.4 we know that $f \backsim g$. In particular, $\begin{bmatrix} p & q \\ r & s \end{bmatrix} g = f$. Then we have

$$\frac{-b' + \sqrt{D}}{2a'} = \tau' = \frac{p\tau + q}{r\tau + s} = \frac{2aqs - bps - bqr + 2cpr + \sqrt{D}(ps - qr)}{2(as^2 - bsr + cr^2)} = \frac{-b' + (ps - qr)\sqrt{D}}{2a'},$$

where we used the fact that $\frac{p\tau+q}{r\tau+s} = \frac{2aqs-bps-bqr+2cpr+\sqrt{D}(ps-qr)}{2(as^2-bsr+cr^2)}$ as proven in Claim 4.5.3 and the other equalities are all by construction Next by equating the $\sqrt{D}$ parts, we find that

$$\frac{1}{2a'} = \frac{ps-qr}{2a'}$$

so that $ps - qr = 1$ and so $\begin{bmatrix} p & q \\ r & s \end{bmatrix} \in SL_2(\mathbb{F}[T])$. ■

Combining the above four claims we may obtain that $f \backsim g$ via γ if and only if $\gamma\tau = \tau'$ if and only if $\langle 1, \tau \rangle_{\mathbb{F}[T]}$ is equivalent to $\langle 1, \tau' \rangle_{\mathbb{F}[T]}$ in $I(\mathcal{O})/P(\mathcal{O})$. We now have by taking the forward implications that φ is well defined.

We have by taking the reverse implications that φ is injective. We still need to prove that it is surjective and a homomorphism. These are the next two lemmas.

Lemma 4.5.7 *φ is surjective.*

Proof: Recall that $\mathcal{O} = \left\langle 1, \sqrt{D} \right\rangle_{\mathbb{F}[T]}$. Let $\mathcal{C}' \in I(\mathcal{O})/P(\mathcal{O})$, and $[\mathfrak{a}] \in \mathcal{C}'$. That is, $\mathfrak{a}$ is a proper fractional ideal of $\mathcal{O}$. By this we know that we may write $\mathfrak{a} = \langle \alpha, \beta \rangle_{\mathbb{F}[T]}$ where $\alpha, \beta \in \mathbb{F}(T)[\mathfrak{d}]$, and α, β are $\mathbb{F}[T]$ independent. Then write $\tau := \frac{\beta}{\alpha}$ so that

$$\mathfrak{a} = \langle \alpha, \beta \rangle_{\mathbb{F}[T]} = \alpha \langle 1, \tau \rangle_{\mathbb{F}[T]}.$$

Let $ax^2 + bx + c$ be the minimal polynomial of τ (it must be of degree 2 because α and β are $\mathbb{F}[T]$ independent). We then know that $\tau = \frac{-b \pm \sqrt{D}}{2a}$. If $\tau = \frac{-b-\sqrt{D}}{2a}$ multiply $ax^2 + bx + c$ through by negative 1 so that without loss of generality $\tau = \frac{-b+\sqrt{D}}{2a}$. Then we have

$$\varphi([ax^2 + bx + c]) = \left[\left\langle a, \frac{-b+\sqrt{D}}{2} \right\rangle_{\mathbb{F}[T]} \right]$$

$$= \left[a \left\langle 1, \frac{-b+\sqrt{D}}{2a} \right\rangle_{\mathbb{F}[T]} \right]$$

$$= \left[\alpha \langle 1, \tau \rangle_{\mathbb{F}[T]} \right] = \mathcal{C}'$$

because $a \left\langle 1, \frac{-b+\sqrt{D}}{2a} \right\rangle_{\mathbb{F}[T]} = a\alpha^{-1} \left(\alpha \langle 1, \tau \rangle_{\mathbb{F}[T]} \right)$, so that these ideals are equivalent. We have thus constructed an element (namely, $[a, b, c]$) that maps to $\mathcal{C}'$. Hence φ is surjective.

■

Lemma 4.5.8 *φ is a homomorphism of groups.*

Proof: We know by 3.2.8 that given any two $\mathcal{C}_1, \mathcal{C}_2 \in Q(D)/\backsim$ we may choose $[a, b, a'c] \in \mathcal{C}_1$, $[a', b, ac] \in \mathcal{C}_2$ such that $\langle a, a' \rangle_{\mathbb{F}[T]} = \langle 1 \rangle_{\mathbb{F}[T]}$. Then we have

$$\begin{aligned}
\varphi'([[a,b,a'c]])\varphi'([[a',b,ac]]) &= \left[\left\langle a, \frac{-b+\sqrt{D}}{2}\right\rangle_{\mathbb{F}[T]}\right]\left[\left\langle a', \frac{-b+\sqrt{D}}{2}\right\rangle_{\mathbb{F}[T]}\right] \\
&= \left[\left\langle aa', a\frac{-b+\sqrt{D}}{2}, a'\frac{-b+\sqrt{D}}{2}, \left(\frac{-b+\sqrt{D}}{2}\right)^2\right\rangle_{\mathbb{F}[T]}\right] \\
&= \left[\left\langle aa', \frac{-b+\sqrt{D}}{2}\right\rangle_{\mathbb{F}[T]}\right] \\
&= \varphi'([[aa', b, c]]) \\
&= \varphi'([[a,b,a'c]][[a',b,ac]])
\end{aligned}$$

where the third equality is from C.2. ■

And we finally have the main result,

Theorem 4.5.9 *$Q(D)/\backsim \cong I(\mathcal{O})/P(\mathcal{O})$ as groups.*

Proof: The previous lemma's, and in fact everything in this section lead to this theorem. ■

Chapter 5

Conclusions and Discussion

After working out many of the results from [2] over $\mathbb{F}[T]$ we find that for the most part the results are mostly the same. We did stick to the case that 2 is a unit the entire time which simplified some proofs. It is not entirely clear what would happen in characteristic 2.

The primary difficulty in generalizing from $\mathbb{Z}$ is that we lose properties of the greatest common divisor. In particular, 3.2.4 explicitly fails to hold in a general unique factorization domain. Consider for instance any unique factorization domain which whose nontrivial generating sets have more than two elements. Such as $\mathbb{F}[x_1, x_2, x_3, x_4]$. Take the coefficients of f include at least one of x_1, x_2, while M includes x_3, and we shall never obtain x_4 by $\mathbb{F}[x_1, x_2, x_3, x_4]$ combinations of M and those elements represented by f. However, 3.2.4 and possibly A.1 are the only facts in the first part of the theory that relies on more than a general integral domain in which 2 is a unit.

In the specialization to $\mathbb{F}[T]$ we also run into the fact that we need to deal with the degree at times. For instance, while over $\mathbb{Z}$ one can talk fairly easily about a unique reduced form in every equivalence class, in $\mathbb{F}[T]$ we were able to determine no such classification . However, we were able to find a somewhat reduced form in each case (it usually is not unique).

In the latter part of the theory much notation was retained for intuition's sake, although some of the ideals and orders are simpler than in $\mathbb{Z}$. In particular, the mapping φ between $Q(D)/\backsim$ and $I(\mathcal{O})/P(\mathcal{O})$ can be stated less cumbersomely. We were also able to develop this equivalence of $Q(D)/\backsim$ and $I(\mathcal{O})/P(\mathcal{O})$ without the need of developing any theory regarding the conductor of $\mathcal{O}$ or norms.

One lingering question though regarding the previous comments, is as to whether we have

taken the best approach toward these forms. In particular, some things may have been more clear by dealing with the differing yet equivalent viewpoint and segregating forms $ax^2 + 2bxy + cy^2$ by their the determinant $ac - b^2$ instead of the discriminant.

Appendices

Appendix A Proofs of Random Things

Claim A.1 *With* $f \in Q(*)$, $\begin{bmatrix} p & q \\ r & s \end{bmatrix} f := f(px+qy, rx+sy)$, $GL_2(A)$ *acts on* $Q(*)$ *and* $SL_2(A)$ *acts on* $Q(D)$.

Proof: First let us prove that 2×2 matrices over A act on the set of all binary quadratic forms. By construction we have closure. Let $f = [a,b,c]$ be a binary quadratic form. Clearly $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} f = f$. Let $\begin{bmatrix} p & q \\ r & s \end{bmatrix}, \begin{bmatrix} p_2 & q_2 \\ r_2 & s_2 \end{bmatrix}$ be 2×2 matrices over A. Then we have by the Associativity of matrices,

$$\begin{aligned}
\left(\begin{bmatrix} p & q \\ r & s \end{bmatrix} \begin{bmatrix} p_2 & q_2 \\ r_2 & s_2 \end{bmatrix} \right) f &= \begin{bmatrix} x & y \end{bmatrix} \left(\begin{bmatrix} p & q \\ r & s \end{bmatrix} \begin{bmatrix} p_2 & q_2 \\ r_2 & s_2 \end{bmatrix} \right)^{\mathrm{T}} \begin{bmatrix} a & b \\ c & d \end{bmatrix} \left(\begin{bmatrix} p & q \\ r & s \end{bmatrix} \begin{bmatrix} p_2 & q_2 \\ r_2 & s_2 \end{bmatrix} \right) \begin{bmatrix} x \\ y \end{bmatrix} \\
&= \begin{bmatrix} x & y \end{bmatrix} \begin{bmatrix} p_2 & q_2 \\ r_2 & s_2 \end{bmatrix}^{\mathrm{T}} \begin{bmatrix} p & q \\ r & s \end{bmatrix}^{\mathrm{T}} \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} p & q \\ r & s \end{bmatrix} \begin{bmatrix} p_2 & q_2 \\ r_2 & s_2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \\
&= \begin{bmatrix} x & y \end{bmatrix} \begin{bmatrix} p_2 & q_2 \\ r_2 & s_2 \end{bmatrix}^{\mathrm{T}} \left(\begin{bmatrix} p & q \\ r & s \end{bmatrix}^{\mathrm{T}} \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} p & q \\ r & s \end{bmatrix} \right) \begin{bmatrix} p_2 & q_2 \\ r_2 & s_2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \\
&= \begin{bmatrix} p_2 & q_2 \\ r_2 & s_2 \end{bmatrix} \cdot \begin{bmatrix} x & y \end{bmatrix} \left(\begin{bmatrix} p & q \\ r & s \end{bmatrix}^{\mathrm{T}} \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} p & q \\ r & s \end{bmatrix} \right) \begin{bmatrix} x \\ y \end{bmatrix} \\
&= \begin{bmatrix} p_2 & q_2 \\ r_2 & s_2 \end{bmatrix} \left(\begin{bmatrix} p & q \\ r & s \end{bmatrix} f \right),
\end{aligned}$$

which gives us a group action. (This is actually an action from the right. But for convenience sake we will write it as an action from the left, and always remember that $(\gamma_1\gamma_2)f = \gamma_2(\gamma_1 f)$.

Second let us prove that $GL_2(A)$ acts on $Q(*)$.

The the primary difficulty here is closure. That is, to show that $\gamma f \in Q(*)$ when $\gamma \in GL_2(A)$ and $f \in Q(*)$. Let $\gamma \in GL_2(A)$. Then we know $\gamma^{-1} \in GL_2(A)$. Let $f \in Q(*)$. Then we know that we cannot have a common factor amongst the coefficients of f. That is, we cannot write $f = \alpha g$ with $\alpha \in A \setminus A^\star$ and g is some form over A (g is not necessarily primitive). Relying on the fact

that A is a PID, we know that this is if and only if. (That is, f fails to be primitive if and only if we can write $f = \alpha g$ as above).

Assume for the purpose of later contradiction that $\gamma f \notin Q(*)$. Then we can write $\gamma f = \alpha g$ where $\alpha \in A \setminus A^{\star}$. Then

$$\gamma^{-1}\gamma f = \gamma^{-1}\alpha g$$

$$\therefore f = \alpha\gamma^{-1} g$$

$$\therefore f = \alpha h.$$

where h is a binary quadratic form. But we know that $f \in Q(*)$, and so this is a contradiction. Hence $\gamma f \in Q(*)$. Then because $SL_2(A) \leq GL_2(A)$ we know that $SL_2(A)$ acts on $Q(*)$ as well.

Third let us prove that $SL_2(A)$ acts on $Q(D)$. We now need only show that the discriminant is the invariant under the action. Denote $\gamma := \begin{bmatrix} p & q \\ r & s \end{bmatrix} \in SL_2(A)$, then consider that

$\gamma f = [f(p,r), 2apq + bqr + bps + 2crs, f(q,s)]$, so that

$$\begin{aligned}
Disc(\gamma f) &= (2apq + bqr + bps + 2crs)^2 - 4f(p,r)f(q,s) \\
&= 4a^2p^2q^2 + 4abpq^2r + 4abp^2qs + 4apqrs + b^2q^2r^2 + 2b^2pqrs \\
&\quad +4bcqr^2s + b^2p^2s^2 + 4bcprs^2 + 4c^2r^2s^2 \\
&\quad -4(ap^2 + bpr + cr^2)(aq^2 + bqs + cs^2) \\
&= 4a^2p^2q^2 + 4abpq^2r + 4abp^2qs + 8acpqrs + b^2q^2r^2 + 2b^2pqrs \\
&\quad +4bcqr^2s + b^2p^2s^2 + 4bcprs^2 + 4c^2r^2s^2 \\
&\quad -4a^2p^2q^2 - 4abp^2qs - 4acp^2s^2 - 4abpq^2r - 4b^2pqrs - 4bcprs^2 - 4acq^2r^2 - 4bcqr^2s - 4c^2r^2s^2 \\
&= 8acpqrs + b^2q^2r^2 + b^2p^2s^2 \\
&\quad -4acp^2s^2 - 2b^2pqrs - 4acq^2r^2 \\
&= b^2q^2r^2 + b^2p^2s^2 - 2b^2pqrs - 4acpqrs - 4acp^2s^2 + 8acq^2r^2 \\
&= b^2(q^2r^2 + p^2s^2 - 2pqrs) - 4ac(p^2s^2 + q^2r^2 - 2pqrs) \\
&= b^2(q^2r^2 + ps(ps - qr) - pqrs) - 4ac(p^2s^2 + qr(qr - ps) - pqrs) \\
&= b^2(q^2r^2 + ps - pqrs) - 4ac(p^2s^2 - qr - pqrs) \\
&= b^2(qr(qr - ps) + ps) - 4ac(ps(ps - qr) - qr) \\
&= b^2(-qr + ps) - 4ac(ps - qr) \\
&= b^2 - 4ac.
\end{aligned}$$

Hence the discriminant is invariant under the action by $SL_2(A)$.

■

Claim A.2 *With $f \smile g$ iff there exist $\gamma \in GL_2(A)$ such that $\gamma f = g$, then $\smile$ is an equivalence relation.*

Proof: Let $f, g, h \in S(*)$ with $f \smile g$ and $g \smile h$.

Reflexive: Choosing $\gamma = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in GL_2(A)$ we have that $f \smile f$.

Symmetric: We have that there is a $\gamma \in GL_2(A)$ so that $\gamma f = g$. Inverting γ we then have

$\gamma^{-1}g = \gamma^{-1}\gamma f = f$, so that $g \backsim f$.

Transitive: Writing $\gamma_1 f = g, \gamma_2 g = h$ we then have that $h = \gamma_2 g = (\gamma_1\gamma_2)f$ so that $f \backsim h$.

■

Claim A.3 *With $f \backsim g$ iff there exist $\gamma \in SL_2(A)$ such that $\gamma f = g$, then $\backsim$ is an equivalence relation.*

Proof: Let $f, g, h \in S(*)$ with $f \backsim g$ and $g \backsim h$.

Reflexive: $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in SL_2(A)$ so that we have $f \backsim f$.

Symmetric: We have that there is a $\gamma \in SL_2(A)$ so that $\gamma f = g$. Inverting γ we then have $\gamma^{-1}g = \gamma^{-1}\gamma f = f$. Now, $\det(\gamma^{-1}) = 1^{-1} = 1$ so that $\gamma^{-1} \in SL_2(A)$. Thus so that $g \backsim f$.

Transitive: Writing $\gamma_1 f = g, \gamma_2 g = h$ we then have that $h = \gamma_2 g = (\gamma_1\gamma_2)f$ so that $f \backsim h$, because $\det(\gamma_1\gamma_2) = 1 \cdot 1 = 1$. ■

Claim A.4 *With $f = [a, b, c] \in Q(D)$, $B = 2an + b = 2a'n' + b'$, then $C := \frac{B^2 - D}{4aa'} \in A$.*

Proof: We know that $D = b^2 - 4ac$, and $B - b = 2na$. Thus

$$B^2 - D = B^2 - (b^2 - 4ac) = (B - b)(B + b) + 4ac = 2na(B + b) + 4ac = a(2n(B + b) + 4c).$$

so that $a|B^2 - D$. Similarly $a'|B^2 - D$. Because $\langle a, a' \rangle_A = \langle 1 \rangle_A$ we then know that $aa'|B^2 - D$. $4 \in \mathbb{F}$, and so $C \in A$. ■

Claim A.5 *With $f_1 = [a, b, c]$, $B = 2an + b = 2a'n' + b$, then* $\begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} f = [a_2, B, a_1 C]$.

Proof: First by A.4 we see that

$$\frac{B^2 - D}{4aa'} = \frac{a(2n(B + b) + 4c)}{4aa'} = \frac{2na(2b + 2an) + 4ac}{4aa'} = \frac{(4abn + 4a^2n^2 + 4ac)}{4aa'} \in A.$$

This will be C. Then by using 3.2.1 we obtain

$$\begin{aligned}
\begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} f &= [f(1,0), 2an+b, f(n,1)] \\
&= [f(1,0), B, an^2+bn+c] \\
&= [f(1,0), B, \frac{(4aa')(bn+an^2+c)}{4aa'}] \\
&= [f(1,0), B, a'\frac{(4abn+4a^2n^2+4ac)}{4aa'}] \\
&= [f(1,0), B, a_1 C].
\end{aligned}$$

■

Claim A.6 *With $f=[a,b,c] \in Q(*)$,$r=\prod_j p_j$ and $s=\prod_i m_i$ where $M=\prod_i m_i \prod_j p_j \prod_k q_k$ with m_i, p_i, q_k all irreducible, $m_i \nmid a$, $p_j | a, p_j \nmid c$, and $q_k | a, q_k | c, q_k \nmid b$, then $(f(r,s), M) = (1)$.*

Proof: Consider that

$$\begin{aligned}
f(r,s) &= a\left(\prod_j p_j\right)^2 + b\left(\prod_j p_j\right)\left(\prod_i m_i\right) + c\left(\prod_i m_i\right)^2 \\
&= q_1 \prod_i m_i + a\left(\prod_j p_j\right)^2 \\
&= q_2 \prod_k q_k + b\left(\prod_j p_j\right)\left(\prod_i m_i\right) \\
&= q_3 \prod_j p_j + c\left(\prod_i m_i\right)^2.
\end{aligned}$$

so that in the case of each irreducible divisor α of M, α divides precisely two terms of $f(r,s)$ and thus does not divide $f(r,s)$ (the second equality uses the fact that $q_k | a, q_k | c$). Hence because no irreducible divisor M is also an irredicuble divisor of $f(r,s)$, we must have $\langle f(r,s), M\rangle_A = \langle 1\rangle_A$. ■

Claim A.7 *With $f_1=[a_1,b,a_2c]$, $f_2=[a_2,b,a_1c]$, $\begin{bmatrix} r & t \\ s & u \end{bmatrix} f_2 = g_2$, $\begin{bmatrix} r & t \\ s & u \end{bmatrix} \in SL_2(A)$, $a_1 = a_1'$, $a_2c = a_2'c'$, and $\langle a_1, a_2'\rangle_A = \langle 1\rangle_A$ then $ta_2' = -sa_1c$, $a_2t = -sa_1c'$, $ua_2' = ra_2 + bs$, and $c'r =$*

$uc + bt/a_1$.

Proof: By inverting γ and noting that $a_1' = a_1$ we get that,

$$\begin{bmatrix} r & s \\ t & u \end{bmatrix} \begin{bmatrix} a_2 & b/2 \\ b/2 & a_1 c \end{bmatrix} = \begin{bmatrix} a_2' & b/2 \\ b/2 & a_1 c' \end{bmatrix} \begin{bmatrix} u & -t \\ -s & r \end{bmatrix},$$

which gives the following four equations.

$$ra_2 + bs/2 = ua_2' - bs/2$$

$$\frac{br}{2} + sa_1 c = -a_2' t + \frac{br}{2}$$

$$a_2 t + \frac{bu}{2} = \frac{bu}{2} - a_1 c' s$$

$$bt/2 + uca_1 = -bt/2 + a_1 c' r,$$

which give respectively,

$$ua_2' = ra_2 + bs$$

$$ta_2' = -sa_1 c$$

$$a_2 t = -sa_1 c'$$

$$a_1 c' r = uca_1 + bt.$$

In the last, we note that $t/a_1 \in A$ and so we have $c'r = uc + bt/a_1$.

■

Claim A.8 *With* $\begin{bmatrix} r & t \\ s & u \end{bmatrix} \in SL_2(A)$, $ta_2' = -sa_1 c$, *and* $\langle a_1, a_2' \rangle_A = \langle 1 \rangle_A$, *then* $\begin{bmatrix} r & t/a_1 \\ sa_1 & u \end{bmatrix} \in SL_2(A)$.

Proof: To be in $SL_2(A)$, we must have $\det\left(\begin{bmatrix} r & t/a_1 \\ sa_1 & u \end{bmatrix}\right) = 1$, and all the entries in A. Indeed $t/a_1 \in A$ because $a_1 | t$, and so $\det\left(\begin{bmatrix} r & t/a_1 \\ sa_1 & u \end{bmatrix}\right) = ru - st = \det\left(\begin{bmatrix} r & t \\ s & u \end{bmatrix}\right) = 1$. ■

Claim A.9 *With* $f_1 = [a_1, b, a_2c], f_2 = [a_2, b, a_1c]$ *and* $g_1 = [a_1', b', a_2'c'], g_2 = [a_2', b', a_1'c']$, $f_1 = g_1$, $\langle a_1, a_2' \rangle_A = \langle 1 \rangle_A$, $f_1 \backsim g_1$, $f_2 \backsim g_2$, *then* $g_1 * g_2 \backsim f_1 * f_2$.

Proof: First note that because $f_1 = g_1$ we know that $a_1 = a_1'$, and that $a_2c = a_2'c'$. In fact, the equivalence we want is via $\gamma' := \begin{bmatrix} r & t/a_1 \\ sa_1 & u \end{bmatrix}$, by verifying that $\gamma'(f_1 * f_2) = g_1 * g_2$, which is to say that

$$\begin{bmatrix} r & sa_1 \\ t/a_1 & u \end{bmatrix} \begin{bmatrix} a_1a_2 & b/2 \\ b/2 & c \end{bmatrix} \begin{bmatrix} r & t/a_1 \\ sa_1 & u \end{bmatrix} = \begin{bmatrix} a_1'a_2' & b/2 \\ b/2 & c' \end{bmatrix},$$

which is equivalent to showing that

$$\begin{bmatrix} r & sa_1 \\ t/a_1 & u \end{bmatrix} \begin{bmatrix} a_1a_2 & b/2 \\ b/2 & c \end{bmatrix} = \begin{bmatrix} a_1'a_2' & b/2 \\ b/2 & c' \end{bmatrix} \begin{bmatrix} u & -t/a_1 \\ -sa_1 & r \end{bmatrix},$$

The left hand side is

$$\begin{bmatrix} r & sa_1 \\ t/a_1 & u \end{bmatrix} \begin{bmatrix} a_1a_2 & b/2 \\ b/2 & c \end{bmatrix} = \begin{bmatrix} ra_1a_2 + bsa_1/2 & br/2 + sca_1 \\ a_2t + bu/2 & bt/(2a_1) + uc \end{bmatrix},$$

while indeed the right hand side is

$$\begin{aligned} \begin{bmatrix} a_1'a_2' & b/2 \\ b/2 & c' \end{bmatrix} \begin{bmatrix} u & -t/a_1 \\ -sa_1 & r \end{bmatrix} &= \begin{bmatrix} a_1a_2' & b/2 \\ b/2 & c' \end{bmatrix} \begin{bmatrix} u & -t/a_1 \\ -sa_1 & r \end{bmatrix} \\ &= \begin{bmatrix} a_1a_2'u - bsa_1/2 & br/2 - a_2't \\ bu/2 - c'sa_1 & rc' - bt/(2a_1) \end{bmatrix} \\ &= \begin{bmatrix} ra_1a_2 + bsa_1 - bsa_1/2 & br/2 + sca_1 \\ bu/2 + a_2t & uc + bt/a_1 - bt/(2a_1) \end{bmatrix} \\ &= \begin{bmatrix} ra_1a_2 + bsa_1/2 & br/2 + sca_1 \\ bu/2 + a_2t & uc + bt/(2a_1) \end{bmatrix}. \end{aligned}$$

using the identies found in $A.7$ for the last equality. This is the same as the left hand side, and so proves the claim. ■

Claim A.10 *With* $f_1 = [a_1, b, a_2c], f_2 = [a_2, b, a_1c]$ *and* $g_1 = [a_1', b', a_2'c'], g_2 = [a_2', b', a_1'c']$, $b = b'$,

$\langle a_1, a_2' \rangle_A = \langle 1 \rangle_A$, $f_1 \backsim g_1$, $f_2 \backsim g_2$, *then* $[g_2 * g_1] = [g_2 * f_1]$.

Proof: By comparing (g_2, g_1) with (g_2, f_1) we may apply case 1, and so this is indeed similar. ■

Claim A.11 *With* $f_1 = [a_1, b, a_2 c], f_2 = [a_2, b, a_1 c]$ *and* $g_1 = [a_1', b', a_2' c'], g_2 = [a_2', b', a_1' c']$,$B = b + 2a_1 a_2 n = b' + 2a_1 a_2 n'$, $f_1 \backsim g_1$, $f_2 \backsim g_2$, $F_1 := \begin{bmatrix} 1 & a_2 n \\ 0 & 1 \end{bmatrix} f_1$, $F_2 := \begin{bmatrix} 1 & a_1 n \\ 0 & 1 \end{bmatrix} f_2$, $G_1 := \begin{bmatrix} 1 & a_2' n' \\ 0 & 1 \end{bmatrix} g_1$, $G_2 := \begin{bmatrix} 1 & a_1' n' \\ 0 & 1 \end{bmatrix} g_2$, $H_1 := \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} f_1 * f_2 = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} [a_1 a_2, b/2, c]$, $H_2 := \begin{bmatrix} 1 & n' \\ 0 & 1 \end{bmatrix} g_1 * g_2 = \begin{bmatrix} 1 & n' \\ 0 & 1 \end{bmatrix} [a_1' a_2', b'/2, c']$, *then* $F_1 = [a_1, B/2, *]_D$, $F_2 = [a_2, B/2, *]_D$, $G_1 = [a_1', B/2, *]_D$, $G_2 = [a_2', B/2, *]_D$, $H_1 = [a_1 a_2, B/2, *]_D$, *and* $H_2 = [a_1' a_2', B/2, *]_D$.

Proof: The equality for F_1 (and similarly G_1) is because

$$\begin{aligned}
\begin{bmatrix} 1 & 0 \\ a_2 n & 1 \end{bmatrix} \begin{bmatrix} a_1 & b/2 \\ b/2 & a_2 c \end{bmatrix} \begin{bmatrix} 1 & a_2 n \\ 0 & 1 \end{bmatrix} &= \begin{bmatrix} a_1 & b/2 \\ a_1 a_2 n + b/2 & a_2 bn/2 + a_2 c \end{bmatrix} \begin{bmatrix} 1 & a_2 n \\ 0 & 1 \end{bmatrix} \\
&= \begin{bmatrix} a_1 & a_1 a_2 n + b/2 \\ a_1 a_2 n + b/2 & a_1 a_2^2 n^2 + b a_2 n/2 + a_2 bn/2 + a_2 c \end{bmatrix} \\
&= \begin{bmatrix} a_1 & B/2 \\ B/2 & a_1 a_2^2 n^2 + b a_2 n/2 + a_2 bn/2 + a_2 c \end{bmatrix} \\
&= \begin{bmatrix} a_1 & B/2 \\ B/2 & a_1 a_2^2 n^2 + a_2 bn + a_2 c \end{bmatrix} \\
&= \begin{bmatrix} a_1 & B/2 \\ B/2 & a_2(a_1 a_2 n^2 + bn + c) \end{bmatrix}.
\end{aligned}$$

The equalitiy for F_2 (and similarly G_2) is because

$$\begin{aligned}
\begin{bmatrix} 1 & 0 \\ a_1 n & 1 \end{bmatrix} \begin{bmatrix} a_2 & b/2 \\ b/2 & a_1 c \end{bmatrix} \begin{bmatrix} 1 & a_1 n \\ 0 & 1 \end{bmatrix} &= \begin{bmatrix} a_2 & b/2 \\ a_1 a_2 n + b/2 & a_1 bn/2 + a_1 c \end{bmatrix} \begin{bmatrix} 1 & a_1 n \\ 0 & 1 \end{bmatrix} \\
&= \begin{bmatrix} a_2 & a_1 a_2 n + b/2 \\ a_1 a_2 n + b/2 & a_1^2 a_2 n^2 + a_1 bn + a_1 bn/2 + a_1 c \end{bmatrix} \\
&= \begin{bmatrix} a_2 & B/2 \\ B/2 & a_1(a_1 a_2 n^2 + bn + c) \end{bmatrix}.
\end{aligned}$$

The equality for H_1 (and similarly H_2) is because

$$\begin{aligned}
\begin{bmatrix} 1 & 0 \\ n & 1 \end{bmatrix} \begin{bmatrix} a_1 a_2 & b/2 \\ b/2 & c \end{bmatrix} \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} &= \begin{bmatrix} a_1 a_2 & b/2 \\ a_1 a_2 n + b/2 & nb/2 + c \end{bmatrix} \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} \\
&= \begin{bmatrix} a_1 a_2 & a_1 a_2 n + b/2 \\ a_1 a_2 n + b/2 & a_1 a_2 n^2 + bn + c \end{bmatrix} \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} \\
&= \begin{bmatrix} a_1 a_2 & B/2 \\ B/2 & a_1 a_2 n^2 + bn + c \end{bmatrix}.
\end{aligned}$$

■

Claim A.12 *With* $F_1 = [a_1, B/2, a_2(a_1 a_2 n^2 + bn + c)]$, $F_2 = [a_2, B/2, a_1(a_1 a_2 n^2 + bn + c)]$, $H_1 = [a_1 a_2, B/2, a_1 a_2 n^2 + bn + c]$, *and* $\langle a_1 a_2, a_1' a_2' \rangle_A = \langle 1 \rangle_A$, *then* F_1 *and* F_2 *are concordant, and* $F_1 * F_2 = H_1$.

Proof: Denote $C = a_1 a_2 n^2 + bn + c$, so that $F_1 = [a_1, B/2, a_2 C]$ and $F_2 = [a_2, B/2, a_1 C]$. Hence by construction F_1 and F_2 are concordant. (note that $a_1 a_2 \neq 0$ because f_1 and f_2 are concordant). Further merely by writing out what we have defined as composition we then know that $F_1 * F_2 = [a_1 a_2, B/2, C] = H_1$. ■

Claim A.13 *With* $f_0 = [1, 0, -\frac{D}{4}]$, *then* $\begin{bmatrix} 1 & b/2 \\ & 1 \end{bmatrix} f_0 = [1, b, ac]$ *and* $\begin{bmatrix} 1 & -b/2 \\ 0 & 1 \end{bmatrix} f_0 = [1, -b, ac]$.

Proof: This is because

$$\begin{aligned}\begin{bmatrix} 1 & 0 \\ b/2 & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & -D/4 \end{bmatrix}\begin{bmatrix} 1 & b/2 \\ 0 & 1 \end{bmatrix} &= \begin{bmatrix} 1 & 0 \\ b/2 & -D/4 \end{bmatrix}\begin{bmatrix} 1 & b/2 \\ 0 & 1 \end{bmatrix} \\ &= \begin{bmatrix} 1 & b/2 \\ b/2 & b^2/4 - D/4 \end{bmatrix} \\ &= \begin{bmatrix} 1 & b/2 \\ b/2 & ac \end{bmatrix},\end{aligned}$$

and

$$\begin{aligned}\begin{bmatrix} 1 & 0 \\ -b/2 & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & D/4 \end{bmatrix}\begin{bmatrix} 1 & -b/2 \\ 0 & 1 \end{bmatrix} &= \begin{bmatrix} 1 & 0 \\ -b/2 & D/4 \end{bmatrix}\begin{bmatrix} 1 & -b/2 \\ 0 & 1 \end{bmatrix} \\ &= \begin{bmatrix} 1 & -b/2 \\ -b/2 & b^2/4 + D/4 \end{bmatrix} \\ &= \begin{bmatrix} 1 & -b/2 \\ -b/2 & ac \end{bmatrix}.\end{aligned}$$

■

Claim A.14 *For $\mathcal{C} \in Q(D)/\backsim$, there always exists a form in $\mathcal{C}$ with nonzero first and third coefficient.*

Proof: If $f = [0, b, 0]$ take $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} f$. If $f = [c, -b, 0]$ then without loss of generality we may take $f = [0, b, c]$. For $f = [0, b, c]$ then either $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} f = [a, 2a + b, a + b]$ or $\begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} f = [a, 4a + b, 4a + b]$ has nonzero first and third coefficient. Lastly if $f = [a, 0, 0]$ take $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} f = [a, 2a, a]$. ■

Claim A.15 *With* $g_1 := \begin{bmatrix} 1 & n_1 \\ 0 & 1 \end{bmatrix} f_1$, $g_2 := \begin{bmatrix} 1 & n_2 \\ 0 & 1 \end{bmatrix} f_2$, $g_3 := \begin{bmatrix} 1 & n_3 \\ 0 & 1 \end{bmatrix} f_3$, *then* $g_1 = [a_1, B, \delta_1]$, $g_2 = [a_2, B, \delta_2]$, $g_3 = [a_3, B, \delta_3]$ *for some appropriate* $\delta_1, \delta_2, \delta_3$.

Proof: The equality for g_1 (and similarly g_2) are because

$$\begin{aligned}
\begin{bmatrix} 1 & 0 \\ n_1 & 1 \end{bmatrix} \begin{bmatrix} a_1 & b_1/2 \\ b_1/2 & a_2c_1 \end{bmatrix} \begin{bmatrix} 1 & n_1 \\ 0 & 1 \end{bmatrix} &= \begin{bmatrix} a_1 & b_1/2 \\ a_1n_1 + b_1/2 & b_1n_1 + a_2c_1 \end{bmatrix} \begin{bmatrix} 1 & n_1 \\ 0 & 1 \end{bmatrix} \\
&= \begin{bmatrix} a_1 & a_1n_1 + b_1/2 \\ a_1n_1 + b_1/2 & a_1n_1^2 + b_1n_1/2 + b_1n_1 + a_2c_1 \end{bmatrix} \\
&= \begin{bmatrix} a_1 & B/2 \\ B/2 & a_1n_1^2 + b_1n_1/2 + b_1n_1 + a_2c_1 \end{bmatrix}.
\end{aligned}$$

The equality for g_3 is because

$$\begin{aligned}
\begin{bmatrix} 1 & 0 \\ n_3 & 1 \end{bmatrix} \begin{bmatrix} a_3 & b_3/2 \\ b_3/2 & c_3 \end{bmatrix} \begin{bmatrix} 1 & n_3 \\ 0 & 1 \end{bmatrix} &= \begin{bmatrix} a_3 & b_3/2 \\ a_3n_3 + b_3/2 & b_3n_3/2 + c_3 \end{bmatrix} \begin{bmatrix} 1 & n_3 \\ 0 & 1 \end{bmatrix} \\
&= \begin{bmatrix} a_3 & a_3n_3 + b_3/2 \\ a_3n_3 + b_3/2 & a_3n_3^2 + b_3n_3/2 + b_3n_3/2 + c_3 \end{bmatrix} \\
&= \begin{bmatrix} a_3 & B/2 \\ B/2 & a_3n_3^2 + b_3n_3/2 + b_3n_3/2 + c_3 \end{bmatrix}.
\end{aligned}$$

Labeling δ_i appropriately, we have the desired equalities.

■

Claim A.16 *With $g_1 = [a_1, B, \delta_1]$, $g_2 = [a_2, B, \delta_2]$, $g_3 = [a_3, B, \delta_3]$, and $\langle a_3, a_1a_2 \rangle_A = \langle 1 \rangle_A$, then $g_1 * g_2 * g_3$ is unambiguous.*

Proof: First note that $D = B^2 - 4a_1\delta_1 = B^2 - 4a_2\delta_2$ so that $a_1|\delta_2$ and $a_2|\delta_1$. Thus by 3.2.7 g_2 and g_2 are concordant. Denote $g_1 * g_2 = [a_1a_2, B, \epsilon_1]$. Now note that $g_1 * g_2$ and g_3 are concordant again by 3.2.7 because $D = B^2 - 4a_1a_2\epsilon_1 = B^2 - 4a_3\delta_3$ and $\langle a_1a_2, a_3 \rangle_A = \langle 1 \rangle_A$. Hence we have

$$(g_1 * g_2) * g_3 = [a_1a_2a_3, B, \epsilon_2].$$

Next we have that g_2 and g_3 are concordant because $\langle a_2, a_3 \rangle_A = \langle 1 \rangle_A$ and $D = B^2 - 4a_2\delta_2 = B^2 - 4a_3\delta_3$. Denote $g_2 * g_3 = [a_2a_3, B, \epsilon_3]$. Then g_1 and $g_2 * g_3$ are concordant because

$\langle a_1, a_2a_3\rangle_A = \langle 1\rangle_A$ and $D = B^2 - 4a_1\delta_1 = B^2 - 4a_1a_2\epsilon_3$. Hence we have

$$g_1 * (g_2 * g_3) = [a_1a_2a_3, B, \epsilon_4].$$

Now, finally, $\epsilon_4 = \epsilon_2$ because $D = B^2 - 4a_1a_2a_3\epsilon_4 = B^2 - 4a_1a_2a_3\epsilon_2$. Therefore $g_1 * g_2 * g_3$ is unambiguous. ■

Appendix B Proofs of Some More Random Things

Claim B.1 *With $f = [a, b, c]$ where two of a, b, c are zero and the other is a unit, then* $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} f$ *has two nonzero entries.*

Proof: Suppose that a (or c before a change of variables) is the nonzero coefficient, then

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} f = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} f[a, 0, 0] = [a, 2a, a].$$

Suppose that b is the nonzero coefficient, then

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} f = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} f[0, b, 0] = [0, b, b].$$

■

Claim B.2 *With $a = 0, b \neq 0, c \neq 0$, one of* $\begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} f$, $\begin{bmatrix} 3 & 1 \\ 2 & 1 \end{bmatrix} f$, $\begin{bmatrix} 3 & 2 \\ 1 & 1 \end{bmatrix} f$ *has all nonzero coefficients.*

Proof: We will work out that $\begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} f = [2b+c, 3b+2c, b+c]$, $\begin{bmatrix} 3 & 1 \\ 2 & 1 \end{bmatrix} f = [2(3b+2c), 5b+4c, b+c]$, $\begin{bmatrix} 3 & 2 \\ 1 & 1 \end{bmatrix} f = [3b+c, 5b+2c, 2b+c]$. Then we will note that either there is no $\mathbb{F}$ combination of b, c to give zero, in which case all three have nonzero entires. Or if there is, such a combination is unique, all of these three forms do not have a coefficient in common. (each coefficient is a $\mathbb{F}$ combination, and so this shows that at least one of them must have all nonzero coefficients). With that we will

be done.

$$\begin{aligned}
\begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}[0,b,c] &= \begin{bmatrix} x & y \end{bmatrix}\begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} 0 & b/2 \\ b/2 & c \end{bmatrix}\begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} x \\ y \end{bmatrix} \\
&= \begin{bmatrix} x & y \end{bmatrix}\begin{bmatrix} b/2 & b+c \\ b/2 & b/2+c \end{bmatrix}\begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} x \\ y \end{bmatrix} \\
&= \begin{bmatrix} x & y \end{bmatrix}\begin{bmatrix} 2b+c & 3b/2+c \\ 3b/2+c & b+c \end{bmatrix}\begin{bmatrix} x \\ y \end{bmatrix}. \\
&= [2b+c, 3b+2c, b+c]
\end{aligned}$$

$$\begin{aligned}
\begin{bmatrix} 3 & 1 \\ 2 & 1 \end{bmatrix}[0,b,c] &= \begin{bmatrix} x & y \end{bmatrix}\begin{bmatrix} 3 & 2 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} 0 & b/2 \\ b/2 & c \end{bmatrix}\begin{bmatrix} 3 & 1 \\ 2 & 1 \end{bmatrix}\begin{bmatrix} x \\ y \end{bmatrix} \\
&= \begin{bmatrix} x & y \end{bmatrix}\begin{bmatrix} b & 3b/2+2c \\ b/2 & b/2+c \end{bmatrix}\begin{bmatrix} 3 & 1 \\ 2 & 1 \end{bmatrix}\begin{bmatrix} x \\ y \end{bmatrix} \\
&= \begin{bmatrix} x & y \end{bmatrix}\begin{bmatrix} 6b+4c & 5b/2+2c \\ 5b/2+2c & b+c \end{bmatrix}\begin{bmatrix} x \\ y \end{bmatrix}. \\
&= [2(3b+2c), 5b+4c, b+c]
\end{aligned}$$

$$\begin{aligned}
\begin{bmatrix} 3 & 2 \\ 1 & 1 \end{bmatrix}[0,b,c] &= \begin{bmatrix} x & y \end{bmatrix}\begin{bmatrix} 3 & 1 \\ 2 & 1 \end{bmatrix}\begin{bmatrix} 0 & b/2 \\ b/2 & c \end{bmatrix}\begin{bmatrix} 3 & 2 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} x \\ y \end{bmatrix} \\
&= \begin{bmatrix} x & y \end{bmatrix}\begin{bmatrix} b/2 & 3b/2+c \\ b/2 & b+c \end{bmatrix}\begin{bmatrix} 3 & 2 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} x \\ y \end{bmatrix} \\
&= \begin{bmatrix} x & y \end{bmatrix}\begin{bmatrix} 3b+c & 5b/2+c \\ 5b/2+c & 2b+c \end{bmatrix}\begin{bmatrix} x \\ y \end{bmatrix}. \\
&= [3b+c, 5b+2c, 2b+c]
\end{aligned}$$

■

Claim B.3 *With $a, b \in \mathbb{F}[T]$, $\mathfrak{d}$ the square root of a squarefree element of $\mathbb{F}[T]$, then $\langle 1, a\mathfrak{d} + b\rangle_{\mathbb{F}_{(T)}} = \mathbb{F}(T)[\mathfrak{d}]$.*

Proof: ($\subseteq$) Trivial.

($\supseteq$) Let $\gamma + \lambda\mathfrak{d}$ be an arbitrary element of $\mathbb{F}(T)[\mathfrak{d}]$. (so $\gamma, \lambda, a, b \in \mathbb{F}(T)$) Then $\gamma + \lambda\mathfrak{d} = \left(\lambda a^{-1}\right) \cdot (a\mathfrak{d} + b) + \left(\gamma - b\lambda a^{-1}\right) \cdot 1$. ■

Claim B.4 *With $f = [a, b, c] \in Q(*)$, $b + 2ma = r$ where $r = 0$ or $\deg(r) < \deg(a)$, $a, b, c, m, r \in \mathbb{F}[T]$ and $[a_2, b_2, c_2] = \begin{bmatrix} 1 & m \\ 0 & 1 \end{bmatrix} f$, then $\deg(b_2) < \deg(a_2) = \deg(a)$.*

Proof: First note that the case $r = 0$ is redundant but was stated for completeness sake because r comes from the division algorithm. This is because if $r = 0$, $\deg(r) = -\infty$ and so $\deg(r) < \deg(a)$ anyway. (if $a = 0$ we already showed that we can reduce f so that $a \neq 0$). In any event, let us work out that

$$\begin{aligned}
\begin{bmatrix} 1 & m \\ 0 & 1 \end{bmatrix} [a, b, c] &= \begin{bmatrix} x & y \end{bmatrix} \begin{bmatrix} 1 & 0 \\ m & 1 \end{bmatrix} \begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix} \begin{bmatrix} 1 & m \\ 0 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \\
&= \begin{bmatrix} x & y \end{bmatrix} \begin{bmatrix} a & b/2 \\ b/2 + am & bm/2 + c \end{bmatrix} \begin{bmatrix} 1 & m \\ 0 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \\
&= \begin{bmatrix} x & y \end{bmatrix} \begin{bmatrix} a & b/2 + am \\ b/2 + am & bm/2 + am^2 + bm/2 + c \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \\
&= [a, b + 2am, am^2 + bm + c] \\
&= [a, r, am^2 + bm + c] \\
&= [a_2, b_2, c_2].
\end{aligned}$$

Thus $a_2 = a$, $b_2 = r$, so that indeed $\deg(b_2) < \deg(a_2) = \deg(a)$.

■

Claim B.5 *There are $n, m \in \mathbb{F}[T]$ so that $\beta = m + n\tau$ and $a|n$ iff $\beta \in \langle 1, a\tau\rangle_{\mathbb{F}[T]}$.*

Proof: This is quite easy once you think about it: ($\Rightarrow$) Trivial: Write $\beta = m + n'a\tau$. ($\Leftarrow$) Nearly as trivial: Write $\beta = m + n'a\tau$, and then define $n := n'a$. ■

Appendix C Proofs of Random Things Relating To the Class Group Isomorphism

Claim C.1 *With* $b \in \mathbb{F}[T]$*, then* $\left\langle 1, \frac{-b-\sqrt{D}}{2} \right\rangle_{\mathbb{F}[T]} = \left\langle 1, \sqrt{D} \right\rangle_{\mathbb{F}[T]}$.

Proof: ($\subseteq$) is trivial by noting that $2 \in \mathbb{F}[T]$.

($\supseteq$): Let $\alpha + \beta\sqrt{D}$ be an arbitrary element in $\left\langle 1, \sqrt{D} \right\rangle_{\mathbb{F}[T]}$. Then $\alpha + \beta\sqrt{D} = (\alpha + \beta b) \cdot 1 + 2\beta \cdot \left(\frac{-b+\sqrt{D}}{2}\right) \in \left\langle 1, \frac{-b+\sqrt{D}}{2} \right\rangle_{\mathbb{F}[T]}$. ■

Claim C.2 *With* $a, a', b, \in \mathbb{F}[T]$ *then* $\left\langle aa', a\frac{-b+\sqrt{D}}{2}, a'\frac{-b+\sqrt{D}}{2}, \left(\frac{-b+\sqrt{D}}{2}\right)^2 \right\rangle_{\mathbb{F}[T]} = \left\langle aa', \frac{-b+\sqrt{D}}{2} \right\rangle_{\mathbb{F}[T]}$

Proof:

($\subseteq$): This is trivial because the latter three generators of $\left\langle aa', a\frac{-b+\sqrt{D}}{2}, a'\frac{-b+\sqrt{D}}{2}, \left(\frac{-b+\sqrt{D}}{2}\right)^2 \right\rangle_{\mathbb{F}[T]}$ are multiples of $\frac{-b+\sqrt{D}}{2}$.

($\supseteq$): Because $(a, a') = (1)$, we can write $\lambda a + \gamma a' = 1$, and thus

$$\frac{-b+\sqrt{D}}{2} = \lambda a \frac{-b+\sqrt{D}}{2} + \gamma a' \frac{-b+\sqrt{D}}{2},$$

and so we have equality. ■

Bibliography

[1] J.W.S. Cassels. *Rational Quadratic Forms.* Academic Press, 1978.

[2] David A. Cox. *Primes of the form $x^2 + ny^2$.* Wiley, 1989.

[3] Daniel D. Flath. *Introduction to Number Theory.* Wiley, 1988.

[4] Thomas W. Hungerford. *Algebra.* Springer, 2003.

[5] N.J.A. Sloane John H. Conway. *Sphere packings, lattices, and groups.* Springer-Verlag, 1993.

[6] A.V. Malyshev. Quadratic form. http://eom.springer.de/Q/q076080.htm, 2001.

[7] O.T O'Meara. *Introduction to Quadratic Forms.* Academic Press, 1963.

[8] Catherine M. Trentacoste. Construction of a dimension two rank one drinfeld module. Masters Thesis, 2009.

Index