Gauss Composition and Higher Analogues

Pan Jing Bin

Supervisor: A/P Chin Chee Whye

Department of Mathematics

National University of Singapore

UROPS Write up

Contents

1 Introduction

The existence of an underlying group structure on binary quadratic forms was first discovered by Gauss and published in his acclaimed 1801 paper *Disquisitiones Arithmeticae*. Later on in the 19th century, the theory of ideals was developed to study integer solutions of polynomial equations such as the infamous Fermat's Last Theorem. It was then that Mathematicians quickly realised that the theory of binary quadratic forms is just a special case of a much more elegant and abstract theory. Since then, binary quadratic forms have gradually been overshadowed by the theory of algebraic number fields.

Nevertheless, developments in this neglected theory still occur occasionally. In the present, Canadian-American mathematician Manjul Bhargava developed a new formulation Gauss's composition using a configuration of integers which is now known as Bhargava's cube. The cube allow Gauss's composition to be generalised elegantly to higher analogues, and Bhargava went on to define 14 new composition laws.

In this report, chapter 2 will first give a brief review of the classical theory of binary quadratic forms due to Gauss. In chapter 3, we will explore the ideal class group in the general setting of Dedekind domains. In chapter 4, we will introduce the concepts from algebraic number theory that are necessary to make the connection between Dedekind domains and algebraic number rings. We will then focus our discussion on quadratic rings in chapter 5, before finishing off by establishing the relationship between binary quadratic forms and the ideal class group. Chapter 6 will then talk about Bhargava's reformulation of Gauss composition.

2 Classical Theory of Binary Quadratic Forms

This chapter reviews the theory of binary quadratic form which we shall assume throughout the report. As such, all proofs will be omitted.

2.1 Basic Theory

Definition 2.1.1. A **binary quadratic form** f is a quadratic homogeneous polynomial in two variables

$$f(x,y) = ax^2 + bxy + cy^2 = \begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}.$$

If $a, b, c \in \mathbb{Z}$, then f is an **integral binary quadratic form**. Unless stated otherwise, all binary quadratic forms in this paper are assumed to be integral.

Definition 2.1.2. The **discriminant** Δ of a binary quadratic form $ax^2 + bxy + cy^2$ is given by

$$\Delta = b^2 - 4ac.$$

Remark 2.1.3. For simplicity, the notation $[a, b, c]$ will sometimes be used to denote the binary quadratic form $ax^2 + bxy + cy^2$. We may also write $[a, b, *]$ or $[a, *, *]$ if the second and third coefficients are irrelevant or can be easily computed by the discriminant formula.

Proposition 2.1.4. There exists a binary quadratic form of discriminant Δ if and only if $\Delta \equiv 0$ or $1 \pmod 4$.

Definition 2.1.5. An integer Δ is a **fundamental discriminant** if $\Delta \neq 1$ and Δ satisfies one of the following two conditions :

(a) $\Delta \equiv 1 \pmod 4$ and Δ is square-free.

(b) $\Delta = 4m$ for some square-free integer m and $m \equiv 2$ or $3 \pmod 4$.

Definition 2.1.6. $SL_2(\mathbb{Z})$ is the group

$$\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| \; a, b, c, d \in \mathbb{Z}, \; ad - bc = 1 \right\}.$$

Theorem 2.1.7. $SL_2(\mathbb{Z})$ is generated by the elements

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Definition 2.1.8. An element $M \in SL_2(\mathbb{Z})$ act on a integral binary quadratic form $f(x, y) = ax^2 + bxy + cy^2$ by

$$\big(M \cdot f\big)(x, y) = \begin{pmatrix} x & y \end{pmatrix} M \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} M^T \begin{pmatrix} x \\ y \end{pmatrix}.$$

The discriminant of the binary quadratic form is invariant under the $SL_2(\mathbb{Z})$ action.

Remark 2.1.9. Let $f = [a, b, c]$ be a binary quadratic form. The action of the following 3 matrices are of particular importance :

$$\begin{aligned} (T^k)^T \cdot f &= [a, 2ak + b, ak^2 + bk + c] \\ T^k \cdot f &= [a + bk + ck^2, b + 2ck, c] \\ S \cdot f &= [c, -b, a] \end{aligned}$$

where $k \in \mathbb{Z}$ and S and T are given in Theorem 2.1.7.

Definition 2.1.10. Two binary quadratic forms f and g are said to be **equivalent** (or $SL_2(\mathbb{Z})$-equivalent) if f and g lie in the same orbit under the $SL_2(\mathbb{Z})$-action. This is denoted by $f \sim g$.

For a binary quadratic form f, we use $\overline{f}$ to denote the $SL_2(\mathbb{Z})$-equivalence class containing f.

2.2 Form Class Group

Definition 2.2.1. A binary quadratic form $f = [a, b, c]$ is **primitive** if $\gcd(a, b, c) = 1$.

If $f \sim g$, then f is primitive if and only if g is primitive.

Proposition 2.2.2. If Δ is a fundamental discriminant, then all binary quadratic forms of discriminant Δ is primitive.

Proposition 2.2.3. Let f and g be two primitive binary quadratic forms of discriminant Δ. Then there exists $a, a', B, C \in \mathbb{Z}$ such that

$$f \sim [a, B, Ca'] \;\text{ and }\; g \sim [a', B, Ca].$$

Definition 2.2.4 (Form class group)**.** Let $C^2(\Delta)$ denote the set of $SL_2(\mathbb{Z})$-equivalence classes of primitive binary quadratic forms of discriminant Δ. Let $C_1, C_2 \in C^2(\Delta)$ be two equivalence classes. Then $\exists a, a', B, C \in \mathbb{Z}$ such that

$$[a, B, Ca'] \in C_1 \;\text{ and }\; [a', B, Ca] \in C_2.$$

Let C_3 be the equivalence class containing $[aa', B, C]$.

Define $\bullet : C^2(\Delta) \times C^2(\Delta) \to C^2(\Delta)$ by :

$$C_1 \bullet C_2 = C_3.$$

Then $\bullet$ is a well-defined binary operation and $\big(C^2(\Delta), \bullet\big)$ is a finite abelian group.

Remark 2.2.5. If there is no ambiguity, we will use $C^2(\Delta)$ to denote the group $(C^2(\Delta), \bullet)$.

Example 2.2.6. We consider $C^2(-56)$. Note that -56 is a fundamental discriminant. Let $f = [2, 0, 7]$ and $g = [3, 2, 5]$. To compose $\overline{f}$ and $\overline{g}$, first observe that

$$f \sim [2, 8, 15] \text{ via } (T^2)^T \;\text{ and }\; g \sim [3, 8, 10] \text{ via } T^T.$$

Thus $\overline{f} \bullet \overline{g}$ is the equivalence class containing the form $[6, 8, 5]$.

3 Ideal Class Group

In this chapter, we will study the ideal class group in the general abstract setting of Dedekind domains. All rings in this chapter are assumed to be commutative with unity.

3.1 Noetherian and Integrally Closed Domains

We recall some basic concepts from commutative ring theory.

Definition 3.1.1. Let R be a ring. A R-module M satisfies the **ascending chain condition** on its submodules if given any increasing chain of R-submodules of M :

$$M_1 \subseteq M_2 \subseteq M_3 \subseteq \cdots$$

there exists $n \in \mathbb{Z}_{\geq 1}$ such that $M_n = M_{n+1} = \cdots$.

Definition 3.1.2. Let R be a ring. A R-module M is **Noetherian** if it satisfies any one of the three equivalent conditions :

(a) M satisfies the ascending chain condition.

(b) Every non-empty set of submodules of M contains a maximal element with respect to inclusion.

(c) Every R-submodule of M is finitely generated.

A ring R is **Noetherian** if it is Noetherian when regarded as an R-module via multiplication.

Definition 3.1.3. Let R be a ring and S a subring of R. An element $r \in R$ is **integral over** S if there exists $k \in \mathbb{Z}_{\geq 1}$ and $s_0, s_1, \cdots, s_{k-1} \in S$ such that

$$r^k + s_{k-1} \cdot r^{k-1} + \cdots + s_1 \cdot r + s_0 = 0_R.$$

In other words, r is the root of a monic polynomial with coefficients in S. The set of elements of R that are integral over S is called the **integral closure** of S in R.

Definition 3.1.4. Let R be an integral domain and K be its field of fractions. Then R is an **integrally closed domain** (or R is **integrally closed**) if the integral closure of R in K is R itself.

We note down two elementary propositions about prime ideals which will come in handy in the next section.

Proposition 3.1.5. Let R be a ring. Let $I_1, I_2, \cdots, I_k$ be ideals of R and let P be a prime ideal of R. Then

$$I_1 I_2 \cdots I_k \subseteq P \implies I_i \subseteq \mathfrak{p} \text{ for some } i \in \{1, \cdots, k\}.$$

Proof. Assume otherwise. Then for each $i \in \{1, \cdots, k\}$, there exists $x_i \in I_i$ such that $x_i \notin P$. Since P is prime, $x_1 x_2 \cdots x_k \notin P$. This is a contradiction to $I_1 I_2 \cdots I_k \subseteq P$.

Proposition 3.1.6. Let R be a Noetherian integral domain. Then every non-zero ideal of R contains a product of non-zero prime ideals.

Remark 3.1.7. The empty product of ideals is defined to be R.

Proof. Assume otherwise. Let Φ denote the set of all non-zero ideals of R which does not contain a product of non-zero prime ideals. Then Φ is non-empty. Since R is Noetherian, Φ contains a maximal element M. Clearly M is not prime and $M \neq R$. Thus there exists $x, y \in R \setminus I$ such that $xy \in I$. Letting (x) and (y) denote the principal ideals generated by x and y respectively, we have that the ideals $I + (x)$ and $I + (y)$ contain I properly. But I is maximal in Φ so $I + (x)$ and $I + (y)$ cannot be elements of Φ. There exists prime ideals $P_1, \cdots, P_t, Q_1, \cdots, Q_r$ such that

$$P_1 P_2 \cdots P_t \subseteq I + (x) \text{ and } Q_1 Q_2 \cdots Q_r \subseteq I + (y).$$

Since $xy \in I$,

$$\big[I + (x)\big]\big[I + (y)\big] \subseteq I$$

and so $P_1 \cdots P_t Q_1 \cdots Q_r \subseteq I$, a contradiction.

3.2 Dedekind Domains

Definition 3.2.1. An integral domain R is a **Dedekind domain** if it satisfies all three conditions :

(a) R is Noetherian.

(b) R is integrally closed.

(c) Every non-zero prime ideal of R is maximal.

Definition 3.2.2. Let R be an integral domain and let K be its field of fractions. A **fractional ideal** I of R is a R-submodule of K such that there exists $r \in R \setminus \{0\}$ such that $rI \subseteq R$.

A fractional ideal I is **invertible** if there exists a fractional ideal J of R such that $IJ = R$.

Remark 3.2.3. The element r can be thought of as a common denominator for all the elements in I, hence the name fractional ideal.

It follows directly from the definition that all ordinary ideals of R are also fractional ideals. However, the converse is not true. For clarity, ordinary ideals will sometimes be referred to as **integral ideals**.

Proposition 3.2.4. Let R be a Dedekind domain and let F be a fractional ideal of R. If there exists a non-zero integral ideal I such that $FI = I$, then $F \subseteq R$.

Proof. Let $x \in F$. We aim to prove that $x \in R$. First observe that

$$xI \subseteq I \implies x^2 I = x(xI) \subseteq xI \subseteq I.$$

By induction, we have $x^n I \subseteq I$ for all positive integers n. Since any non-zero element of I serves as a common denominator for the x^n, the set

$$R[x] = \left\{ \sum_{k=0}^{n} r_k x^k \;\middle|\; r_k \in R,\ n \in \mathbb{Z}_{\geq 0} \right\}$$

is a fractional ideal of R. Since R is Noetherian, $R[x]$ is generated by some finite set $\{p_1(x), p_2(x), \cdots, p_k(x)\}$, where each $p_i(x)$ is a polynomial with coefficients in R of degree d_i. Let $m = \max\{d_1, \cdots, d_k\}$. Then there exists $s_1, \cdots, s_k \in R$ such that

$$\begin{aligned} x^{m+1} &= s_1 p_1(x) + \cdots + s_k p_k(x) \\ \implies x^{m+1} &- s_1 p_1(x) - \cdots - s_k p_k(x) = 0_R \end{aligned}$$

so x is integral over R. Since R is integrally closed, we have $x \in R$ as desired.

Theorem 3.2.5. Let R be a Dedekind domain which is not a field. Then every maximal ideal of R is invertible.

Proof. Let M be a maximal ideal of R and let K be its field of fractions. Since R is not a field, M is not the zero ideal. Define

$$M' = \{x \in K \mid xM \ \subseteq R\}.$$

It is easy to check that M' is a R-submodule of K. Since any non-zero element of M is a common denominator for M', we have that M' is a fractional ideal of R. It remains to prove that $M'M = R$. The fact that $M'M \subseteq R$ follows directly from the definition of M'. On the other hand, we have $R \subseteq M'$ and so

$$M = RM \subseteq M'M.$$

By maximality of M, we must have $M'M = M$ or $M'M = R$. It suffices to show that the former case is impossible.

If $M'M = M$, then $M' \subseteq R$ (Proposition 3.2.4) and so $M' = R$. Let $r \in M \setminus \{0_R\}$. Then r is not a unit so $(r) = Rr$ is a proper ideal of R. Thus Rr contains a non-empty product of non-zero prime ideals (Proposition 3.1.6).

Let $P_1P_2\cdots P_n$ be a product such that n is minimised. We have $P_1P_2\cdots P_n \subseteq Rr \subseteq M$. Since M is maximal, it is prime so there exists $i \in \{1, 2, \cdots, n\}$ such that $P_i \subseteq M$ (Proposition 3.1.5). Without loss of generality, we may assume that $i = 1$. Since R is Dedekind, P_1 is maximal and thus $M = P_1$.

Let $J = P_2\cdots P_n$ (If $n = 1$, then $J = R$ is the empty product). By the minimality of n, we get that $J \not\subseteq Rr$ so there exists $x \in J$ such that $x \notin Rr$. Thus $xr^{-1} \notin R$.

On the other hand, $MJ \subseteq Rr$ and so $Mx \subseteq Rr$. Then we have $M(xr^{-1}) \subseteq R$. Thus $xr^{-1} \in M'$ which is a contradiction to $M' = R$.

Corollary 3.2.6. Let R be a Dedekind domain which is not a field. Let M be a maximal ideal of R. Then M has a unique inverse M' and we have $R \subseteq M'$.

Proof. We first prove that the inverse is unique. Let M_1 and M_2 be fractional ideals of R such that $M_1M = M_2M = R$. Then

$$M_1 = M_1R = M_1MM_2 = RM_2 = M_2.$$

In the proof of Theorem 3.2.5, we have $R \subseteq M'$. Since M' is the unique inverse of M, the conclusion follows.

Theorem 3.2.7. Let R be a Dedekind domain and let $\mathfrak{P}$ be the set of non-zero prime ideals of R. Then every non-zero fractional ideal I of R may be uniquely expressed in the form

$$I = \prod_{P \in \mathfrak{P}} P^{n_p} \tag{1}$$

where for all $P \in \mathfrak{P}$, one has $n_p \in \mathbb{Z}$ with $n_p = 0$ for all but finitely many P.

Remark 3.2.8. By Theorem 3.2.5, every non-zero prime ideal P has an inverse P'. For $n \in \mathbb{Z}_{<0}$, we define $P^n = (P')^{-n}$.

Proof. If R is a field, then the only fractional ideals of R are the zero ideal and R itself so this statement is trivially true. Thus we may assume that R is not a field.

We first prove that the existence statement holds for integral ideals. Assume otherwise. Let Φ denote the set of all non-zero integral ideals of R which cannot be expressed as a product of prime ideals. Then Φ is non-empty. Since R is Noetherian, Φ contains a maximal element M. Then $M \neq R$ since R is the empty product of prime ideals. Thus M is contained in a maximal ideal P which has an inverse P^{-1}. Then $M \subseteq P$ and so $MP^{-1} \subseteq R$. On the other hand, $R \subseteq P^{-1}$ (Corollary 3.2.6) and so $M \subseteq MP^{-1}$.

If $MP^{-1} = M$, then $P^{-1} = R$ (Proposition 3.2.4). If that is the case, then

$$R = PP^{-1} = PR = P$$

which is impossible. Thus MP^{-1} is an integral ideal of R containing M properly. We have $MP^{-1} \notin \Phi$ so $MP^{-1} = P_1 P_2 \cdots P_n$ is a product of prime ideals. It follows that $M = P_1 P_2 \cdots P_n P$ is also a product of prime ideals, a contradiction.

Now let F be a fractional ideal of R. Then there exists $r \in R$ such that rF is an integral ideal of R. We have that

$$(r) = S_1 S_2 \cdots S_t \quad \text{and} \quad rF = (r)F = Q_1 Q_2 \cdots Q_k$$

are products of prime ideals. Then $F = S_1^{-1} S_2^{-1} \cdots S_t^{-1} Q_1 Q_2 \cdots Q_k$ which completes the proof.

Next, we will show the uniqueness of (1).

Let $\prod_{P \in \mathfrak{P}} P^{n_p} = \prod_{P \in \mathfrak{P}} P^{m_p}$ be two products of prime ideals. Then $\prod_{P \in \mathfrak{P}} P^{n_p - m_p} = R$.

If $n_{\mathfrak{p}} - m_{\mathfrak{p}} \neq 0$ for some prime ideals $P \in \mathfrak{P}$, then after separating the positive and negative exponents, we may write

$$P_1^{\alpha_1} P_2^{\alpha_2} \cdots P_r^{\alpha_r} = Q_1^{\beta_1} Q_2^{\beta_2} \cdots Q_s^{\beta_s}$$

where $P_i, Q_j \in \mathfrak{P}$ with $P_i \neq Q_j$ and $\alpha_i, \beta_j \in \mathbb{Z}_{\geq 1}$ for all i, j. But this means that $Q_1^{\beta_1} \cdots Q_s^{\beta_s} = P_1^{\alpha_1} \cdots P_r^{\alpha_r} \subseteq P_1$ and so there exists $i \in \{1, 2, \cdots, s\}$ such that $Q_i \subseteq P_1$. (Proposition 3.1.5) This is a contradiction as both P_1 and Q_i are maximal and $P_1 \neq Q_i$.

Corollary 3.2.9. Let R be a Dedekind domain. Then every non-zero fractional ideal of R is invertible.

Proof. Let I be a fractional ideal of R. Write $I = \displaystyle\prod_{P \in \mathfrak{P}} P^{n_p}$ as a product of prime ideals. Then the inverse of I is simply given by

$$I^{-1} = \prod_{P \in \mathfrak{P}} P^{-n_p}.$$

3.3 Ideal Class Group

Theorem 3.3.1. Let R be a Dedekind domain and $F(R)$ be the set of all non-zero fractional ideals of R. Then $F(R)$ is an abelian group under the usual ideal multiplication.

Proof. Associativity and commutativity of the group operation follows from associativity and commutativity of multiplication of ideals in the ring R.

Since any non-zero fractional ideal $I \in F(R)$ is a R-module, we have $IR = I$ so R is the identity element of the group.

Finally, every non-zero fractional ideal $I \in F(R)$ has an inverse by Corollary 3.2.9.

Definition 3.3.2. Let $P(R)$ denote the set of non-zero principal fractional ideals of R (i.e. fractional ideals of R generated by a single non-zero element). It is easy to check that $P(R)$ is a subgroup of $F(R)$. Define the **ideal class group** of R (denoted by $Cl(R)$) to be the quotient group

$$Cl(R) = F(R)/P(R).$$

We will finish off this section by establishing some basic formulas. For a fractional ideal I and a prime ideal P in a Dedekind domain R, we let $n_p(I)$ denote the exponent of P in the factorisation of I as a product of prime ideals.

Proposition 3.3.3. Let I and J be non-zero fractional ideals of a Dedekind domain R. Then for all non-zero prime ideals P of R, we have :

(a) $n_p(IJ) = n_p(I) + n_p(J)$.

(b) $I \subseteq R \implies n_p(I) \geq 0$.

(c) $I \subseteq J \implies n_p(I) \geq n_p(J)$.

Proof. Statement (a) is trivial and statement (c) follows directly from statement (b).

For (b), write $I = \prod_{P \in \mathfrak{P}} P^{n_p(I)}$. Splitting the positive and negative exponents, we have

$$\prod_{P \in \mathfrak{P}} P^{n_p(I)} \subseteq R \implies P_1^{\alpha_1} P_2^{\alpha_2} \cdots P_s^{\alpha_s} \subseteq Q_1^{\beta_1} Q_2^{\beta_2} \cdots Q_r^{\beta_r}$$

where $P_i, Q_j \in \mathfrak{P}$ with $P_i \neq Q_j$ and $\alpha_i, \beta_j \in \mathbb{Z}_{\geq 1}$ for all i, j. If the right hand side is not the empty product, then $P_1^{\alpha_1} P_2^{\alpha_2} \cdots P_s^{\alpha_s} \subseteq Q_1$ so $P_i \subseteq Q_1$ for some $i \in \{1, \cdots, s\}$ by Proposition 3.1.5. This is a contradiction since P_i and Q_1 are distinct maximal ideals.

4 Algebraic Number Theory

In this chapter, we will introduce the basic concepts from algebraic number theory that are needed to make the connection between Dedekind domains and number rings.

4.1 Algebraic Number and Algebraic Integers

Definition 4.1.1. An **algebraic number** is a complex number that is a root of a non-zero polynomial with coefficients in $\mathbb{Q}$.

An algebraic number that is a root of a monic polynomial with coefficients in $\mathbb{Z}$ is known as an **algebraic integer**.

Definition 4.1.2. Let α be an algebraic number. There exist a unique monic polynomial (denoted by m_α) with coefficients in $\mathbb{Q}$ having α as a root. Then m_α is the **minimal polynomial** of α.

The **degree** of α is the degree of its minimal polynomial. The roots of m_α (including α itself) are the **conjugates** of α.

The uniqueness of the minimal polynomial is a direct consequence of the following proposition.

Proposition 4.1.3. Let $p(x) \in \mathbb{Q}[x]$ be a non-zero polynomial having α as a root. Then $m_\alpha(x) \mid p(x)$ in $\mathbb{Q}[x]$.

Proof. By minimality of the degree of $m_\alpha(x)$, we have $\deg(p(x)) \geq \deg(m_\alpha(x))$. Using the Euclidean algorithm for polynomials, there exist polynomials $q(x), r(x) \in \mathbb{Q}[x]$ with $\deg(r(x)) < \deg(m_\alpha(x))$ such that

$$p(x) = m_\alpha(x)q(x) + r(x).$$

Substituting α into the equation, we get $r(\alpha) = 0$. By minimality of the degree of $m_\alpha(x)$, we conclude that $r(x)$ must be the zero polynomial.

Remark 4.1.4. If $m_1(x), m_2(x) \in \mathbb{Q}[x]$ both satisfy the definition of minimal polynomial of an algebraic number α, then $m_1(x)$ divides $m_2(x)$ in $\mathbb{Q}[x]$ and vice versa. Thus $m_1(x)$ and $m_2(x)$ are scalar multiples of each other. Under the additional condition that the leading coefficient is 1, the minimal polynomial of α must be unique.

Proposition 4.1.5. Let α be an algebraic number. Then $m_\alpha(x)$ is irreducible over $\mathbb{Q}$.

Proof. Assume that $m_\alpha(x) = g(x)h(x)$, where $g(x), h(x) \in \mathbb{Q}[x]$ are polynomials of degree strictly lower than $m_\alpha(x)$. Then $g(\alpha)h(\alpha) = 0$ so we have either $g(\alpha) = 0$ or $h(\alpha) = 0$ since $\mathbb{C}$ is also an integral domain. This contradicts the minimality of the degree of $m_\alpha(x)$.

Proposition 4.1.6. Let α be an algebraic number of degree n. Then α has n distinct conjugates, including itself.

Proof. It suffices to prove that $m_\alpha(x)$ has no repeated roots. Assume that $m_\alpha(x)$ has a repeated root, β. First note that since $m_\alpha(x)$ is irreducible over $\mathbb{Q}$, and $m_\beta(x) \mid m_\alpha(x)$ in $\mathbb{Q}[x]$, we must have $m_\beta(x) = m_\alpha(x)$.

Since β is a repeated root of $m_\alpha(x)$, it is a root of $m'_\alpha(x)$. But $\deg(m'_\alpha(x)) < \deg(m_\alpha(x))$ so $m'_\alpha(x)$ must be the zero polynomial. On the other hand, by writing $m_\alpha(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ for some $a_0, \cdots, a_{n-1} \in \mathbb{Q}$, we have

$$m'_\alpha(x) = nx^{n-1} + \cdots + +a_2x + a_1$$

which is clearly not the zero polynomial.

Proposition 4.1.7 (Gauss's lemma)**.** Let $f(x) \in \mathbb{Z}[x]$ and $g(x), h(x) \in \mathbb{Q}[x]$ be three monic polynomials such that $f(x) = g(x)h(x)$. Then $g(x), h(x) \in \mathbb{Z}[x]$.

Proof. Let m, n be the smallest positive integers such that $mg(x)$ and $nh(x)$ have coefficients in $\mathbb{Z}$. Then the greatest common divisor of the coefficients of $mg(x)$ is 1. (Otherwise m can be replaced by the smaller integer m/d, where d is the greatest common divisor of the coefficients of $mg(x)$) The same holds for $nh(x)$. It suffices to show that $m = n = 1$.

Assume that $mn > 1$. Let p be a prime dividing mn. Then $mnf(x) = mg(x) \cdot nh(x)$. We have $\overline{mg(x)} \cdot \overline{nh(x)} = \overline{mnf(x)}$, where the bars indicate the image of the polynomials under the quotient map $\mathbb{Z}[x] \to (\mathbb{Z}/p\mathbb{Z})[x]$. Since p divides mn, $\overline{mg(x)} \cdot \overline{nh(x)} = 0$ in $(\mathbb{Z}/p\mathbb{Z})[x]$ which is an Euclidean domain (Recall that $\mathbb{Z}/p\mathbb{Z}$ is a field). Thus either $\overline{mg(x)} = 0$ or $\overline{nh(x)} = 0$ so p divides the greatest common divisor of the coefficients of either $mg(x)$ or $nh(x)$. This is a contradiction as the greatest common divisor of the coefficients of $mg(x)$ and $nh(x)$ is 1.

Proposition 4.1.8. Let α be an algebraic integer and let $m_\alpha(x)$ be its minimal polynomial. Then $m_\alpha(x) \in \mathbb{Z}[x]$.

Proof. Let $f(x) \in \mathbb{Z}[x]$ be a monic polynomial that contains α as a root. Then by Proposition 4.1.3, there exists $q(x) \in \mathbb{Q}[x]$ such that $f(x) = m_\alpha(x)q(x)$.

Since $f(x)$ and $m_\alpha(x)$ are monic, $q(x)$ is also monic. Then by Proposition 4.1.7, we have $m_\alpha(x) \in \mathbb{Z}[x]$.

Corollary 4.1.9. The only algebraic integers in $\mathbb{Q}$ are the ordinary integers.

Proof. Let $\alpha \in \mathbb{Q}$. Then $m_\alpha(x) = x - \alpha$. This polynomial is in $\mathbb{Z}[x]$ if and only if $\alpha \in \mathbb{Z}$.

4.2 Algebraic Number Fields and Number Rings

Definition 4.2.1. Let F be a field containing a subfield K. Then F is an **extension field** of K.

The larger field F can also be viewed as a K-vector space. The dimension of this vector space (denoted by $[F : K]$) is known as the **degree** of the extension.

Definition 4.2.2. Let R be a ring containing a subfield K. An element $x \in R$ is **algebraic over** K if there exists $n \in \mathbb{Z}_{\geq 1}$ and $a_0, a_1, \cdots, a_n \in K$, not all zero, such that $a_n x^n + \cdots + a_1 x + a_0 = 0$.

Elements which are not algebraic over K are called **transcendental** over K.

Definition 4.2.3. A ring R containing a subfield K is **algebraic** over K if every element of R is algebraic over K. If R is a field, then R is an **algebraic extension** of K.

Proposition 4.2.4. Let F be a field containing a subfield K. If the degree of F over K is finite, then F is an algebraic extension of K.

Proof. Let $u \in F$ and let n denote the degree of F over K. Then $\{1, u, \cdots, u^n\}$ is a linearly dependent set over K. Thus there exists $a_0, \cdots, a_n \in K$, not all zero, such that

$$a_n u^n + a_{n-1} u^{n-1} + \cdots + a_1 u + a_0 = 0$$

as desired.

Definition 4.2.5. An **algebraic number field** is an extension field of finite degree over $\mathbb{Q}$.

We will now state, but not prove, the following theorem from Galois Theory.

Theorem 4.2.6 (Primitive element theorem)**.** Let K be an algebraic number field of degree n. Then there exists an algebraic number α (of degree n) such that the set

$$\left\{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}\right\}$$

is a $\mathbb{Q}$-basis for K. We may also denote K by $\mathbb{Q}[\alpha]$.

Theorem 4.2.7. Let $\alpha \in \mathbb{C}$. Then the following are equivalent.

(a) α is an algebraic integer.

(b) The additive group of the ring $\mathbb{Z}[\alpha]$ is finitely generated.

(c) There exists a finitely generated non-trivial additive subgroup A of $\mathbb{C}$ such that $\alpha A \subseteq A$.

Proof. $(a) \implies (b)$: Let $f(x) \in \mathbb{Z}[x]$ be a monic polynomial which contains α as a root and let $n = \deg(f(x))$. Then $\mathbb{Z}[\alpha]$ is generated by $\{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}\}$.

$(b) \implies (c)$: Choose $A = \mathbb{Z}[\alpha]$.

$(c) \implies (a)$: Let $a_1, a_2, \cdots, a_n$ be the generators of A.

For each a_i, observe that αa_i can be expressed in the form

$$\alpha a_i = c_{i,1}a_1 + c_{i,2}a_2 + \cdots + c_{i,n}a_n$$

where $c_{i,j} \in \mathbb{Z}$ for all i, j. Thus we obtain n equations which can be expressed as a matrix equation :

$$\begin{pmatrix} \alpha a_1 \\ \alpha a_2 \\ \vdots \\ \alpha a_n \end{pmatrix} = \begin{pmatrix} c_{1,1} & c_{1,2} & \cdots & c_{1,n} \\ c_{2,1} & c_{2,2} & \cdots & c_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ c_{n,1} & c_{n,2} & \cdots & c_{n,n} \end{pmatrix} \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}. \tag{2}$$

Let M denote the $n \times n$ matrix in (2). Since $a_1, a_2, \cdots, a_n$ are not all zero, α is an eigenvalue of M. Thus α is the root of the characteristic polynomial $c_M(x)$ of M, which is monic. Finally, since M has entries in $\mathbb{Z}$, we conclude that $c_M(x)$ has coefficients in $\mathbb{Z}$.

Corollary 4.2.8. The set of all algebraic integers in $\mathbb{C}$ (denoted by $\mathbb{A}$) is a subring of $\mathbb{C}$.

Proof. Let $\alpha, \beta \in \mathbb{A}$. We will prove that $\mathbb{A}$ contains $\alpha - \beta$ and $\alpha\beta$. Let $\{a_1, a_2, \cdots, a_n\}$ and $\{b_1, b_2, \cdots, b_m\}$ generate $\mathbb{Z}[\alpha]$ and $\mathbb{Z}[\beta]$ respectively. Then the ring $\mathbb{Z}[\alpha, \beta]$ has a generating set $\left\{ a_ib_j \mid 1 \leq i \leq n, 1 \leq j \leq m \right\}$. Since $\mathbb{Z}[\alpha, \beta]$ contains $\alpha - \beta$ and $\alpha\beta$, we have that $(\alpha - \beta)\mathbb{Z}[\alpha, \beta]$ and $\alpha\beta\mathbb{Z}[\alpha, \beta]$ are both subsets of $\mathbb{Z}[\alpha, \beta]$. Hence $\alpha - \beta$ and $\alpha\beta$ are indeed algebraic integers.

Definition 4.2.9. Let K be an algebraic number field. Then $\mathbb{A} \cap K$ is the **number ring** corresponding to the number field K.

4.3 Trace and Norm

Definition 4.3.1. An **embedding** of a field K into a field F is a ring homomorphism $\sigma : K \to F$.

Proposition 4.3.2. Let K and F be fields and $\sigma : K \to F$ be an embedding. Then σ is injective.

Proof. The kernel of σ is an ideal of K and since K is a field, we have $\ker(\sigma) = K$ or $\ker(\sigma) = \{0\}$. The former case cannot happen since F is a field and so cannot be the zero ring.

We will now state, but do not prove, another theorem from Galois Theory which will be needed in defining the trace and norm.

Theorem 4.3.3. Let $K = \mathbb{Q}[\alpha]$ be a number field of degree n over $\mathbb{Q}$. Each conjugate β of α determines a unique embedding $g_\beta : K \to \mathbb{C}$ via

$$g\left(\sum_{k=0}^{n-1} c_k \cdot \alpha^k\right) = \sum_{k=0}^{n-1} c_k \cdot \beta^k \text{ with } c_0, c_1, \cdots, c_{n-1} \in \mathbb{Q}.$$

Furthermore, every embedding must be of this form. Since α has n conjugates, there are exactly n embeddings from K into $\mathbb{C}$.

More generally, let L and K be two number fields of degree d_K and d_L over $\mathbb{Q}$ and assume that $K \subseteq L$. Then $[L : K] = d_L/d_k$ and every embedding of K into $\mathbb{C}$ extends to exactly $[L : K]$ embeddings of L into $\mathbb{C}$.

Definition 4.3.4 (Trace and Norm)**.** Let K be a number field of degree n over $\mathbb{Q}$ and let $\sigma_1, \sigma_2, \cdots, \sigma_n$ be the embeddings of K in $\mathbb{C}$. Define the functions $T^K : K \to \mathbb{C}$ and $N^K : K \to \mathbb{C}$ by

$$\begin{aligned} T^K(\alpha) &= \sigma_1(\alpha) + \sigma_2(\alpha) + \cdots + \sigma_n(\alpha) \\ N^K(\alpha) &= \sigma_1(\alpha)\sigma_2(\alpha) \cdots \sigma_n(\alpha). \end{aligned}$$

Remark 4.3.5. The trace and norm of an algebraic number α depends on the underlying number field K. If there is no ambiguity, then $T(\alpha)$ and $N(\alpha)$ may be used to denote the trace and norm instead.

Proposition 4.3.6. T^K is a $\mathbb{Q}$-linear map.

Proof. Recall that every embedding from K to $\mathbb{C}$ fixes $\mathbb{Q}$. Let $\alpha, \beta \in K$ and $q, s \in \mathbb{Q}$.

$$\begin{aligned} T^K(q\alpha + s\beta) &= \sigma_1(q\alpha + s\beta) + \cdots + \sigma_n(q\alpha + s\beta) \\ &= \sigma_1(q)\sigma_1(\alpha) + \cdots + \sigma_n(q)\sigma_n(\alpha) + \sigma_1(s)\sigma_1(\beta) + \cdots + \sigma_n(s)\sigma_n(\beta) \\ &= q\sigma_1(\alpha) + \cdots + q\sigma_n(\alpha) + s\sigma_1(\beta) + \cdots + s\sigma_n(\beta) \\ &= qT^K(\alpha) + sT^K(\beta). \end{aligned}$$

Theorem 4.3.7. Let K be a number field of degree m over $\mathbb{Q}$. Let $\alpha \in K$ be an algebraic number and let d denote its degree. Then

$$\begin{aligned} T^K(\alpha) &= \frac{m}{d} t(\alpha) \\ N^K(\alpha) &= \big[n(\alpha)\big]^{m/d} \end{aligned}$$

where $t(\alpha)$ and $n(\alpha)$ denote the sum and product of the d conjugates of α over $\mathbb{Q}$ respectively.

Proof. Clearly $\mathbb{Q}[\alpha] \subseteq K$. Let the embeddings of $\mathbb{Q}[\alpha]$ into $\mathbb{C}$ be $\sigma_1, \sigma_2, \cdots, \sigma_d$. For each i, we know that σ_i extends to m/d embeddings of K (Theorem 4.3.3), denoted by $\sigma_{i,1}, \cdots, \sigma_{i,m/d}$ respectively. Then

$$\begin{aligned} T^K(\alpha) &= \sigma_{1,1}(\alpha) + \cdots + \sigma_{1,m/d}(\alpha) + \sigma_{2,1}(\alpha) + \cdots + \sigma_{d,m/d}(\alpha) \\ &= \frac{m}{d}\sigma_1(\alpha) + \frac{m}{d}\sigma_2(\alpha) + \cdots + \frac{m}{d}\sigma_d(\alpha) \\ &= \frac{m}{d} t(\alpha). \end{aligned}$$

Similarly,

$$\begin{aligned} N^K(\alpha) &= \sigma_{1,1}(\alpha) \cdots \sigma_{1,m/d}\sigma_{2,1}(\alpha) \cdots \sigma_{d,m/d}(\alpha) \\ &= \big[\sigma_1(\alpha)\big]^{m/d}\big[\sigma_2(\alpha)\big]^{m/d} \cdots \big[\sigma_d(\alpha)\big]^{m/d} \\ &= \big[n(\alpha)\big]^{m/d}. \end{aligned}$$

Corollary 4.3.8. $T^K(\alpha)$ and $N^K(\alpha)$ are rational.

Proof. We can write $m_\alpha(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_d)$ where $\alpha_1, \cdots, \alpha_d$ are the conjugates of α. Then $-t(\alpha)$ is the coefficient of the x^{d-1} term and $(-1)^d \cdot n(\alpha)$ is the coefficient of the constant term. Thus $t(\alpha)$ and $n(\alpha)$ are rational since $m_\alpha(x) \in \mathbb{Q}[x]$. It then follows by Theorem 4.3.7 that $T^K(\alpha)$ and $N^K(\alpha)$ are also rational.

Corollary 4.3.9. If α is an algebraic integer, then $T^K(\alpha)$ and $N^K(\alpha)$ are integers.

Proof. If α is an algebraic integer then $m_\alpha(x) \in \mathbb{Z}[x]$ by Proposition 4.1.8. Using the same argument as above, $t(\alpha)$ and $n(\alpha)$ are integers and thus $T^K(\alpha)$ and $N^K(\alpha)$ are also integers.

Definition 4.3.10 (Discriminant)**.** Let K be a number field of degree n over $\mathbb{Q}$ and let $\alpha_1, \alpha_2, \cdots, \alpha_n \in K$. Define the **discriminant** of $\alpha_1, \alpha_2, \cdots, \alpha_n$ to be

$$\operatorname{disc}(\alpha_1, \alpha_2, \cdots, \alpha_n) = \det\left(\begin{pmatrix} T^K(\alpha_1\alpha_1) & T^K(\alpha_1\alpha_2) & \cdots & T^K(\alpha_1\alpha_n) \\ T^K(\alpha_2\alpha_1) & T^K(\alpha_2\alpha_2) & \cdots & T^K(\alpha_2\alpha_n) \\ \vdots & \vdots & \ddots & \vdots \\ T^K(\alpha_n\alpha_1) & T^K(\alpha_n\alpha_2) & \cdots & T^K(\alpha_n\alpha_n) \end{pmatrix}\right).$$

By Corollary 4.3.8 and 4.3.9, it is clear that $\operatorname{disc}(\alpha_1, \cdots, \alpha_n) \in \mathbb{Q}$. When $\alpha_1, \cdots, \alpha_n$ are all algebraic integers, then $\operatorname{disc}(\alpha_1, \cdots, \alpha_n) \in \mathbb{Z}$.

Theorem 4.3.11. Let K be a number field of degree n over $\mathbb{Q}$ and let $\alpha_1, \cdots, \alpha_n \in K$ be linearly independent over $\mathbb{Q}$. Then $\operatorname{disc}(\alpha_1, \cdots, \alpha_n) \neq 0$.

Proof. Assume otherwise. Let R_i denote the rows of the matrix $\left[T^K(\alpha_i\alpha_j)\right]$. Then there exists $a_1, \cdots, a_n \in \mathbb{Q}$, not all zero, such that $a_1R_1 + \cdots + a_nR_n = 0$. Let $\alpha = a_1\alpha_1 + \cdots + a_n\alpha_n$. Since $\alpha_1, \cdots, \alpha_n$ are linearly independent over $\mathbb{Q}$ we have $\alpha \neq 0$.

We first show that the set $\{\alpha\alpha_1, \cdots, \alpha\alpha_n\}$ is a $\mathbb{Q}$-basis for K. It suffices to show that the set is linearly independent. Let $b_1, \cdots, b_n \in \mathbb{Q}$ be such that

$$b_1\alpha\alpha_1 + \cdots + b_n\alpha\alpha_n = 0.$$

By dividing by α on both sides,

$$b_1\alpha_1 + \cdots + b_n\alpha_n = 0$$

so $b_1 = \cdots = b_n = 0$ since $\{\alpha_1, \cdots, \alpha_n\}$ is linearly independent over $\mathbb{Q}$.

Now for $j \in \{1, \cdots, n\}$, we consider the j-th row of the equation $a_1R_1 + \cdots + a_nR_n = 0$. T^K is $\mathbb{Q}$-linear by Proposition 4.3.6 so we have

$$\begin{aligned} & a_1T^K(\alpha_j\alpha_1) + a_2T^K(\alpha_j\alpha_2) + \cdots + a_nT^K(\alpha_j\alpha_n) = 0 \\ \implies & T^K(a_1\alpha_1\alpha_j) + T^K(a_2\alpha_2\alpha_j) + \cdots + T^K(a_n\alpha_n\alpha_j) = 0 \\ \implies & T^K(\alpha\alpha_j) = 0. \end{aligned}$$

As the set $\{\alpha\alpha_1, \cdots, \alpha\alpha_n\}$ spans K over $\mathbb{Q}$, we have that $T(\beta) = 0$ for all $\beta \in K$. This is a contradiction as $T(1) = n$.

4.4 Additive Structure of the Number Ring

In this section, let K be a number field of degree n over $\mathbb{Q}$ and let $R = \mathbb{A} \cap K$ be the corresponding number ring. We shall provide a concrete description of the additive structure of R.

Theorem 4.4.1. $R \cong \mathbb{Z}^n$ as $\mathbb{Z}$-modules.

Proof. Firstly recall from commutative ring theory that when R is a principal ideal domain (PID), any submodule of a free R-module of rank n must also be a free R-module of rank at most n. Thus if we have the following chain of $\mathbb{Z}$-modules :

$$A \subseteq B \subseteq C$$

where A and C are both free $\mathbb{Z}$-modules of rank n, then B must also necessarily be a $\mathbb{Z}$-module of rank n.

Thus we will prove this theorem by constructing the $\mathbb{Z}$-modules A and C explicitly. We first need a simple lemma.

Lemma 4.4.2. For all $\alpha \in K$, there exists $n \in \mathbb{Z} \setminus \{0\}$ such that $n\alpha \in \mathbb{A}$.

Proof. Let $d \in \mathbb{Z}$ be a common denominator for the coefficients of $m_\alpha(x)$. We have

$$m_\alpha(x) = x^n + \frac{c_{n-1}}{d}x^{n-1} + \cdots + \frac{c_1}{d}x + \frac{c_0}{d} \quad \text{with } c_0, \cdots, c_{n-1} \in \mathbb{Z}.$$

Multiplying by d^n and substituting α into the polynomial gives

$$\begin{aligned} & d^n\alpha^n + d^{n-1}c_{n-1}\alpha^{n-1} + d^{n-1}c_{n-2}\alpha^{n-2} \cdots + d^{n-1}c_1\alpha + d^{n-1}c_0 = 0 \\ \implies & (d\alpha)^n + c_{n-1}(d\alpha)^{n-1} + dc_{n-2}(d\alpha)^{n-2} + \cdots + d^{n-2}c_1(d\alpha) + d^{n-1}c_0 = 0. \end{aligned}$$

Thus $d\alpha$ is an algebraic integer since it is the root of the monic polynomial :

$$g(x) = x^n + c_{n-1} + dc_{n-2} + \cdots + d^{n-2}c_1x + d^{n-1}c_0$$

and the proof of our lemma is complete.

By the preceding lemma, any $\mathbb{Q}$-basis of K can be transformed into a $\mathbb{Q}$-basis of K consisting entirely of algebraic integers by multiplying each element by a suitable integer. Let $\{\alpha_1, \cdots, \alpha_n\}$ be a $\mathbb{Q}$-basis consisting entirely of algebraic integers. We define

$$A = \big\{b_1\alpha_1 + b_2\alpha_2 + \cdots + b_n\alpha_n \mid b_1, b_2, \cdots, b_n \in \mathbb{Z}\big\}.$$

Then $A \subseteq \mathbb{A} \cap K = R$ and it is clear from the definition that A is a free $\mathbb{Z}$-module of rank n.

To define the other $\mathbb{Z}$-module C, we need another lemma.

Lemma 4.4.3. Let $d = \operatorname{disc}(\alpha_1, \cdots, \alpha_n)$. Then for all $\beta \in R$, there exist integers $m_1, \cdots, m_n$ such that

$$\beta = \frac{m_1\alpha_1 + \cdots + m_n\alpha_n}{d}.$$

Remark 4.4.4. Since $\{\alpha_1, \alpha_2, \cdots, \alpha_n\}$ are linearly independent over $\mathbb{Q}$, $d \neq 0$ by Theorem 4.3.11.

Proof. Write $\beta = x_1\alpha_1 + \cdots + x_n\alpha_n$ with $x_1, \cdots, x_n \in \mathbb{Q}$. Let $\sigma_1, \cdots, \sigma_n$ be the embeddings of K in $\mathbb{C}$. Since each σ_j is $\mathbb{Q}$-linear, we get the matrix equation

$$\begin{pmatrix} \sigma_1(\beta) \\ \sigma_2(\beta) \\ \vdots \\ \sigma_n(\beta) \end{pmatrix} = \begin{pmatrix} \sigma_1(\alpha_1) & \sigma_1(\alpha_2) & \cdots & \sigma_1(\alpha_n) \\ \sigma_2(\alpha_1) & \sigma_2(\alpha_2) & \cdots & \sigma_2(\alpha_n) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n(\alpha_1) & \sigma_n(\alpha_2) & \cdots & \sigma_n(\alpha_n) \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}.$$

Let M denote the $n \times n$ matrix in the above equation. The i, j entry of $M^T M$ is given by

$$\sum_{k=1}^{n} \sigma_k(\alpha_i)\sigma_k(\alpha_j) = \sum_{k=1}^{n} \sigma_k(\alpha_i\alpha_j) = T^K(\alpha_i\alpha_j).$$

Thus

$$\det(M)^2 = \det(M^T M) = \operatorname{disc}(\alpha_1, \cdots, \alpha_n) = d.$$

For each $t \in \{1, \cdots, n\}$, let M_t be the matrix obtained from M by replacing the t-th column of M with $\begin{pmatrix} \sigma_1(\beta) & \sigma_2(\beta) & \cdots & \sigma_n(\beta) \end{pmatrix}^T$. By Cramer's rule,

$$x_t = \frac{\det(M_t)}{\det(M)} \implies dx_t = \det(M)\det(M_t).$$

Since every entry of M and M_t is an algebraic integer, $\det(M)$ and $\det(M_t)$ are also algebraic integers. Thus dx_t is a rational algebraic integer so $dx_t \in \mathbb{Z}$. Choose $m_t = dx_t$ and we are done.

Now define

$$C = \left\{ \frac{c_1}{d}\alpha_1 + \frac{c_2}{d}\alpha_2 + \cdots + \frac{c_n}{d}\alpha_n \;\middle|\; c_1, c_2, \cdots, c_n \in \mathbb{Z} \right\}$$

which is clearly isomorphic as $\mathbb{Z}$-modules to $\mathbb{Z}^n$. By the preceding lemma, $R \subseteq C$ and the proof of the theorem is complete.

Corollary 4.4.5. Let I be a non-zero ideal of R. Then $I \cong \mathbb{Z}^n$ as $\mathbb{Z}$-modules.

Proof. Let $\{\alpha_1, \cdots, \alpha_n\}$ be a $\mathbb{Z}$-basis for R. Let $\alpha \in I \setminus \{0\}$ and let $m = N^K(\alpha)$. Then m is a non-zero integer by Corollary 4.3.9. On the other hand, $m = \alpha\beta$ where β is the product of the other conjugates of α. Clearly β is an algebraic integer, and since $\beta = m/\alpha$, we have $\beta \in K$. Thus $\beta \in R$ and since I is an ideal, $m = \alpha\beta \in I$. Define M to be the $\mathbb{Z}$-submodule of I that is generated by $\{m\alpha_1, \cdots, m\alpha_n\}$. Clearly $M \cong \mathbb{Z}^n$ as submodules since $\{m\alpha_1, \cdots, m\alpha_n\}$ is still linearly independent over $\mathbb{Z}$. Observe that

$$M \subseteq I \subseteq R$$

so we have $I \cong \mathbb{Z}^n$ as $\mathbb{Z}$-modules.

4.5 Alternative Formulation of Trace and Norm

Now that we have established the additive structure of a number ring, we give here an alternative formulation of Trace and Norm.

For this particular section, we will adopt a more general setting. Let A be a commutative ring with unity and let S be a subring of A with unity such that $A \cong S^m$ for some $m \in \mathbb{Z}_{\geq 1}$.

Definition 4.5.1. For each $\alpha \in A$, we can define the S-linear multiplication map $\varphi_\alpha : A \to A$ by

$$\varphi_\alpha(w) = \alpha w.$$

By fixing a S-basis $\{x_1, \cdots, x_m\}$, we can represent φ_α by a matrix Φ_α. Define $T^A(\alpha)$ and $N^A(\alpha)$ by

$$T^A(\alpha) = \mathrm{Tr}(\Phi_\alpha) \quad \text{and} \quad N^A(\alpha) = \det(\Phi_\alpha).$$

Remark 4.5.2. Since the trace and determinant of a S-linear map in invariant under a change of basis, the above definition is independent of the choice of S-basis of A.

Theorem 4.5.3. When $S = \mathbb{Q}$ and $A = \mathbb{Q}[\beta]$ for some algebraic number β, Definition 4.5.1 and Definition 4.3.4 are equivalent.

Proof. We first prove that the statement holds for β. Assume without loss of generality that $\{1, \beta, \cdots, \beta^{m-1}\}$ is our basis. Then

$$\Phi_\beta = \begin{pmatrix} 0 & 0 & 0 & \cdots & -a_0 \\ 1 & 0 & 0 & \cdots & -a_1 \\ 0 & 1 & 0 & \cdots & -a_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & -a_{m-1} \end{pmatrix}$$

where $m_\beta(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_0$. Then we have $\mathrm{Tr}(\Phi_\beta) = -a_{m-1}$ and that $\det(\Phi_\alpha) = (-1)^m a_0$. This agrees with the earlier definition by Corollary 4.3.8.

We now prove the general case. Let $\alpha \in A$ be an algebraic number of degree k. Since $\mathbb{Q}[\beta]$ contains $\mathbb{Q}[\alpha]$ as a subfield, let $\{x_1, \cdots, x_{m/k}\}$ be a basis for $\mathbb{Q}[\beta]$ as a $\mathbb{Q}[\alpha]$-vector space. Then the set

$$\left\{x_1, \alpha x_1, \cdots, \alpha^{k-1}x_1, x_2, \alpha x_2, \cdots, \alpha^{k-2}x_2, \cdots \alpha^{k-1}x_{m/k}\right\}$$

is a $\mathbb{Q}$-basis for $\mathbb{Q}[\beta]$.

Under this basis, we have the matrix representation :

$$\Phi_\alpha = \begin{pmatrix} B_1 & 0 & \cdots & 0 \\ 0 & B_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & B_{m/k} \end{pmatrix}, \text{ where } B_i = \begin{pmatrix} 0 & 0 & \cdots & -y_0 \\ 1 & 0 & \cdots & -y_1 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & -y_{k-1} \end{pmatrix} \quad \text{for each } i$$

and $m_\alpha(x) = x^k + y_{k-1}x^{k-1} + \cdots + y_0$. Then

$$\begin{aligned} \mathrm{Tr}(\Phi_\alpha) &= \mathrm{Tr}(B_1) + \cdots + \mathrm{Tr}(B_{m/k}) \\ &= \frac{m}{k} t(\alpha). \end{aligned}$$

Similarly,

$$\begin{aligned} \det(\Phi_\alpha) &= \det(B_1) \cdots \det(B_{m/k}) \\ &= \big[n(\alpha)\big]^{m/k} \end{aligned}$$

which agrees with Theorem 4.3.7.

Now we change our setting. Let $R = \mathbb{A} \cap \mathbb{Q}[\beta]$ be the number ring corresponding to the number field $\mathbb{Q}[\beta]$. From the preceding section, we know that $R \cong \mathbb{Z}^m$ as $\mathbb{Z}$-modules. Thus we may define T^R and N^R without invoking the underlying number field $\mathbb{Q}[\beta]$. The next theorem shows their equivalence.

Theorem 4.5.4. For all $\alpha \in R$, we have $T^R(\alpha) = T^{\mathbb{Q}[\beta]}(\alpha)$ and $N^R(\alpha) = N^{\mathbb{Q}[\beta]}(\alpha)$.

Proof. We first need a lemma.

Lemma 4.5.5. Let $X = \{x_1, x_2, \cdots, x_t\}$ be a set of vectors in a $\mathbb{Q}$-vector space that is linearly independent over $\mathbb{Z}$. Then X is linearly independent over $\mathbb{Q}$.

Proof. Let $a_1, \cdots, a_t \in \mathbb{Q}$ be such that $a_1x_1 + a_2x_2 + \cdots + a_tx_t = 0$. Let $d \in \mathbb{Z} \setminus \{0\}$ be a common denominator for $a_1, \cdots, a_t$. We have

$$(da_1)x_1 + (da_2)x_2 + \cdots + (da_t)x_t = 0$$

for $da_1, \cdots, da_t \in \mathbb{Z}$ so $da_1 = \cdots = da_t = 0$ since X is a linearly independent set over $\mathbb{Z}$. Thus $a_1 = \cdots = a_t = 0$.

Proof. (of Theorem 4.5.4) Let $\{y_1, y_2, \cdots, y_m\}$ be a $\mathbb{Z}$-basis for R. Then $\{y_1, y_2, \cdots, y_m\}$ is also a $\mathbb{Q}$-basis for $\mathbb{Q}[\beta]$. Under this common basis, the $\mathbb{Z}$-linear multiplication map $\varphi_\alpha : R \to R$ and the $\mathbb{Q}$-linear multiplication map $\psi_\alpha : \mathbb{Q}[\beta] \to \mathbb{Q}[\beta]$ have the same matrix representation so the trace and determinant of the two maps must be equal.

This alternative definition also allows us to discuss the notion of discriminant in a more general setting than just number rings.

Definition 4.5.6. If $S = \mathbb{Z}$ and $A \cong \mathbb{Z}^m$ as $\mathbb{Z}$-modules, then define the **discriminant** of A by

$$\operatorname{disc}(A) = \det\left(\begin{pmatrix} T^A(\alpha_1\alpha_1) & T^A(\alpha_1\alpha_2) & \cdots & T^A(\alpha_1\alpha_m) \\ T^A(\alpha_2\alpha_1) & T^A(\alpha_2\alpha_2) & \cdots & T^A(\alpha_2\alpha_m) \\ \vdots & \vdots & \ddots & \vdots \\ T^A(\alpha_m\alpha_1) & T^A(\alpha_m\alpha_2) & \cdots & T^A(\alpha_m\alpha_m) \end{pmatrix}\right)$$

where $\{\alpha_1, \cdots, \alpha_m\}$ is a $\mathbb{Z}$-basis for A.

Proposition 4.5.7. The definition given above is independent of the choice of $\mathbb{Z}$-basis for A.

Proof. Let $\{\alpha_1, \cdots, \alpha_m\}$ and $\{\beta_1, \cdots, \beta_m\}$ be two bases for A. Then $\exists M \in GL_m(\mathbb{Z})$ such that

$$\begin{pmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_m \end{pmatrix} = M \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_m \end{pmatrix} \implies \begin{pmatrix} T^A(\beta_1) \\ T^A(\beta_2) \\ \vdots \\ T^A(\beta_m) \end{pmatrix} = M \begin{pmatrix} T^A(\alpha_1) \\ T^A(\alpha_2) \\ \vdots \\ T^A(\alpha_m) \end{pmatrix}$$

since T^A is $\mathbb{Z}$-linear. Using the fact that $\det(M) = \pm 1$, a direct computation reveals that

$$\begin{aligned} &\det\left(\begin{pmatrix} T^A(\alpha_1\alpha_1) & T^A(\alpha_1\alpha_2) & \cdots & T^A(\alpha_1\alpha_m) \\ T^A(\alpha_2\alpha_1) & T^A(\alpha_2\alpha_2) & \cdots & T^A(\alpha_2\alpha_m) \\ \vdots & \vdots & \ddots & \vdots \\ T^A(\alpha_m\alpha_1) & T^A(\alpha_m\alpha_2) & \cdots & T^A(\alpha_m\alpha_m) \end{pmatrix}\right) \\ &= \det\left(M \begin{pmatrix} T^A(\alpha_1\alpha_1) & T^A(\alpha_1\alpha_2) & \cdots & T^A(\alpha_1\alpha_m) \\ T^A(\alpha_2\alpha_1) & T^A(\alpha_2\alpha_2) & \cdots & T^A(\alpha_2\alpha_m) \\ \vdots & \vdots & \ddots & \vdots \\ T^A(\alpha_m\alpha_1) & T^A(\alpha_m\alpha_2) & \cdots & T^A(\alpha_m\alpha_m) \end{pmatrix} M^T \right) \\ &= \det\begin{pmatrix} T^A(\beta_1\beta_1) & T^A(\beta_1\beta_2) & \cdots & T^A(\beta_1\beta_m) \\ T^A(\beta_2\beta_1) & T^A(\beta_2\beta_2) & \cdots & T^A(\beta_2\beta_m) \\ \vdots & \ddots & \vdots \\ T^A(\beta_m\beta_1) & T^A(\beta_m\beta_2) & \cdots & T^A(\beta_m\beta_m) \end{pmatrix}. \end{aligned}$$

4.6 Relation between Number Rings and Dedekind Domains

We are now ready to prove the main result in this chapter.

Theorem 4.6.1. Every number ring is a Dedekind domain.

Proof. Let R be a number ring corresponding to a number field K of degree n over $\mathbb{Q}$. We will prove that R satisfies the 3 conditions of Definition 3.2.1.

Let I be an ideal of R. To prove that R is noetherian, it suffices to prove that I is finitely generated over R. By Corollary 4.4.5, $I \cong \mathbb{Z}^n$ as $\mathbb{Z}$-modules. Let $X = \{x_1, \cdots, x_n\}$ be a generating set for I over $\mathbb{Z}$. Then X is clearly also a generating set for I over R.

Let P be a non-zero prime ideal of R. In the next chapter, we will prove that R/P is finite in the more general setting of lattices (Corollary 5.2.6 and Remark 5.2.7). Since P is prime, R/P is also an integral domain. Thus R/P is a field so P is maximal in R.

Finally, we will prove that R is an integrally closed domain. Let $a_0, \cdots, a_{n-1} \in R$ be algebraic integers of degree $d_0, d_1, \cdots, d_{n-1}$ and $\alpha \in K$ be such that

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0 = 0.$$

To show that $\alpha \in \mathbb{A}$, it suffices to prove that the ring $M = \mathbb{Z}[a_0, \cdots, a_{n-1}, \alpha]$ is finitely generated over $\mathbb{Z}$ by Theorem 4.2.7. Observe that

$$\left\{a_0^{m_0} a_1^{m_1} \cdots a_{n-1}^{m_{n-1}} \alpha^m \mid m_0, \cdots, m_{n-1}, m \in \mathbb{Z}_{\geq 0}\right\}$$

is a generating set for M over $\mathbb{Z}$. For each i, we have that $a_i^{d_i}$ and higher powers can be written as a $\mathbb{Z}$-linear combination of lower powers of a_i. Similarly, α^n and higher powers can be written as a sum of products of $a_0, \cdots a_{n-1}$ and lower powers of α. Thus the finite set

$$\left\{a_0^{m_0} a_1^{m_1} \cdots a_{n-1}^{m_{n-1}} \alpha^m \mid 0 \leq m_i < d_i,\ 0 \leq m < n\right\}$$

generates M over $\mathbb{Z}$.

4.7 Quadratic fields

We will end off this chapter by looking at a particular class of number rings.

Definition 4.7.1. A **quadratic number field** is an algebraic number field of degree two over $\mathbb{Q}$.

Proposition 4.7.2. Every quadratic field is of the form $\mathbb{Q}[\sqrt{d}]$, where d is a square-free integer excluding 1 and 0.

Proof. Let $K = \mathbb{Q}[\alpha]$ be a quadratic number field. Then α has degree two so we write $\alpha^2 = b\alpha + c$ for some $b, c \in \mathbb{Q}$. Solving, we get $\alpha = (b \pm \sqrt{b^2 + 4c})/2$. Note that $b^2 + 4c$ cannot be a perfect square since α has degree 2.

Thus $K = \mathbb{Q}[\sqrt{b^2 + 4c}]$. Write $b^2 + 4c = n/m$ for some $n, m \in \mathbb{Z}$ and further let $nm = v^2 d$ where v is the largest integer such that $v^2 \mid nm$ in $\mathbb{Z}$. Then d is square free and we cannot have $d = 0$ or $d = 1$ since $b^2 + 4c$ is not a perfect square. Observe that

$$K = \mathbb{Q}[\sqrt{b^2 + 4c}] = \mathbb{Q}[\sqrt{n/m}] = \mathbb{Q}[\sqrt{nm}] = \mathbb{Q}[v\sqrt{d}] = \mathbb{Q}[\sqrt{d}]$$

as desired.

Proposition 4.7.3. Let $\mathbb{Q}[\sqrt{d_1}]$ and $\mathbb{Q}[\sqrt{d_2}]$ be two quadratic fields, where d_1 and d_2 are square-free integers with $d_1, d_2 \notin \{0, 1\}$. Then $\mathbb{Q}[\sqrt{d_1}] = \mathbb{Q}[\sqrt{d_2}]$ if and only if $d_1 = d_2$.

Proof. We will only prove that $\mathbb{Q}[\sqrt{d_1}] = \mathbb{Q}[\sqrt{d_2}] \implies d_1 = d_2$. The other direction is obvious.

Since $\{1, \sqrt{d_1}\}$ is a $\mathbb{Q}$-basis for $\mathbb{Q}[\sqrt{d_1}]$, there exists $a, b \in \mathbb{Q}$ such that $a + b\sqrt{d_1} = \sqrt{d_2}$. By squaring both sides, we have $a^2 + b^2 d_1 + 2ab\sqrt{d_1} = d_2$. Thus $ab = 0$ by linear independence of $\{1, \sqrt{d_1}\}$.

If $b = 0$, then $a = \sqrt{d_2}$ which contradicts the $\mathbb{Q}$-linear independence of $\{1, \sqrt{d_2}\}$. Thus $a = 0$ so we have $b\sqrt{d_1} = \sqrt{d_2}$. This means that $b^2 d_1 = d_2$ and since d_2 is square-free, we must have $b = 1$ so $d_1 = d_2$.

Remark 4.7.4. From Proposition 4.7.2 and Proposition 4.7.3, we deduce that there is a bijection between the set of square-free integers (excluding 0 and 1) and the set of quadratic number fields via

$$d \longleftrightarrow \mathbb{Q}[\sqrt{d}].$$

We now give a concrete characterisation of number rings corresponding to quadratic number fields.

Theorem 4.7.5. Let $K = \mathbb{Q}[\sqrt{d}]$ be a quadratic field where d is a square-free integer excluding 0 and 1 $\big($In particular, $d \not\equiv 0 \pmod 4\big)$. Let $R = \mathbb{A} \cap K$ be the corresponding number ring. Then

1. $R = \left\{a + b\sqrt{d} \;\middle|\; a, b \in \mathbb{Z}\right\}$ if $d \equiv 2$ or $3 \pmod 4$.
2. $R = \left\{\dfrac{a + b\sqrt{d}}{2} \;\middle|\; a, b \in \mathbb{Z},\ a \equiv b \pmod 2\right\}$ if $d \equiv 1 \pmod 4$.

Proof. Let $z = a + b\sqrt{d}$. Then z is the root of $f(x) = x^2 - 2ax + a^2 - db^2$. If $a, b \in \mathbb{Z}$, $f(x)$ clearly has coefficients in $\mathbb{Z}$.

If $d \equiv 1 \pmod 4$ and we have $a = a'/2$ and $b = b'/2$ instead, where $a', b' \in \mathbb{Z}$ and $a' \equiv b' \pmod 2$, then firstly observe that $2a \in \mathbb{Z}$. We also have $(a')^2 - d(b')^2 \equiv 0 \pmod 4$ so $a^2 - db^2 \in \mathbb{Z}$. Thus $f(x)$ also has coefficients in $\mathbb{Z}$.

We now prove that every element in R must be of the above form. Let $\alpha = r + s\sqrt{d} \in R$, where $r, s \in \mathbb{Q}$. If $s = 0$, then $\alpha = r \in \mathbb{Z}$ by Corollary 4.1.9 and we are done. If $s \neq 0$, then $m_\alpha(x) = x^2 - 2rx + r^2 - ds^2$. By Proposition 4.1.8, we have $2r \in \mathbb{Z}$ and $r^2 - ds^2 \in \mathbb{Z}$.

Thus $4r^2 \in \mathbb{Z}$ and $4r^2 - 4ds^2 \in \mathbb{Z}$ and so $4ds^2 = d(2s)^2 \in \mathbb{Z}$. Write $2s = p/q$ where $p, q \in \mathbb{Z}$ with $\gcd(p, q) = 1$. We have $q^2 \mid d$ in $\mathbb{Z}$ so $q = \pm 1$ since d is square-free. Thus $2s \in \mathbb{Z}$.

Let $x = 2r$ and $y = 2s$. By multiplying 4 to $r^2 - ds^2$, we have $x^2 - dy^2 \equiv 0 \pmod 4$. If $d \equiv 2$ or $3 \pmod 4$, then $x \equiv y \equiv 0 \pmod 2$ so $r, s \in \mathbb{Z}$. On the other hand, if $d \equiv 1 \pmod 4$, we have $x \equiv y \pmod 2$. This completes the proof.

Finally, we will give explicit formulas for computing trace, norm and discriminant. Let R be a number ring corresponding to the quadratic field $\mathbb{Q}[\sqrt{d}]$ where d is a square-free integer that is not 0 or 1.

Proposition 4.7.6. Let $r = a + b\sqrt{d} \in R$. Then $T^R(r) = 2a$ and $N^R(r) = a^2 - b^2 d$.

Proof. We use the definition given in section 4.5. A $\mathbb{Z}$-basis for R is given by $\{1, \sqrt{d}\}$ if $d \equiv 2$ or $3 \pmod 4$ and $\left\{1, \frac{1+\sqrt{d}}{2}\right\}$ if $d \equiv 1 \pmod 4$. Under this basis, the $\mathbb{Z}$-linear multiplication map $\varphi_r : R \to R$ is represented by the matrix

$$\Phi_r = \begin{pmatrix} a & bd \\ b & a \end{pmatrix} \quad \text{or} \quad \Phi_r = \begin{pmatrix} a - b & \frac{bd-b}{2} \\ 2b & a + b \end{pmatrix}$$

respectively. In both cases, $\mathrm{tr}(\Phi_r) = 2a$ and $\det(\Phi_r) = a^2 - bd^2$.

Proposition 4.7.7. The discriminant of the ring is given by

$$\operatorname{disc}(R) = \begin{cases} 4d & \text{if } d \equiv 2 \text{ or } 3 \pmod 4 \\ d & \text{if } d \equiv 1 \pmod 4. \end{cases}$$

Proof. If $d \equiv 2$ or $3 \pmod 4$, then using the basis $\left\{1, \sqrt{d}\right\}$, we have

$$\operatorname{disc}(R) = \det\left(\begin{pmatrix} T^R(1) & T^R(\sqrt{d}) \\ T^R(\sqrt{d}) & T^R(d) \end{pmatrix}\right) = \det\left(\begin{pmatrix} 2 & 0 \\ 0 & 2d \end{pmatrix}\right) = 4d.$$

If $d \equiv 1 \pmod 4$, then using the basis $\left\{1, \frac{1+\sqrt{d}}{2}\right\}$, we have

$$\operatorname{disc}(R) = \det\left(\begin{pmatrix} T^R(1) & T^R\left(\frac{1+\sqrt{d}}{2}\right) \\ T^R\left(\frac{1+\sqrt{d}}{2}\right) & T^R\left(\frac{1+d}{4} + \frac{\sqrt{d}}{2}\right) \end{pmatrix}\right) = \det\left(\begin{pmatrix} 2 & 1 \\ 1 & \frac{1+d}{2} \end{pmatrix}\right) = d.$$

5 Quadratic Rings

In this chapter, we will generalise to the same setting as which Manjul Bhargava adopted in his PhD thesis.

5.1 Basic Definitions

Definition 5.1.1. A commutative ring R with unity is called a **quadratic ring** if its additive group is isomorphic to $\mathbb{Z}^2$.

If R is a quadratic ring, then the notion of trace, norm and discriminant can still be discussed by using the definitions given in section 4.5.

Remark 5.1.2. If R is a quadratic ring and we have $\alpha, \beta \in R$, then we let $\langle \alpha, \beta \rangle$ denote

$$\left\{ x \cdot \alpha + y \cdot \beta \;\middle|\; x, y \in \mathbb{Z} \right\}.$$

Proposition 5.1.3. Let R be a quadratic ring. Then there exists $\tau \in R$ such that $\{1_R, \tau\}$ is a $\mathbb{Z}$-basis for R.

Proof. Let $N = \langle 1_R \rangle$. Then N is a free $\mathbb{Z}$-submodule of R of rank 1. It suffices to prove that R/N is also a free $\mathbb{Z}$-module of rank 1 since we can then choose τ to be the generator of R/N. We will do that by showing that R/N is a torsion-free $\mathbb{Z}$-module.

Suppose R/N is not torsion-free. Let $x \in R$ be such that $\overline{x}$ is a non-zero torsion element in R/N, where $\overline{x}$ indicates the image of x in the quotient. Then there exists $A \in \mathbb{Z}_{\geq 1}$ such that $A \cdot \overline{x} = 0_{R/N}$. Thus there exist $T \in \mathbb{Z} \setminus \{0\}$ such that $A \cdot x = T \cdot 1_R$. By dividing both sides if necessary, we may assume $\gcd(A, T) = 1$. Note that $A \geq 2$ since $\overline{x}$ is non-zero in the quotient. Let $\{\alpha, \beta\}$ be a $\mathbb{Z}$-basis for R. We write $x = a_1\alpha + b_1\beta$ and $1_R = a_2\alpha + b_2\beta$ for some $a_1, a_2, b_1, b_2 \in \mathbb{Z}$. We have

$$Aa_1 \cdot \alpha + Ab_1 \cdot \beta = Ta_2 \cdot \alpha + Tb_2 \cdot \beta.$$

By comparing coefficients, we have $Aa_1 = Ta_2$ and $Ab_1 = Tb_2$. Since $\gcd(A, T) = 1$, we have $T \mid a_1$ and $T \mid b_1$ in $\mathbb{Z}$. Then

$$A \cdot \left(\frac{a_1}{T} \cdot \alpha + \frac{b_1}{T} \cdot \beta \right) = a_2 \cdot \alpha + b_2 \cdot \beta.$$

Since $a_2 \cdot \alpha + b_2 \cdot \beta = 1_R$, for all $n \in \mathbb{Z}_{\geq 1}$, we have

$$A^n \cdot \left(\frac{a_1}{T} \cdot \alpha + \frac{b_1}{T} \cdot \beta \right)^n = a_2 \cdot \alpha + b_2 \cdot \beta.$$

Choose n such that $A^n > \max\{a_2, b_2\}$ (this is possible since $A \geq 2$) and we get our desired contradiction.

Proposition 5.1.4. Let R be a quadratic ring and let D be its discriminant. Then $D \equiv 0$ or $1 \pmod 4$.

Proof. There exists a $\mathbb{Z}$-basis of R of the form $\{1, \tau\}$ by the previous proposition. Since τ^2 can be expressed as a $\mathbb{Z}$-linear combination of 1 and τ, we have that τ satisfies a quadratic equation $\tau^2 + r\tau + s = 0$ for some $r, s \in \mathbb{Z}$. Under this basis, a direct computation reveals that

$$\begin{aligned} \operatorname{disc}(R) &= \det\left(\begin{pmatrix} T^R(1) & T^R(\tau) \\ T^R(\tau) & T^R(\tau^2) \end{pmatrix}\right) \\ &= \det\left(\begin{pmatrix} 2 & -r \\ -r & r^2 - 2s \end{pmatrix}\right) \\ &= r^2 - 4s. \end{aligned}$$

When r is even, $\operatorname{disc}(R) \equiv 0 \pmod 4$ and when r is odd, $\operatorname{disc}(R) \equiv 1 \pmod 4$.

Definition 5.1.5. A quadratic ring R is **nondegenerate** if its discriminant is non-zero.

Definition 5.1.6. Let R be a quadratic ring of discriminant D. A $\mathbb{Z}$-basis $\{1, \tau\}$ of R is **regular** if τ satisfies

$$\begin{aligned} \tau^2 - \frac{D}{4} &= 0 \quad \text{if } D \equiv 0 \pmod 4 \\ \tau^2 - \tau + \frac{1 - D}{4} &= 0 \quad \text{if } D \equiv 1 \pmod 4. \end{aligned}$$

Proposition 5.1.7. Every quadratic ring has a regular $\mathbb{Z}$-basis.

Let R be a ring and let D be its discriminant. Then R admits a $\mathbb{Z}$-basis of the form $\{1, \tau\}$, where τ satisfies $\tau^2 + r\tau + s = 0$ for some $r, s \in \mathbb{Z}$.

If $D \equiv 0 \pmod 4$, then from the proof of Proposition 5.1.4, we know that r is even. Observe that

$$\begin{aligned} \left(\tau + \frac{r}{2}\right)^2 - \frac{D}{4} &= \tau^2 + r\tau + \frac{r^2}{4} - \frac{r^2}{4} + s \\ &= \tau^2 + r\tau + s \\ &= 0 \end{aligned}$$

and so $\tau + \frac{r}{2}$ is a root to $x^2 - \frac{D}{4}$. If $D \equiv 1 \pmod 4$, then r is odd and we have

$$\begin{aligned}
&\left(\tau + \frac{r+1}{2}\right)^2 - \left(\tau + \frac{r+1}{2}\right) + \frac{1-D}{4} \\
&= \tau^2 + (r+1)\tau + \frac{r^2+2r+1}{4} - \tau - \frac{r+1}{2} + \frac{1}{4} - \frac{r^2}{4} + s \\
&= \tau^2 + r\tau + s \\
&= 0
\end{aligned}$$

so $\tau + \frac{r+1}{2}$ is a root to $x^2 - x + \frac{1-D}{4}$.

Since $\{1, \tau\}$ is a $\mathbb{Z}$-basis for R, we have that $\{1, \tau + r/2\}$ of $\{1, \tau + (r+1)/2\}$ (depending on whether $D \equiv 0$ or $1 \pmod 4$) are also $\mathbb{Z}$-bases for R. This completes the proof of the proposition.

Corollary 5.1.8. All quadratic rings of the same discriminant are isomorphic to each other as rings.

Proof. We already know that all quadratic rings are isomorphic to $\mathbb{Z}^2$ as additive groups. By Proposition 5.1.7, the multiplicative structure of a quadratic ring is completely determined by its discriminant. The conclusion follows.

Proposition 5.1.9. Let D be an integer congruent to 0 or 1 modulo 4. Then there exists a quadratic ring of discriminant D.

Proof. For an integer $D \equiv 0$ or $1 \pmod 4$, an explicit quadratic ring R of discriminant D is given by

$$R = \begin{cases} \mathbb{Z}[x] \ / \ (x^2) & \text{if } D = 0 \\ \mathbb{Z} \cdot (1,1) + \sqrt{D}(\mathbb{Z} \oplus \mathbb{Z}) & \text{if } D \text{ is a perfect square} \\ \mathbb{Z}[(D + \sqrt{D})/2] & \text{otherwise.} \end{cases}$$

By Corollary 5.1.8 and Proposition 5.1.9, there is a bijection between the set of integers congruent to 0 or 1 modulo 4 and the set of isomorphism classes of quadratic rings.

However, the isomorphism is not canonical since the regular basis given in Definition 5.1.6 is not unique. This is because for every nondegenerate quadratic ring of discriminant D, there are 2 different elements which satisfy

$$x^2 - \frac{D}{4} = 0 \ \text{ or } \ x^2 - x + \frac{1-D}{4} = 0. \tag{3}$$

Thus all nondegenerate quadratic rings R have two automorphisms, namely the identity automorphism and a non-trivial automorphism φ. If $\{1, \tau\}$ is a regular basis of R, and τ' is the other root to (3), then $\varphi : R \to R$ is given by

$$\varphi(a + b\tau) = a + b\tau'.$$

To eliminate the extra automorphism, we consider oriented quadratic rings by fixing a choice of τ. This gives rise to a natural projection map $\pi : R \to \mathbb{Z}$ via

$$\pi(a + b\tau) = b$$

Since π has kernel $\mathbb{Z}$, it induces a group isomorphism $R/\mathbb{Z} \to \mathbb{Z}$.

Definition 5.1.10. An **oriented quadratic ring** is a pair (R, π) where R is a quadratic ring and $\pi : R/\mathbb{Z} \to \mathbb{Z}$ is the group isomorphism induced by the choice of τ.

Since there are no automorphisms on oriented quadratic rings, we now state the theorem in full.

Theorem 5.1.11. There is a bijection between the set of integers congruent to 0 or 1 modulo 4 and the set of oriented quadratic rings.

We use $S(D)$ to denote the unique oriented quadratic ring of discriminant D.

Remark 5.1.12. For an oriented quadratic ring $S(D)$, we will use φ to denote the unique non-trivial automorphism on $S(D)$.

Next, we generalise the concept of fractional ideals to our new setting as well.

Definition 5.1.13. Let $S(D)$ be an oriented quadratic ring and define $K = S(D) \otimes_{\mathbb{Z}} \mathbb{Q}$. A **fractional ideal** I of $S(D)$ is a $S(D)$-submodule of K such that there exists $s \in S(D)$ with the following properties :

(i) s is invertible in K.

(ii) $sI \subseteq S(D)$.

Since $S(D) \cong \mathbb{Z}^2$ as $\mathbb{Z}$-modules, any non-zero fractional ideal of $S(D)$ must be isomorphic to either $\mathbb{Z}$ or $\mathbb{Z}^2$ as $\mathbb{Z}$-modules. In this report, we are only interested in studying the latter case.

Definition 5.1.14. An **oriented fractional ideal** is a pair (I, ϵ) where I is a fractional ideal of $S(D)$ that is isomorphic to $\mathbb{Z}^2$ as a $\mathbb{Z}$-module and $\epsilon = \pm 1$ indicates the **orientation** of I. Multiplication of oriented fractional ideals is done component wise. If $k \in K$ is a scalar, then define

$$k \cdot (I, \epsilon) = \big(kI,\ \epsilon \cdot \operatorname{sgn}(N^{S(D)}(k))\big).$$

For simplicity, we will sometimes denote an oriented ideal (I, ϵ) simply by I and let $\text{sgn}(I) = \epsilon$ denote the orientation of I. An oriented ideal I is **positively oriented** if $\text{sgn}(I) = 1$ and **negatively oriented** if $\text{sgn}(I) = -1$.

Proposition 5.1.15. Let I be an oriented fractional ideal of an oriented quadratic ring $S(D)$. Then there exists $n \in \mathbb{Z} \setminus \{0\}$ such that $n \cdot I \subseteq S(D)$.

Proof. Let $\{\alpha_1, \alpha_2\}$ be a $\mathbb{Z}$-basis for I. If $\{1, \tau\}$ is a regular basis for $S(D)$, then there exists $x_1, x_2, y_1, y_2 \in \mathbb{Q}$ such that

$$\alpha_1 = x_1 \cdot 1_R + y_1 \cdot \tau \quad \text{and} \quad \alpha_2 = x_2 \cdot 1_R + y_2 \cdot \tau.$$

Let n be a common denominator for x_1, x_2, y_1, y_2 and we are done.

Definition 5.1.16. Let $S(D)$ be an oriented quadratic ring. A regular basis $\{1, \tau\}$ of S is **positively oriented** if $\pi(\tau) > 0$. For an oriented fractional ideal I of $S(D)$, a $\mathbb{Z}$-basis $\{\alpha, \beta\}$ is positively oriented if the change-of-basis matrix from $\{1, \tau\}$ to $\{\alpha, \beta\}$ has positive determinant.

Proposition 5.1.17. Let $S(D)$ be an oriented quadratic ring and let $\{1, \tau\}$ be a regular $\mathbb{Z}$-basis for $S(D)$. Then for any $a, b \in \mathbb{Z}$,

$$N^{S(D)}(a + b\tau) = \begin{cases} a^2 - \frac{b^2 D}{4} & \text{if } D \equiv 0 \pmod 4 \\ (a + \frac{b}{2})^2 - \frac{b^2 D}{4} & \text{if } D \equiv 1 \pmod 4). \end{cases}$$

Proof. If $D \equiv 0 \pmod 4$, then $\tau^2 = \dfrac{D}{4}$. Using the basis $\{1, \tau\}$, we have

$$\begin{aligned} N^{S(D)}(a + b\tau) &= \det\left(\begin{pmatrix} a & bD/4 \\ b & a \end{pmatrix}\right) \\ &= a^2 - \frac{b^2 D}{4}. \end{aligned}$$

If $D \equiv 1 \pmod 4$, then $\tau^2 = \tau + \dfrac{D-1}{4}$. We have

$$\begin{aligned} N^{S(D)}(a + b\tau) &= \det\left(\begin{pmatrix} a & (bD - b)/4 \\ b & a + b \end{pmatrix}\right) \\ &= a^2 + ab - \frac{b^2 D - b^2}{4} \\ &= \left(a + \frac{b}{2}\right)^2 - \frac{b^2 D}{4}. \end{aligned}$$

Proposition 5.1.18. Let $S(D)$ be an oriented quadratic ring and let $\{1, \tau\}$ be a regular basis for $S(D)$. Then we have the following three identities :

$$\begin{aligned}
\tau + \varphi(\tau) &= \begin{cases} 0 & \text{if } D \equiv 0 \pmod 4 \\ 1 & \text{if } D \equiv 1 \pmod 4 \end{cases} \\
\tau \cdot \varphi(\tau) &= \begin{cases} -\frac{D}{4} & \text{if } D \equiv 0 \pmod 4 \\ \frac{1-D}{4} & \text{if } D \equiv 1 \pmod 4 \end{cases} \\
\tau - \varphi(\tau) &= \pm\sqrt{D}.
\end{aligned}$$

Proof. If $D = 0$, then $S(D) \cong \mathbb{Z}[x] \ / \ (x^2)$ and we have $\tau = \varphi(\tau) = x$ so the three identities trivially hold.

If $D \neq 0$, then in the explicit list of quadratic rings given in Proposition 5.1.9, the two choices of τ are

(a) $\left(\dfrac{\sqrt{D}}{2}, \dfrac{-\sqrt{D}}{2}\right)$ and $\left(\dfrac{-\sqrt{D}}{2}, \dfrac{\sqrt{D}}{2}\right)$ if $D \equiv 0 \pmod 4$ is a square.

(b) $\left(\dfrac{\sqrt{D}+1}{2}, \dfrac{-\sqrt{D}+1}{2}\right)$ and $\left(\dfrac{-\sqrt{D}+1}{2}, \dfrac{\sqrt{D}+1}{2}\right)$ if $D \equiv 1 \pmod 4$ is a square.

(c) $\dfrac{\sqrt{D}}{2}$ and $\dfrac{-\sqrt{D}}{2}$ if $D \equiv 0 \pmod 4$ is not a square.

(d) $\dfrac{\sqrt{D}+1}{2}$ and $\dfrac{-\sqrt{D}+1}{2}$ if $D \equiv 1 \pmod 4$ is not a square.

The three identities can then be verified directly.

Proposition 5.1.19. Let $S(D)$ be an oriented quadratic ring and let $\varphi : S(D) \to S(D)$ be the unique non-trivial automorphism on $S(D)$. Then for any $\alpha \in S(D)$, we have

$$N^{S(D)}(\alpha) = \alpha \cdot \varphi(\alpha).$$

Proof. Let $\{1, \tau\}$ be a regular basis for $S(D)$. There exists $a, b \in \mathbb{Z}$ such that $\alpha = a + b\tau$. Then observe that

$$\begin{aligned}
\alpha \cdot \varphi(\alpha) &= (a + b\tau) \cdot (a + b\varphi(\tau)) \\
&= a^2 + ab(\tau + \varphi(\tau)) + b^2(\tau \cdot \varphi(\tau))
\end{aligned}$$

If $D \equiv 0 \pmod 4$,

$$a^2 + ab(\tau + \varphi(\tau)) + b^2(\tau \cdot \varphi(\tau)) = a^2 - \frac{b^2 D}{4}.$$

If $D \equiv 1 \pmod 4$,

$$\begin{aligned} a^2 + ab(\tau + \varphi(\tau)) + b^2(\tau \cdot \varphi(\tau)) &= a^2 + ab + \frac{b^2(1 - D)}{4} \\ &= \left(a + \frac{b}{2}\right)^2 - \frac{b^2 D}{4}. \end{aligned}$$

Both cases agree with Proposition 5.1.17.

5.2 Norm of an Ideal

In order to generalise the notion of norm to arbitrary quadratic rings, we will develop the concept in the language of lattices.

Definition 5.2.1. Let V be a finite-dimensional $\mathbb{Q}$-vector space of dimension n. A $\mathbb{Z}$-submodule L of V is a **lattice** if $L \cong \mathbb{Z}^n$ as $\mathbb{Z}$-modules.

Remark 5.2.2. Note that any quadratic ring $S(D)$ can be viewed as a $\mathbb{Z}$-submodule of the 2-dimensional $\mathbb{Q}$-vector space $S(D) \otimes_{\mathbb{Z}} \mathbb{Q}$. Thus every quadratic ring and every oriented fractional ideal of a quadratic ring are lattices.

Before we can properly define the norm of an ideal, we will first need to prove a few propositions. For the rest of this section, V and n will be as defined in Definition 5.2.1.

Proposition 5.2.3. Let L_1 and L_2 be two lattices in V. Then there exist a lattice containing both L_1 and L_2.

Proof. It suffices to prove that the set

$$L_1 + L_2 = \{x + y \mid x \in L_1,\ y \in L_2\}$$

is a lattice of V. It is clear that $L_1 + L_2$ is a finitely generated torsion-free $\mathbb{Z}$-submodule of V. Since $\mathbb{Z}$ is a PID, this implies that $L_1 + L_2$ is free. Any $\mathbb{Z}$-basis for $L_1 + L_2$ is linearly independent over $\mathbb{Q}$ (Lemma 4.5.5) and so cannot contain more than n elements. Thus $L_1 + L_2$ has finite rank m, with $m \leq n$. Finally, $L_1 + L_2$ contains a free $\mathbb{Z}$-module of rank n so $m \geq n$. Hence we get $m = n$ so $L_1 + L_2$ is a lattice.

Proposition 5.2.4. Let L be a lattice in V and let $\varphi : V \to V$ be a $\mathbb{Q}$-linear automorphism. Then $\varphi(L)$ is a lattice in V. If $\varphi(L) \subseteq L$ then $|L/\varphi(L)| = |\det(\varphi)|$.

Proof. Let $\{x_1, \cdots, x_n\}$ be a $\mathbb{Z}$-basis for L. Then $\{\varphi(x_1), \cdots, \varphi(x_n)\}$ is a $\mathbb{Z}$-basis for $\varphi(L)$ since φ is injective. Thus $\varphi(L)$ is a lattice of V.

Under the original basis $\{x_1, \cdots, x_n\}$, the map φ can also be viewed as a $\mathbb{Z}$-linear automorphism $L \to L$ via restriction (denoted by $\varphi|_L$). Thus φ can be represented by a $M_{n\times n}(\mathbb{Z})$ matrix A. By the Smith Normal Form, there exist matrices $P, Q \in GL_n(\mathbb{Z})$ such that

$$PAQ = \begin{pmatrix} a_1 & 0 & \cdots & 0 \\ 0 & a_2 & \cdots & \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a_n \end{pmatrix}$$

is diagonal. Since determinant of P and Q is ± 1, we have that $|\det(A)| = |a_1 \cdots a_n|$.

On the other hand, $L/\varphi(L) = \operatorname{coker}(\varphi|_L) \cong \mathbb{Z}/(a_1) \oplus \cdots \oplus \mathbb{Z}/(a_n)$ and so we have $|L/\varphi(L)| = |a_1 \cdots a_n|$ as desired.

Proposition 5.2.5. Let L_1 and L_2 be two lattices in V. Then there exists a $\mathbb{Q}$-linear automorphism $\varphi : V \to V$ such that $\varphi(L_1) = L_2$.

Proof. Let $X = \{x_1, \cdots, x_n\}$ and $Y = \{y_1, \cdots, y_n\}$ be $\mathbb{Z}$-bases for L_1 and L_2 respectively. Then define $\varphi : V \to V$ by setting $\varphi(x_i) = y_i$ for all i. Since X and Y are also $\mathbb{Q}$-bases for V, the map φ is in fact an automorphism.

Corollary 5.2.6. Let L_1 and L_2 be two lattices in V such that $L_1 \subseteq L_2$. Then L_2/L_1 is finite.

Proof. Let φ be a $\mathbb{Q}$-linear automorphism such that $\varphi(L_2) = L_1$. Then by Proposition 5.2.4, we have that $|L_2/L_1| = |\det(\varphi)|$ which is clearly finite.

Remark 5.2.7. If R is a number ring and I is a non-zero ideal of R, then R and I are both lattices so R/I is finite.

Proposition 5.2.8. Let L_1, L_2, M be lattices in V such that M contains both L_1 and L_2. Let $\varphi : V \to V$ be a $\mathbb{Q}$-linear automorphism such that $\varphi(L_1) = L_2$. Then we have

$$|\det(\varphi)| = \frac{|M/L_2|}{|M/L_1|}.$$

Proof. Let $\pi : V \to V$ be a $\mathbb{Q}$-linear automorphism such that $\pi(M) = L_1$. Then

$$\frac{|M/L_2|}{|M/L_1|} = \frac{|\det(\varphi \circ \pi)|}{|\det(\pi)|} = |\det(\varphi)|.$$

Proposition 5.2.8 gives us two immediate corollaries.

Corollary 5.2.9. If φ_1 and φ_2 are both $\mathbb{Q}$-linear automorphisms with the property that $\varphi_1(L_1) = \varphi_2(L_1) = L_2$, then $|\det(\varphi_1)| = |\det(\varphi_2)|$.

Corollary 5.2.10. If M and N are lattices in V containing both L_1 and L_2, then

$$\frac{|M/L_1|}{|M/L_2|} = \frac{|N/L_1|}{|N/L_2|}.$$

Definition 5.2.11 (Norm of an ideal)**.** Let $S(D)$ be an oriented quadratic ring and let I be a oriented fractional ideal of $S(D)$. Define the **norm** of I by

$$N^{S(D)}(I) = \operatorname{sgn}(I) \cdot \frac{|L/I|}{|L/S(D)|}$$

where L is any lattice in $K = S(D) \otimes_{\mathbb{Z}} \mathbb{Q}$ containing both I and $S(D)$.

Remark 5.2.12. If I is integral and positively oriented, then by choosing $L = S(D)$, we get

$$N^{S(D)}(I) = \frac{|S(D)/I|}{|S(D)/S(D)|} = |S(D)/I|$$

which coincides with the traditional definition of absolute norm of an ideal.

We shall now state some useful properties about the ideal norm.

Proposition 5.2.13. Let $\alpha \in K$ be invertible and be I be an oriented fractional ideal generated by α. Then

$$N^{S(D)}(I) = \operatorname{sgn}(I) \cdot |N^{S(D)}(\alpha)|.$$

Proof. By definition $N^{S(D)}(\alpha) = \det(\varphi_\alpha)$, where $\varphi_\alpha : K \to K$ is the $\mathbb{Q}$-linear multiplication map

$$\varphi_\alpha(w) = \alpha w.$$

Note that φ_α is an automorphism satisfying $\varphi_\alpha(S(D)) = I$ (its inverse is the multiplication map $\varphi_{\alpha^{-1}}$). For any lattice M in K containing I, we have by Proposition 5.2.8,

$$N^{S(D)}(I) = \operatorname{sgn}(I) \cdot \frac{|M/I|}{|M/S(D)|} = \operatorname{sgn}(I) \cdot |\det(\varphi_\alpha)|.$$

Corollary 5.2.14. Let J be a oriented fractional ideal of $S(D)$ and let $\alpha \in J$. Then $\dfrac{N^{S(D)}(\alpha)}{N^{S(D)}(J)} \in \mathbb{Z}$.

Proof. If α is not invertible in K, then α is a zero divisor so the multiplication map $\varphi_\alpha : K \to K$ is not bijective. Then $N^{S(D)}(\alpha) = \det(\varphi_\alpha) = 0$ so the statement trivially holds. Thus we may assume α is invertible in K.

Let I be a oriented fractional ideal generated by α and let L be a lattice containing both M and J. Then

$$\begin{aligned}\frac{|N^{S(D)}(\alpha)|}{|N^{S(D)}(J)|} &= \frac{|N^{S(D)}(I)|}{|N^{S(D)}(J)|} \\ &= \frac{|M/I|}{|M/S(D)|} \cdot \frac{|M/S(D)|}{|M/J|} \\ &= \frac{|M/I|}{|M/J|}.\end{aligned}$$

Since $I \subseteq J$, by Corollary 5.2.10

$$\begin{aligned}\frac{|M/I|}{|M/J|} &= \frac{|J/I|}{|J/J|} \\ &= |J/I|\end{aligned}$$

which is an integer.

Theorem 5.2.15. Let I be an oriented fractional ideal of K and J be a oriented principal fractional ideal of K generated by some invertible $j \in K$. Then

$$N^{S(D)}(IJ) = N^{S(D)}(I)N^{S(D)}(J).$$

Proof. Note that the multiplication map $\varphi_j : K \to K$ is again an automorphism satisfying $\varphi_j(I) = IJ$. For any lattice M in K containing both I and J, we have by Propositions 5.2.8 and 5.2.13 :

$$\begin{aligned}N^{S(D)}(IJ) &= \operatorname{sgn}(IJ) \cdot \frac{|M/IJ|}{|M/S(D)|} \\ &= \operatorname{sgn}(I) \cdot \frac{|M/I|}{|M/S(D)|} \cdot \operatorname{sgn}(J) \cdot \frac{|M/IJ|}{|M/I|} \\ &= N^{S(D)}(I) \cdot \operatorname{sgn}(J) \cdot |\det(\varphi_j)| \\ &= N^{S(D)}(I)N^{S(D)}(J).\end{aligned}$$

Remark 5.2.16. The ideal norm is not multiplicative in general. Take for example $S(D) = \mathbb{Z}[\sqrt{-9}]$ and let $I = (3, 3i)$. Then $S(D)/I = \{0 + I,\ 1 + I,\ 2 + I\}$ and so

$$|S(D)/I| = 3.$$

On the other hand, $I^2 = (9, 9i)$ and so $S(D)/I^2 = \{x + 3yi + I \mid 0 \le x < 9,\ 0 \le y < 3\}$. Thus we have

$$|S(D)/I^2| = 27.$$

5.3 Narrow Class Group

In this section, let D be a non-zero integer congruent to 0 or 1 modulo 4 and let $S(D)$ be the unique oriented quadratic ring of discriminant D. Further let $\{1, \tau\}$ be a regular $\mathbb{Z}$-basis for $S(D)$. Firstly, we define a standard basis for oriented fractional ideals to make computations easier.

Theorem 5.3.1. Every oriented integral ideal I of $S(D)$ has a unique $\mathbb{Z}$-basis of the form $\{a, b + g\tau\}$ satisfying

(i) $a, b, g \in \mathbb{Z}$.

(ii) $a > 0$.

(iii) $0 \leq b < a$.

(iv) $0 < g \leq a$.

(v) g divides both a and b in $\mathbb{Z}$.

Proof. We will prove this theorem via several smaller propositions.

Proposition 5.3.2. The ideal I has a $\mathbb{Z}$-basis of the form $\{a, b + g\tau\}$, where

(i) $a, b, g \in \mathbb{Z}$.

(ii) $a > 0$.

(iii) $0 \leq b < a$.

(iv) $0 < g \leq a$.

Proof. Let $\{\alpha_1, \alpha_2\}$ be any $\mathbb{Z}$-basis of I. Write

$$\alpha_1 = a_1 + b_1\tau \text{ and } \alpha_2 = a_2 + b_2\tau \quad \text{with } a_1, a_2, b_1, b_2 \in \mathbb{Z}.$$

For any $k \in \mathbb{Z}$, observe that $\alpha_1 x + \alpha_2 y = \alpha_1(x + ky) + (\alpha_2 - k\alpha_1)y$. Thus by symmetry, we deduce that the two operations

$$\{\alpha_1, \alpha_2 - k\alpha_1\} \quad \text{and} \quad \{\alpha_1 - k\alpha_2, \alpha_2\} \tag{4}$$

on the basis do not change the ideal I. This allows us to perform the Euclidean algorithm on b_1 and b_2, which terminates when either $b_1 = 0$ or $b_2 = 0$. Thus, by performing a single swap at the end if necessary, we have $I = \langle a, b + g\tau \rangle$ with $a, b, g \in \mathbb{Z}$. Note that $a \neq 0$ and $g \neq 0$ since I has rank 2 as a $\mathbb{Z}$-module. Next, since we have $\langle a, b + g\tau \rangle = \langle -a, b + g\tau \rangle$, we may assume $a > 0$. Finally, by subtracting multiples of a and $a\tau$ from $b + g\tau$ if needed, we further assume that $0 \leq b < a$ and $0 < g \leq a$.

Proposition 5.3.3. Let $c \in \mathbb{Z} \cap I$. Then $a \mid c$ in $\mathbb{Z}$.

Proof. There exists unique $x, y \in \mathbb{Z}$ such that $c = ax + (b + g\tau)y$. Thus we must have $y = 0$.

Proposition 5.3.4. The $\mathbb{Z}$-basis of I with the properties (i) to (iv) of Proposition 5.3.2 is completely determined by I.

Proof. Let $\{a', b' + g'\tau\}$ be another $\mathbb{Z}$-basis of I satisfying properties (i) to (iv).

By Proposition 5.3.3, we have $a' \mid a$ and $a \mid a'$ in $\mathbb{Z}$. Thus $a = a'$ as both a and a' are positive. Next, observe that there exists $x_1, y_1, x_2, y_2 \in \mathbb{Z}$ such that

$$\begin{aligned} ax_1 + (b + g\tau)y_1 = b' + g'\tau &\implies ax_1 + by_1 = b' \text{ and } gy_1 = g'. \\ ax_2 + (b' + g'\tau)y_2 = b + g\tau &\implies ax_2 + b'y_2 = b \text{ and } g'y_2 = g. \end{aligned}$$

Since $g \mid g'$ and $g' \mid g$ in $\mathbb{Z}$, we again must have $g = g'$ since both g and g' are positive. Thus $y_1 = y_2 = 1$ and since $0 \leq b, b' < a$, it follows that $x_1 = x_2 = 0$ and so $b = b'$.

Proposition 5.3.5. In the basis given in Proposition 5.3.2, we have $g \mid a$ and $g \mid b$ in $\mathbb{Z}$.

Proof. Since $a\tau \in I$, there exists $x, y \in \mathbb{Z}$ such that $ax + (b + g\tau)y = a\tau$. Then we have $gy = a$ and so $g \mid a$.

Next, $(b + g\tau)\tau \in I$ so there exists $x', y' \in \mathbb{Z}$ such that $ax' + (b + g\tau)y' = b\tau + g\tau^2$.

If $D \equiv 0 \pmod 4$, then $\tau^2 = \dfrac{D}{4}$ so we have $gy' = b$.

If $D \equiv 1 \pmod 4$, then $\tau^2 = -\dfrac{1 - D}{4} + \tau$ so we have $gy' = b + g$ instead.

In both cases, we conclude that $g \mid b$.

Propositions 5.3.2 to 5.3.5 prove Theorem 5.3.1.

While all oriented integral ideals I of $S(D)$ can be written in the form $\langle \alpha_1, \alpha_2 \rangle$ for some $\alpha_1, \alpha_2 \in S(D)$, the converse is not true in general. In other words, not all sets of the form $\langle \alpha_1, \alpha_2 \rangle$ are necessarily ideals. The next theorem gives conditions for α_1 and α_2 such that $\langle \alpha_1, \alpha_2 \rangle$ is an ideal.

Theorem 5.3.6. Let a, b and g be integers satisfying

(i) $a > 0$.

(ii) $0 \leq b < a$.

(iii) $g > 0,\ g \mid a$ and $g \mid b$ in $\mathbb{Z}$.

(iv) $ag \mid N^{S(D)}(b + g\tau)$ in $\mathbb{Z}$.

Then $\langle a, b + g\tau \rangle$ is a integral ideal of $S(D)$ having rank 2 as a $\mathbb{Z}$-module with standard basis $\{a, b + g\tau\}$.

Proof. We only need to check that $\langle a, b + g\tau \rangle$ is indeed an ideal of $S(D)$. Firstly, note that $\langle a, b + g\tau \rangle$ is an ideal if and only if $\langle a/g, b/g + \tau \rangle$ is an ideal. Since conditions (i) to (iv) are still satisfied if a, b and g were replaced by $a/g, b/g$ and 1 respectively, we may assume $g = 1$.

To prove that $\langle a, b + \tau \rangle$ is an ideal of $S(D)$, it suffices to prove that the ideal

$$I = \big\{ \chi a + \gamma(b + \tau) \mid \chi, \gamma \in S(D) \big\}$$

has standard basis $\{a, b + \tau\}$. Let $\{t, r + s\tau\}$ be the standard basis for I. Then there exists $u, v \in \mathbb{Z}$ such that $ut + v(r + s\tau) = b + \tau$. Thus $vs = 1$ so $s = 1$ since s is positive. Next we need a lemma.

Lemma 5.3.7. Let $z \in I \cap \mathbb{Z}$. Then $a \mid z$ in $\mathbb{Z}$.

Proof. Note that z is of the form

$$\begin{aligned} z &= a(x_1 + y_1\tau) + (b + \tau)(x_2 + y_2\tau) \\ &= ax_1 + bx_2 + y_2\tau^2 + \tau(ay_1 + by_2 + x_2) \end{aligned}$$

for some $x_1, x_2, y_1, y_2 \in \mathbb{Z}$. If $D \equiv 0 \pmod 4$ then

$$z = ax_1 + bx_2 + \frac{y_2 D}{4} + \tau(ay_1 + by_2 + x_2).$$

For z to be an integer, we must have

$$ay_1 + by_2 + x_2 = 0 \implies x_2 = -ay_1 - by_2.$$

By using the formula in Proposition 5.1.17

$$\begin{aligned} z &= ax_1 + b(-ay_1 - by_2) + \frac{y_2 D}{4} \\ &= ax_1 - aby_1 - \left(b^2 - \frac{D}{4}\right) y_2 \\ &= ax_1 - aby_1 - N^{S(D)}(b+\tau) y_2 \end{aligned}$$

which is divisible by a. If $D \equiv 1 \pmod 4$, then

$$z = ax_1 + bx_2 + y_2\left(\frac{D-1}{4}\right) + \tau(ay_1 + by_2 + x_2 + y_2)$$

For z to be an integer, we must have

$$ay_1 + by_2 + x_2 + y_2 = 0 \implies x_2 = -ay_1 - by_2 - y_2$$

and similarly,

$$\begin{aligned} z &= ax_1 + b(-ay_1 - by_2 - y_2) + y_2\left(\frac{D-1}{4}\right) \\ &= ax_1 - aby_1 - y_2\left[\left(b + \frac{1}{2}\right)^2 - \frac{D}{4}\right] \\ &= ax_1 - aby_1 - y_2 N^{S(D)}(b+\tau). \end{aligned}$$

which is also divisible by a.

This lemma tells us that we must have $t = a$. Finally, observe that since $b + \tau \in I$ and $r + \tau \in I$, we have $b - r \in I$. But $a \mid b - r$ in $\mathbb{Z}$, and together with the condition that $0 \leq b < a$ and $0 \leq r < a$, we have that $b = r$.

Remark 5.3.8. Theorem 5.3.1 generalises to fractional ideals in the following form : Let I be a fractional ideal of $S(D)$. By Proposition 5.1.14, there exist $n \in \mathbb{Z}$ be such that nI is integral. If $\{a, b + g\tau\}$ is the standard basis for nI, then $\{a/n, (b + g\tau)/n\}$ is the standard basis for I. It is easy to check that the uniqueness of the standard basis still holds for fractional ideals.

With the standard basis, the norm of an ideal can be computed easily.

Theorem 5.3.9. Let $I = \langle \alpha_1, \alpha_2 \rangle$ be an oriented fractional ideal of $S(D)$. Then

$$N^{S(D)}(I) = \operatorname{sgn}(I) \cdot \left| \frac{\alpha_1 \varphi(\alpha_2) - \varphi(\alpha_1)\alpha_2}{\sqrt{D}} \right|.$$

Proof. We first prove that the right hand side is independent of the choice of basis. If $\langle \alpha_1, \alpha_2 \rangle$ is replaced with $\langle \alpha_1, \alpha_2 - k\alpha_1 \rangle$ for some $k \in \mathbb{Z}$, then

$$\begin{aligned}\left|\frac{\alpha_1\varphi(\alpha_2 - k\alpha_1) - \varphi(\alpha_1)(\alpha_2 - k\alpha_1)}{\sqrt{D}}\right| &= \left|\frac{\alpha_1\big[\varphi(\alpha_2) - k\varphi(\alpha_1)\big] - \varphi(\alpha_1)\big[\alpha_2 - k\alpha_1\big]}{\sqrt{D}}\right| \\ &= \left|\frac{\alpha_1\varphi(\alpha_2) - \varphi(\alpha_1)\alpha_2}{\sqrt{D}}\right|\end{aligned}$$

so the norm of the ideal is unchanged. The case of $\langle \alpha_1 - k\alpha_2, \alpha_2 \rangle$ is similar. Since any basis of I can be reduced to the canonical basis via these two operations (and swapping of α_1 with α_2), the definition is independent of the choice of basis.

Next, we will prove the result for the case where I is an integral ideal by using the standard basis $\{a, b + g\tau\}$. Under this basis, we have

$$\begin{aligned}\operatorname{sgn}(I) \cdot \left|\frac{\alpha_1\varphi(\alpha_2) - \varphi(\alpha_1)\alpha_2}{\sqrt{D}}\right| &= \operatorname{sgn}(I) \cdot \left|\frac{a[b + g\varphi(\tau)] - a[b + g\tau]}{\sqrt{D}}\right| \\ &= \operatorname{sgn}(I) \cdot \left|\frac{ag\big[\varphi(\tau) - \tau\big]}{\sqrt{D}}\right| \\ &= \operatorname{sgn}(I) \cdot ag\end{aligned}$$

where the last equality is due to Proposition 5.1.18.

Lemma 5.3.10. The elements of the quotient ring $S(D)/I$ are precisely

$$\Big\{x + y\tau + I \mid 0 \le x < a,\ 0 \le y < g\Big\}.$$

Proof. We first prove that any element in $S(D)/I$ is equivalent to an element in the above set. Let $x + y\tau + I \in S(D)/I$. Then by adding or subtracting multiples of $b + g\tau + I$, we may assume $0 \le y < g$. Next, add or subtract multiples of $a + I$ and we have $0 \le x < a$ as desired.

Secondly, we prove that every element in the above set is distinct. Assume that there exists $x_1, x_2, y_1, y_2 \in \mathbb{Z}$ such that

$$x_1 + y_1\tau + I = x_2 + y_2\tau + I \ \text{ and } \ 0 \le x_1, x_2 < a,\ 0 \le y_1, y_2 < g.$$

Without loss of generality assume $y_1 \ge y_2$. Then $(x_1 - x_2) + (y_1 - y_2)\tau \in I$. There exists $u, v \in \mathbb{Z}$ such that

$$(x_1 - x_2) + (y_1 - y_2)\tau = ua + v(b + g\tau).$$

Then $g \mid y_1 - y_2$ in $\mathbb{Z}$ and since $0 \le y_1 - y_2 < g$, we must have $y_1 - y_2 = 0$. Thus $v = 0$ and so $a \mid x_1 - x_2$ in $\mathbb{Z}$.

Similarly, we have $0 \leq x_1, x_2 < a$ so $-a < |x_1 - x_2| < a$ and hence $x_1 - x_2 = 0$. We conclude that $x_1 = x_2$ and $y_1 = y_2$ which completes the proof of the lemma.

Thus $N^{S(D)}(I) = \operatorname{sgn}(I) \cdot |S(D)/I| = \operatorname{sgn}(I) \cdot ag$ so the statement holds when I is integral.

Now let I be a general oriented fractional ideal with $\mathbb{Z}$-basis $\{\beta_1, \beta_2\}$. Then there exists $s \in S(D)$ such that s is invertible in $K = S(D) \otimes_{\mathbb{Z}} \mathbb{Q}$ and sI is an integral ideal. Using the fact that $\{s\beta_1, s\beta_2\}$ is a $\mathbb{Z}$-basis for sI, we have by Proposition 5.2.13 and Theorem 5.2.15 :

$$\begin{aligned} N^{S(D)}(I) &= \frac{N^{S(D)}(sI)}{N^{S(D)}(s)} \\ &= \left| \frac{s\beta_1\varphi(s)\varphi(\beta_2) - \varphi(s)\varphi(\beta_1)s\beta_2}{s\varphi(s)\sqrt{D}} \right| \\ &= \left| \frac{\beta_1\varphi(\beta_2) - \varphi(\beta_1)\beta_2}{\sqrt{D}} \right|. \end{aligned}$$

Definition 5.3.11. Let $P^+(S(D))$ denote the subgroup of all oriented principal fractional ideals of $S(D)$ of the form

$$\Big((k),\ \operatorname{sgn}\big(N^{S(D)}(k)\big)\Big)$$

where k is invertible in K. The **narrow class group** of a quadratic ring $S(D)$ (denoted by $Cl^+(D)$) is defined to be the quotient

$$Cl^+(D) = F(S(D))/P^+(S(D))$$

where $F(S(D))$ is the group of invertible oriented fractional ideals of $S(D)$.

5.4 Relationship Between Form Class Group and Narrow Class Group

We will now prove the main theorem of interest in this paper. The theorem consist of two parts.

Theorem 5.4.1. Let D be a non-zero integer congruent to 0 or 1 modulo 4. Let $BQF(D)$ denote the set of $SL_2(\mathbb{Z})$-equivalence classes of binary quadratic forms of discriminant D and let $FI(D)$ denote the set of oriented fractional ideals (not necessarily invertible) of $S(D)$ modulo multiplication by invertible scalars $k \in K$. Then there is a bijection between $BQF(D)$ and $FI(D)$.

Remark 5.4.2. For an ideal J, we let $\overline{J}$ denote the equivalence class of J in $FI(D)$. Similarly for a binary quadratic form f, let $\overline{f}$ denote its $SL_2(\mathbb{Z})$-equivalence class in $BQF(D)$.

Remark 5.4.3. Both parts of the theorem also holds true for the case of D being a perfect square. However, more careful treatment of the corner cases will be needed since some binary quadratic forms will be of the form $ax^2 + bxy + 0y^2$. Thus we will only prove for the case of D not being a perfect square.

Proof. We will construct explicit bijections from $FI(D)$ to $BQF(D)$ and vice versa. Let $\{1, \tau\}$ be a positively oriented regular basis for $S(D)$.

Let $J = \langle \alpha_1, \alpha_2 \rangle$ be an oriented fractional ideal of $S(D)$, where $\{\alpha_1, \alpha_2\}$ is oriented in accordance to the orientation of J. Define $\Phi : FI(D) \to BQF(D)$ by

$$\Phi(\overline{J}) = \frac{\big[\alpha_1 x + \alpha_2 y\big]\big[\varphi(\alpha_1)x + \varphi(\alpha_2)y\big]}{N^{S(D)}(J)}.$$

Propositions 5.4.4 to 5.4.6 will show that Φ is a well-defined map.

Proposition 5.4.4. $\Phi(\overline{J})$ is an integral binary quadratic form of discriminant D.

Proof. Expanding, we have

$$\Phi(\overline{J}) = \frac{\alpha_1\varphi(\alpha_1)x^2 + \big(\alpha_1\varphi(\alpha_2) + \varphi(\alpha_1)\alpha_2\big)xy + \alpha_2\varphi(\alpha_2)y^2}{N^{S(D)}(J)}.$$

Note that $\dfrac{N(\alpha_1)}{N^{S(D)}(J)}, \dfrac{N(\alpha_2)}{N^{S(D)}(J)}$ and $\dfrac{N(\alpha_1 + \alpha_2)}{N^{S(D)}(J)}$ are all integers (Corollary 5.2.14) so

$$\frac{\alpha_1\varphi(\alpha_2) + \varphi(\alpha_1)\alpha_2}{N^{S(D)}(J)} = \frac{N(\alpha_1 + \alpha_2) - N(\alpha_1) - N(\alpha_2)}{N^{S(D)}(J)}$$

is an integer as well.

A direct computation shows that the discriminant of $\Phi(\overline{J})$ is

$$\begin{aligned}
&\left(\frac{\alpha_1\varphi(\alpha_2)+\varphi(\alpha_1)\alpha_2}{N^{S(D)}(J)}\right)^2 - 4\left(\frac{\alpha_1\varphi(\alpha_1)}{N^{S(D)}(J)}\right)\left(\frac{\alpha_2\varphi(\alpha_2)}{N^{S(D)}(J)}\right)\\
&= \frac{\alpha_1^2\varphi(\alpha_2)^2 - 2\alpha_1\varphi(\alpha_1)\alpha_2\varphi(\alpha_2) + \varphi(\alpha_1)^2\alpha_2^2}{N^{S(D)}(J)^2}\\
&= \frac{(\alpha_1\varphi(\alpha_2) - \varphi(\alpha_1)\alpha_2)^2}{N^{S(D)}(J)^2}\\
&= D.
\end{aligned}$$

where the last equality is due to Theorem 5.3.9.

Proposition 5.4.5. If $\{\alpha_1, \alpha_2\}$ and $\{\beta_1, \beta_2\}$ are similarly oriented $\mathbb{Z}$-bases for J, then

$$\big[\alpha_1 x + \alpha_2 y\big]\big[\varphi(\alpha_1)x + \varphi(\alpha_2)y\big] \text{ and } \big[\beta_1 x + \beta_2 y\big]\big[\varphi(\beta_1)x + \varphi(\beta_2)y\big]$$

are $SL_2(\mathbb{Z})$-equivalent.

Proof. First observe that for any $k \in \mathbb{Z}$, the change-of-basis matrices from $\{\alpha_1, \alpha_2\}$ to $\{\alpha_1, \alpha_2 - k\alpha_1\}$ and $\{\alpha_1 - k\alpha_2, \alpha_2\}$ are given by

$$\begin{pmatrix} 1 & 0 \\ -k & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & -k \\ 0 & 1 \end{pmatrix}$$

respectively. Since both matrices have determinant 1, these two operations does not change the orientation of the $\mathbb{Z}$-basis.

In the proof of Proposition 5.3.2, we have shown that $\{\alpha_1, \alpha_2\}$ and $\{\beta_1, \beta_2\}$ can be reduced to either $\{a, b+g\tau\}$ or $\{b+g\tau, a\}$ via operations of the form (4). Since $\{\alpha_1, \alpha_2\}$ and $\{\beta_1, \beta_2\}$ are both similarly oriented, we deduce that operations of the form (4) are sufficient to transform $\{\alpha_1, \alpha_2\}$ to $\{\beta_1, \beta_2\}$ (In other words, no swapping of the basis elements is needed).

Thus we may assume, without loss of generality, that $\{\beta_1, \beta_2\} = \{\alpha_1, \alpha_2 - k\alpha_1\}$. The case for $\{\beta_1, \beta_2\} = \{\alpha_1 - k\alpha_2, \alpha_2\}$ is similar. We have

$$\begin{aligned}
&\big[\alpha_1 x + (\alpha_2 - k\alpha_1)y\big]\big[\varphi(\alpha_1)x + \varphi(\alpha_2 - k\alpha_1)y\big]\\
&= \big[\alpha_1 x + (\alpha_2 - k\alpha_1)y\big]\big[\varphi(\alpha_1)x + \big(\varphi(\alpha_2) - k\varphi(\alpha_1)\big)y\big]\\
&= \alpha_1\varphi(\alpha_1)x^2 + \big[\alpha_1\varphi(\alpha_2) + \varphi(\alpha_1)\alpha_2 - 2k\alpha_1\varphi(\alpha_1)\big]xy\\
&+ \big[\alpha_2\varphi(\alpha_2) - k(\alpha_1\varphi(\alpha_2) + \varphi(\alpha_1)\alpha_2) + k^2\alpha_1\varphi(\alpha_1)\big]y^2.
\end{aligned}$$

This is $SL_2(\mathbb{Z})$-equivalent to $\alpha_1\varphi(\alpha_1)x^2 + [\alpha_1\varphi(\alpha_2) + \varphi(\alpha_1)\alpha_2]xy + \alpha_2\varphi(\alpha_2)y^2$ via the matrix $(T^{-k})^T$ by Remark 2.1.9.

Proposition 5.4.6. If J and J' are equivalent ideals, then $\Phi\big(\overline{J}\big) = \Phi\big(\overline{J'}\big)$.

Proof. There exists $s \in S(D)$ such that s is invertible in K and $sJ = J'$. Observe that if $J = \langle \alpha_1, \alpha_2 \rangle$, then $J' = \langle s\alpha_1, s\alpha_2 \rangle$. The determinant of the change-of-basis matrix is precisely $N^{S(D)}(s)$. Thus if $\{\alpha_1, \alpha_2\}$ is oriented according to J then $\{s\alpha_1, s\alpha_2\}$ is also oriented according to J'.

Let $I = \big((s),\ \operatorname{sgn}(N^{S(D)}(s))\big)$. Then $IJ = J'$. By Proposition 5.2.13, we have

$$\begin{aligned} N^{S(D)}(I) &= \operatorname{sgn}(N^{S(D)}(s)) \cdot |N^{S(D)}(s)| \\ &= \operatorname{sgn}(s\varphi(s)) \cdot |s\varphi(s)| \\ &= s\varphi(s). \end{aligned}$$

Now by Theorem 5.2.15, we have

$$\begin{aligned} \Phi(J') &= \frac{\big[s\alpha_1 x + s\alpha_2 y\big]\big[\varphi(s\alpha_1)x + \varphi(s\alpha_2)y\big]}{N^{S(D)}(J')} \\ &= \frac{s\varphi(s)\big[\alpha_1 x + \alpha_2 y\big]\big[\varphi(\alpha_1)x + \varphi(\alpha_2)y\big]}{N^{S(D)}(I)N^{S(D)}(J)} \\ &= \frac{s\varphi(s)[\alpha_1 x + \alpha_2 y][\varphi(\alpha_1)x + \varphi(\alpha_2)y]}{s\varphi(s)N^{S(D)}(J)} \\ &= \Phi(J). \end{aligned}$$

We now define the other half of the isomorphism. For a given binary quadratic form $f = [A, B, C]$, define $\Psi : BQF(D) \to FI(D)$ by

$$\Psi\big(\overline{f}\big) = \Big(\big\langle A, b_B + \tau\big\rangle,\ \operatorname{sgn}(A)\Big)$$

where $b_B = \dfrac{B}{2}$ or $\dfrac{B-1}{2}$ depending on whether $D \equiv 0$ or $1 \pmod 4$ respectively.

Remark 5.4.7. Note that regardless of whether $D \equiv 0$ or $1 \pmod 4$, we have that

$$N^{S(D)}(b_B + \tau) = \frac{B^2 - D}{4}.$$

Propositions 5.4.8 and 5.4.9 will show that Ψ is well-defined.

Proposition 5.4.8. Let $f = [A, B, C]$ be a binary quadratic form of discriminant D. Then $\big(\langle A, b_B + \tau\rangle,\ \operatorname{sgn}(A)\big)$ is an oriented integral ideal of $S(D)$ with standard basis $\big\{|A|, b' + \tau\big\}$, where $b' \equiv b_B \pmod{|A|}$.

Proof. Since -1 is a unit in $\mathbb{Z}$, we have $\langle A, b_B + \tau\rangle = \langle -A, b_B + \tau\rangle$. Thus we assume $A > 0$.

There exists $k \in \mathbb{Z}$ such that $0 \leq b_B + kA < A$. Then $\langle A, b_B + \tau\rangle = \langle A, b_B + kA + \tau\rangle$. If $D \equiv 0 \pmod 4$, then using Proposition 5.1.17,

$$\begin{aligned} N^{S(D)}(b_B + kA + \tau) &= N^{S(D)}\left(\frac{B}{2} + kA + \tau\right) \\ &= \left(\frac{B}{2} + kA\right)^2 - \frac{D}{4} \end{aligned}$$

and if $D \equiv 1 \pmod 4$, we have

$$\begin{aligned} N^{S(D)}(b_B + kA + \tau) &= N^{S(D)}\left(\frac{B-1}{2} + kA + \tau\right) \\ &= \left(\frac{B-1}{2} + kA + \frac{1}{2}\right)^2 - \frac{D}{4} \\ &= \left(\frac{B}{2} + kA\right)^2 - \frac{D}{4}. \end{aligned}$$

Using the fact that $B^2 - 4AC = D$, we have

$$\begin{aligned} \left(\frac{B}{2} + kA\right)^2 - \frac{D}{4} &= \frac{B^2 - D}{4} + kAB + k^2A^2 \\ &= AC + kAB + k^2A^2 \end{aligned}$$

which is divisible by A. By Theorem 5.3.6, we have that $\langle A, b_B + kA + \tau\rangle$ is an ideal of $S(D)$ with canonical basis $\{A, b_B + kA + \tau\}$ which completes the proof.

Proposition 5.4.9. Let $\overline{f}, \overline{g} \in BQF(D)$ be two $SL_2(\mathbb{Z})$-equivalent binary quadratic forms. Then $\Psi(\overline{f}) = \Psi(\overline{g})$.

Proof. Let $f = [A, B, C]$. To show that $SL_2(\mathbb{Z})$-equivalent binary quadratic forms get mapped to equivalent ideals, it suffices to prove that this is true under the generators of $SL_2(\mathbb{Z})$, which are S and T. (Theorem 2.1.7) Since $(S^{-1}T^TS)^{-1} = T$ and we know that S and T generate $SL_2(\mathbb{Z})$, we deduce that S and T^T also generate T.

Generator S produces the equivalence $[A, B, C] \sim [C, -B, A]$. Using $\sim$ to denote narrow equivalence of ideals, we have

$$\begin{aligned}
\Big(\big\langle A, b_B + \tau\big\rangle,\ \mathrm{sgn}(A)\Big) &\sim \Big(\Big\langle A\big(b_B + \varphi(\tau)\big),\ N^{S(D)}(b_B + \tau)\Big\rangle,\ \mathrm{sgn}(A) \cdot \mathrm{sgn}\big(N^{S(D)}(b_B + \tau)\big)\Big) \\
&\sim \Big(\Big\langle b_B + \varphi(\tau),\ \frac{B^2 - D}{4A}\Big\rangle,\ \mathrm{sgn}(A) \cdot \mathrm{sgn}\big(N^{S(D)}(b_B + \tau)\big)\Big) \\
&\sim \Big(\Big\langle C,\ b_B + \varphi(\tau)\Big\rangle,\ \mathrm{sgn}(A) \cdot \mathrm{sgn}\big(N^{S(D)}(b_B + \tau)\big)\Big).
\end{aligned}$$

Since -1 is a unit in $\mathbb{Z}$, this is equal to

$$\Big(\Big\langle C,\ -b_B - \varphi(\tau)\Big\rangle,\ \mathrm{sgn}(A) \cdot \mathrm{sgn}\big(N^{S(D)}(b_B + \tau)\big)\Big)$$

By Proposition 5.1.18, we have $-b_B - \varphi(\tau) = b_{-B} + \tau$ in both cases. Thus we get

$$\Big(\Big\langle C,\ b_{-B} + \tau\Big\rangle,\ \mathrm{sgn}(A) \cdot \mathrm{sgn}\big(N^{S(D)}(b_B + \tau)\big)\Big)$$

Observe that $N^{S(D)}(b_B + \tau) = AC$. Thus

$$\mathrm{sgn}(C) = \mathrm{sgn}(A) \cdot \mathrm{sgn}\big(N^{S(D)}(b_B + \tau)\big)$$

and we are done.

The other generator T^T produces the equivalence $[A, B, C] \sim [A, 2A + B, A + B + C]$. Let $k = [A, 2A + B, A + B + C]$. Then

$$\begin{aligned}
\Psi\big(\overline{k}\big) &= \Big(\langle A, b_{2A+B} + \tau\rangle,\ \mathrm{sgn}(A)\Big) \\
&= \Big(\langle A, b_B + A + \tau\rangle,\ \mathrm{sgn}(A)\Big) \\
&= \Big(\langle A, b_B + \tau\rangle,\ \mathrm{sgn}(A)\Big) \\
&= \Psi\big(\overline{f}\big).
\end{aligned}$$

Proposition 5.4.10. Ψ and Φ are inverses of each other.

Proof. Let $f = [A, B, C]$ be a binary quadratic form. Then

$$\Phi \circ \Psi\big(\overline{f}\big) = \Phi\Big[\Big(\big\langle A, b_B + \tau\big\rangle,\ \mathrm{sgn}(A)\Big)\Big].$$

Note that the change of basis matrix from $\{1, \tau\}$ to $\{A, b_B + \tau\}$ is given by $\begin{pmatrix} A & 0 \\ b_B & 1 \end{pmatrix}$.

Thus regardless of whether A is positive or negative, the basis $\{A, b_B + \tau\}$ has the same orientation as the ideal $(\langle A, b_B + \tau\rangle,\ \operatorname{sgn}(A))$. Since the standard basis is of the form $\{|A|, b' + \tau\}$ where $b' \equiv b \pmod{A}$, the norm is given by $\operatorname{sgn}(A) \cdot |A| = A$. Thus we have

$$\begin{aligned}\Phi\Big[\Big(\langle A, b_B + \tau\rangle,\ \operatorname{sgn}(A)\Big)\Big] &= \frac{A^2x^2 + [A(b_B + \varphi(\tau)) + A(b_B + \tau)]xy + ACy^2}{A} \\ &= Ax^2 + Bxy + Cy^2.\end{aligned}$$

On the other hand, if I is a positively oriented fractional ideal with standard basis $\{a, b + g\tau\}$, then

$$\begin{aligned}\Psi \circ \Phi(I) &= \Psi\bigg(\frac{a^2x^2 + [a(b + g\varphi(\tau)) + a(b + g\tau)]xy + (b + g\tau)(b + g\varphi(\tau))y^2}{ag}\bigg) \\ &= \Psi\bigg(\frac{a}{g}x^2 + \Big(\frac{2b}{g} + \tau + \varphi(\tau)\Big)xy + \Big(\frac{N^{S(D)}(b + g\tau)}{ag}\Big)y^2\bigg).\end{aligned}$$

If $D \equiv 0 \pmod 4$, this is equal to

$$\bigg(\Big\langle \frac{a}{g},\ \frac{b}{g} + \frac{\tau + \varphi(\tau)}{2} + \tau\Big\rangle,\ 1\bigg) = \bigg(\Big\langle \frac{a}{g},\ \frac{b}{g} + \tau\Big\rangle,\ 1\bigg).$$

If $D \equiv 1 \pmod 4$, we have

$$\bigg(\Big\langle \frac{a}{g},\ \frac{b}{g} + \frac{\tau + \varphi(\tau) - 1}{2} + \tau\Big\rangle,\ 1\bigg) = \bigg(\Big\langle \frac{a}{g},\ \frac{b}{g} + \tau\Big\rangle,\ 1\bigg).$$

In both cases, this is narrowly equivalent to I. If I is negatively oriented, then the order of the basis must be swapped since the standard basis $\{a, b + g\tau\}$ is positively oriented. We have

$$\begin{aligned}\Psi \circ \Phi(I) &= \Psi\bigg(\frac{(b + g\tau)(b + g\varphi(\tau))x^2 + [(b + g\tau)a + (b + g\varphi(\tau))a]xy + a^2y^2}{-ag}\bigg) \\ &= \Psi\bigg(-\Big(\frac{N^{S(D)}(b + g\tau)}{ag}\Big)x^2 - \Big(\frac{2b}{g} + \tau + \varphi(\tau)\Big)xy - \frac{a}{g}y^2\bigg) \\ &= \Psi\bigg(-\frac{a}{g}x^2 + \Big(\frac{2b}{g} + \tau + \varphi(\tau)\Big)xy - \Big(\frac{N^{S(D)}(b + g\tau)}{ag}\Big)y^2\bigg).\end{aligned}$$

Using a similar argument, in both cases this is equal to

$$\bigg(\Big\langle -\frac{a}{g},\ \frac{b}{g} + \tau\Big\rangle,\ -1\bigg) = \bigg(\Big\langle \frac{a}{g},\ \frac{b}{g} + \tau\Big\rangle,\ -1\bigg)$$

and the same conclusion follows.

In the second part of the theorem, we will study the bijection when restricted to the set of primitive binary quadratic forms and invertible ideals. Let $Cl^+(D)$ denote the narrow class group of the quadratic ring $S(D)$ and let $C^2(D)$ denote the form class group of discriminant D. Let Φ^* and Ψ^* denote the restriction of Φ and Ψ to $Cl^+(D)$ and $C^2(D)$ respectively.

Theorem 5.4.11. For a non-zero integer D congruent to 0 or 1 modulo 4, we have $\Phi^*(Cl^+(D)) = C^2(D)$ and $\Psi^*(C^2(D)) = Cl^+(D)$.

Proof. Let $f = [A, B, C]$ be a binary quadratic form of discriminant D. Since Φ and Ψ are inverses of each other, it suffices to prove that $\Psi\big(\overline{f}\big)$ is invertible if and only if $\gcd(A, B, C) = 1$.

Let $I = \Psi\big(\overline{f}\big)$. Then I is invertible if and only if $IJ = S(D)$, where J is the oriented fractional ideal given by

$$J = \Big(\{z \in K \mid zI \subseteq S(D)\},\ \operatorname{sgn}(I)\Big).$$

Lemma 5.4.12. An explicit $\mathbb{Z}$-basis for J is given by $J = \left\langle 1, \dfrac{b_{-B} + \tau}{A} \right\rangle$.

Proof. The ideal I has $\mathbb{Z}$-basis $\{A, b_B + \tau\}$. Let $\big\{a, b + g\tau\big\}$ be the standard basis of J for some $a, b, g \in \mathbb{Q}$. We must have $a \in \mathbb{Z}$ since

$$a(b_B + \tau) = ab_B + a\tau \in S(D).$$

On the other hand, any integer $n \in J$ must be an integer multiple of a. Since $1 \in J$, we conclude that $a = 1$.

Next, observe that $A \cdot \dfrac{b_{-B} + \tau}{A} \in S(D)$. If $D \equiv 0 \pmod 4$, then

$$(b_B + \tau)\left(\frac{b_{-B} + \tau}{A}\right) = \frac{D - B^2}{4A} = -C \in S(D).$$

If $D \equiv 1 \pmod 4$, then similarly

$$(b_B + \tau)\left(\frac{b_{-B} + \tau}{A}\right) = \frac{1}{A}\left(\left(\tau - \frac{1}{2}\right)^2 - \frac{B^2}{4}\right) = \frac{D - B^2}{4A} = -C \in S(D).$$

In both cases, $\dfrac{b_{-B} + \tau}{A} \in J$. Thus there exists $n' \in \mathbb{Z}$ such that $\dfrac{b_{-B} + \tau}{A} = n'b + n'g\tau$.

In particular, $n'g = \dfrac{1}{A}$. On the other hand,

$$A \cdot (b + g\tau) \in S(D) \implies Ag \in \mathbb{Z}$$

so we must have $n' = \pm 1$ and $g = \dfrac{1}{|A|}$.

We will finish off the proof of our lemma by showing that $\dfrac{b_{-B}}{A} - b \in \mathbb{Z}$. If $D \equiv 0 \pmod 4$,

$$(b_B + \tau)\left(b + \frac{\tau}{A}\right) = b_B b + \frac{D}{4A} + \left(\frac{b_B}{A} + b\right)\tau \in S(D).$$

Thus $\dfrac{b_B}{A} + b \in \mathbb{Z}$ so multiplying by -1 gives $\dfrac{b_{-B}}{A} - b \in \mathbb{Z}$. If $D \equiv 1 \pmod 4$, we have

$$(b_B + \tau)\left(b + \frac{\tau}{A}\right) = b_B b + \frac{D-1}{4A} + \left(\frac{b_B + 1}{A} + b\right)\tau.$$

Similarly, we have $\dfrac{b_B + 1}{A} + b \in \mathbb{Z}$ and so $\dfrac{b_{-B}}{A} - b \in \mathbb{Z}$.

By the lemma, the ideal IJ is generated over $\mathbb{Z}$ by the 4 elements

$$A,\ b_B + \tau,\ b_{-B} + \tau,\ C.$$

Thus any integer in IJ must be a multiple of

$$\gcd\big(A, (b_B - b_{-B}), C\big).$$

Note that $b_B - b_{-B} = B$. Since $IJ = S(D)$ if and only if IJ contains 1, we conclude that I is invertible if and only if $\gcd(A, B, C) = 1$.

Theorem 5.4.13. Ψ and Φ are group homomorphisms.

Proof. Since Ψ and Φ are inverses of each other, it suffices to show that Ψ is a group homomorphism. Let $\overline{f}, \overline{g} \in C^2(D)$. There exists $A, A', B, C \in \mathbb{Z}$ with $f \sim [A, B, CA']$ and $g \sim [A', B, CA]$. Then $f \bullet g \sim [AA', B, C]$.

Let $I = \big\langle A, b_B + \tau \big\rangle$ and $J = \big\langle A', b_B + \tau \big\rangle$. By a direct (but tedious) computation, we have that $IJ = \langle AA', b_B + \tau \rangle$ (A proof is provided in Appendix 7.1). We have

$$\begin{aligned} \Psi(\overline{f}) * \Psi(\overline{g}) &= \big(I, \operatorname{sgn}(A)\big) * \big(J, \operatorname{sgn}(A')\big) \\ &= \big(IJ, \operatorname{sgn}(A)\operatorname{sgn}(A')\big) \\ &= \big(IJ, \operatorname{sgn}(AA')\big) \\ &= \Psi\big(\overline{f \bullet g}\big) \end{aligned}$$

so Ψ is a group homomorphism as desired.

Corollary 5.4.14. Let I and J be invertible oriented fractional ideals of a nondegenerate quadratic ring $S(D)$. Then

$$N^{S(D)}(IJ) = N^{S(D)}(IJ).$$

Proof. By Theorem 5.4.11, there exists primitive binary quadratic forms f, g such that $\Psi(\overline{f})$ and $\Psi(\overline{g})$ are narrowly equivalent to I and J respectively. Let $I' = \Psi(\overline{f})$ and $J' = \Psi(\overline{g})$. There exists $A, A', B, C \in \mathbb{Z}$ such that $f \sim [A, B, CA']$ and $g \sim [A', B, CA]$. We have that $f \bullet g = [AA', B, C]$.

By Proposition 5.4.8, I' and J' has standard basis $\{|A|, b_1 + \tau\}$ and $\{|A'|, b_2 + \tau\}$ respectively, where $b_1 \equiv B \pmod{|A|}$ and $b_2 \equiv B \pmod{|A'|}$. Thus

$$N^{S(D)}(I') = \operatorname{sgn}(A) \cdot |A| = A.$$

Similarly, $N^{S(D)}(J') = A'$. On the other hand, $I'J' = \Psi(\overline{f \bullet g})$ so it has standard basis $\{AA', b_3 + \tau\}$ where $b_3 \equiv B \pmod{|AA'|}$. Thus $N^{S(D)}(I'J') = AA' = N^{S(D)}(I')N^{S(D)}(J')$.

We now return back to our original setting. Since I and J are narrowly equivalent to I' and J', there exists invertible principal oriented ideals

$$P_1 = \big((\alpha_1),\ \operatorname{sgn}(N^{S(D)}(\alpha_1))\big) \quad \text{and} \quad P_2 = \big((\alpha_2),\ \operatorname{sgn}(N^{S(D)}(\alpha_2))\big)$$

such that $I' = P_1 I$ and $J' = P_2 J$. Then $I'J' = P_1 P_2 I J$. Using the multiplicativity of ideal norm for principal ideals (Theorem 5.2.15), we get

$$\begin{aligned}
N^{S(D)}(I)N^{S(D)}(J) &= \frac{N^{S(D)}(P_1)N^{S(D)}(I)N^{S(D)}(P_2)N^{S(D)}(J)}{N^{S(D)}(P_1)N^{S(D)}(P_2)} \\
&= \frac{N^{S(D)}(P_1 I)N^{S(D)}(P_2 J)}{N^{S(D)}(P_1 P_2)} \\
&= \frac{N^{S(D)}(P_1 P_2 I J)}{N^{S(D)}(P_1 P_2)} \\
&= \frac{N^{S(D)}(P_1 P_2)N^{S(D)}(IJ)}{N^{S(D)}(P_1 P_2)} \\
&= N^{S(D)}(IJ).
\end{aligned}$$

6 Bhargava's Reformulation

6.1 Bhargava's Cube

We first introduce the central object used by Manjul Bhargava in his attempt to generalise Gauss' Composition. Most of the proofs for claims made in this section are omitted since they can be verified by a direct (but tedious) computation.

Definition 6.1.1. Let $\mathcal{C}_{2\times2\times2}$ denote $\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2$, where the tensor product is taken over $\mathbb{Z}$. Each element of $\mathcal{C}_{2\times2\times2}$ can be represented as a vector (a, b, c, d, e, f, g, h). This can be viewed as a cube of integers

$$(a, b, c, d, e, f, g, h) \tag{5}$$

Any cube X can be partitioned into

$$M_1 = \begin{bmatrix} a & b \\ c & d \end{bmatrix}, \; N_1 = \begin{bmatrix} e & f \\ g & h \end{bmatrix}$$

or

$$M_2 = \begin{bmatrix} a & c \\ e & g \end{bmatrix}, \; N_1 = \begin{bmatrix} b & d \\ f & h \end{bmatrix}$$

or

$$M_1 = \begin{bmatrix} a & e \\ b & f \end{bmatrix}, \; N_1 = \begin{bmatrix} c & g \\ d & h \end{bmatrix}.$$

Definition 6.1.2. For a cube $X \in \mathcal{C}_{2\times2\times2}$ and $i \in \{1, 2, 3\}$, define

$$Q_i^X(x, y) = -\det\big(M_i x - N_i y\big).$$

If X is given as in (5), then explicit formulas for Q_1^X, Q_2^X and Q_3^X are given by

$$\begin{aligned} Q_1^X &= (bc - ad)x^2 + (ah + de - bg - cf)xy + (fg - eh)y^2 \\ Q_2^X &= (ce - ag)x^2 + (ah + bg - cf - de)xy + (df - bh)y^2 \\ Q_3^X &= (be - af)x^2 + (ah + cf - bg - de)xy + (dg - ch)y^2. \end{aligned}$$

Definition 6.1.3. An element

$$\left(\begin{bmatrix} r_1 & s_1 \\ t_1 & u_1 \end{bmatrix}, \begin{bmatrix} r_2 & s_2 \\ t_2 & u_2 \end{bmatrix}, \begin{bmatrix} r_3 & s_3 \\ t_3 & u_3 \end{bmatrix} \right)$$

of the group $\Gamma = SL_2(\mathbb{Z}) \times SL_2(\mathbb{Z}) \times SL_2(\mathbb{Z})$ act on a cube $X \in C_{2\times2\times2}$ by replacing (M_i, N_i) with $(rM_i + sN_i, tM_i + uN_i)$ for each i. The action of the three factors commute with each other and thus the action is well-defined.

Definition 6.1.4. Two cubes $X, Y \in C_{2\times2\times2}$ are **Γ-equivalent** if X and Y lie in the same orbit under the Γ-action.

It can be verified by direct computation that X and Y are Γ-equivalent if and only if the binary quadratic forms Q_i^X and Q_i^Y are $SL_2(\mathbb{Z})$-equivalent for all $i \in \{1, 2, 3\}$.

Definition 6.1.5. Let $X \in C_{2\times2\times2}$. A direct computation reveals that the discriminant of Q_1^X, Q_2^X and Q_3^X are equal. We define the **discriminant** of X by

$$\operatorname{disc}(X) = \operatorname{disc}(Q_1^X) = \operatorname{disc}(Q_2^X) = \operatorname{disc}(Q_3^X).$$

If X is given as in (5), then we have

$$\begin{aligned}\operatorname{disc}(X) &= a^2h^2 + b^2g^2 + c^2f^2 + d^2e^2 \\ &\quad - 2(abgh + cdef + acfh + bdeg + aedh + bfcg) + 4(adfg + bceh).\end{aligned}$$

Remark 6.1.6. It follows immediately from the definition that the discriminant of a cube must be congruent to either 0 or 1 modulo 4.

By the second part of Definition 6.1.4, we also have that the discriminant of a cube is invariant under the Γ-action.

Definition 6.1.7. A cube $X \in \mathcal{C}_{2\times2\times2}$ is **projective** if its three associated binary quadratic forms Q_1^X, Q_2^X and Q_3^X are all primitive.

Let $C^+_{2\times2\times2}(D)$ denote the set of projective cubes of discriminant D.

Proposition 6.1.8. Let X be a projective cube. Then the greatest common divisor of its entries is 1.

Proof. Note that any common divisor d of the 8 entries of X must also be a common divisor of the coefficients of x and y in the matrix $M_1x - N_1y$. It then follows that d is a common divisor of the coefficients of $Q_1^X(x, y)$ so $d = \pm1$ since Q_1^X is primitive.

6.2 Cube Law

We now state the main theorem of this chapter. A full proof will be given in section 6.3. In this section, we will focus on the consequences of the theorem instead.

For a binary quadratic form f, we let $\overline{f}$ denote the $SL_2(\mathbb{Z})$-equivalence class containing f. Similarly, for a cube X, we let $[X]$ denote the Γ-equivalence class containing X. The theorem is divided into two parts, as given below.

Theorem 6.2.1. Let D be an integer congruent to 0 or 1 modulo 4 and let $Q_{\mathrm{id,D}}$ be a primitive binary quadratic form of discriminant D. If there exists $X_0 \in C^{+}_{2\times2\times2}(D)$ such that

$$Q_1^{X_0} = Q_2^{X_0} = Q_3^{X_0} = Q_{\mathrm{id,D}},$$

then there exists a unique group law on the set of $SL_2(\mathbb{Z})$-equivalence classes of primitive binary quadratic forms of discriminant D satisfying

(i) $\overline{Q_{\mathrm{id,D}}}$ is the identity element.

(ii) For any cube $X \in C^{+}_{2\times2\times2}(D)$, we have $\overline{Q_1^X} + \overline{Q_2^X} + \overline{Q_3^X} = \overline{Q_{\mathrm{id,D}}}$.

Theorem 6.2.2. Let $(C^2(D), +)$ be a group, where $C^2(D)$ is the set of primitive binary quadratic forms of discriminant D. Then for any three forms $P_1, P_2, P_3 \in C^2(D)$ satisfying

$$\overline{P_1} + \overline{P_2} + \overline{P_3} = \overline{Q_{\mathrm{id,D}}},$$

there exists a unique cube $X \in C^{+}_{2\times2\times2}(D)$ up to Γ-equivalence such that

$$Q_1^X = Q_1 \text{ and } Q_2^X = Q_2 \text{ and } Q_3^X = Q_3.$$

If the cubes

$$(0,1,1,0,1,0,0,\frac{D}{4}) \text{ or } (0,1,1,1,1,1,1,\frac{D+3}{4}) \tag{6}$$

were chosen (in accordance with whether $D \equiv 0$ or $1 \pmod 4$), then we have

$$Q_{\mathrm{id,D}} = x^2 - \frac{D}{4}y^2 \text{ or } Q_{\mathrm{id,D}} = x^2 - xy + \frac{1-D}{4}y^2$$

which is precisely the identity element of the form class group.

The main consequence of Theorem 6.2.1 and 6.2.2 is that the unique group law on $C^2(D)$ induces a natural group law on the set $C^+_{2\times2\times2}(D)$ itself.

Theorem 6.2.3. Let D be an integer congruent to 0 or 1 modulo 4. Let the cube $A_{\mathrm{id,D}}$ be defined as in (6). Then there exists a unique group law on the set of Γ-equivalence classes of projective cubes of discriminant D satisfying

(i) $[A_{\mathrm{id,D}}]$ is the identity element

(ii) For any $i \in \{1,2,3\}$, the map $\chi_i : C^+_{2\times2\times2}(D) \to C^2(D)$ defined by

$$\chi_i\big([X]\big) = \overline{Q_i^A}$$

is a group homomorphism.

Proof. Let $\big(C^2(D),+\big)$ denote the unique group law on $C^2(D)$ having $\overline{Q_{\mathrm{id,D}}}$ as the identity element in Theorem 6.2.1. Since the group operation is commutative, for any $X, Y \in C^+_{2\times2\times2}(D)$, we have

$$\begin{aligned}\big(\overline{Q_1^X}+\overline{Q_1^Y}\big)+\big(\overline{Q_2^X}+\overline{Q_2^Y}\big)+\big(\overline{Q_3^X}+\overline{Q_3^Y}\big) &= \big(\overline{Q_1^X}+\overline{Q_2^X}+\overline{Q_3^X}\big)+\big(\overline{Q_1^Y}+\overline{Q_2^Y}+\overline{Q_3^Y}\big)\\ &= \overline{Q_{\mathrm{id,d}}}.\end{aligned}$$

Thus by Theorem 6.2.2, there exists up to Γ-equivalence a unique cube $Z \in C^+_{2\times2\times2}(D)$ such that

$$\overline{Q_i^Z} = \overline{Q_i^X} + \overline{Q_i^Y} \quad \text{for } i \in \{1,2,3\}. \tag{7}$$

Define the composition (denoted by $+_c$) of $[X]$ and $[Y]$ by

$$[X] +_c [Y] = [Z].$$

Then $+_c$ is well-defined due to the existence and uniqueness of the cube Z satisfying the condition (7). Associativity and commutativity of the binary operation $+_c$ follows directly from associativity and commutativity of the group operation in $\big(C^2(D),+\big)$.

Let $V \in C^+_{2\times2\times2}(D)$ be an arbitrary cube. To prove that $[A_{\mathrm{id,D}}]$ is indeed the identity element of the group, observe that for any $i \in \{1,2,3\}$ we have $\overline{Q_i^V} + \overline{Q_{\mathrm{id,D}}} = \overline{Q_i^V}$. Thus we must have

$$[V] + [A_{\mathrm{id,D}}] = [V].$$

Next, we prove that $[V]$ is invertible. Let P_1, P_2 and P_3 denote the inverses of the forms Q_1^V, Q_2^V and Q_3^V respectively. Then

$$\big(\overline{Q_1^V}+\overline{P_1}\big)+\big(\overline{Q_2^V}+\overline{P_2}\big)+\big(\overline{Q_3^V}+\overline{P_3}\big) = \overline{Q_{\mathrm{id,D}}}.$$

Since $\overline{Q_1^V} + \overline{Q_2^V} + \overline{Q_3^V} = \overline{Q_{\mathrm{id,D}}}$, we must also have $\overline{P_1} + \overline{P_2} + \overline{P_3} = \overline{Q_{\mathrm{id,D}}}$. Hence by Theorem 6.2.2, there exists a cube V' such that

$$Q_i^{V'} = P_i \text{ for each } i \in \{1, 2, 3\}.$$

Then $[V] + [V'] = [A_{\mathrm{id,D}}]$ so $[V']$ is the inverse.

Finally, we will prove the uniqueness of the group law satisfying properties (i) and (ii) of Theorem 6.2.3. If $+_g$ is another group law on $C^+_{2\times2\times2}(D)$ satisfying (i) and (ii), then for any $U, W \in C^+_{2\times2\times2}(D)$, we must have

$$[Q_i^R] = [Q_i^U] + [Q_i^W] \text{ for each } i \in \{1, 2, 3\}$$

where $[R] = [U] +_g [W]$. The uniqueness of the group law follows from the uniqueness of the equivalence class $[R]$ satisfying the above condition.

Remark 6.2.4. The proof for Theorem 6.2.3 remains valid if $A_{\mathrm{id,D}}$ is replaced with any arbitrary projective cube A of discriminant D satisfying

$$\overline{Q_1^A} = \overline{Q_2^A} = \overline{Q_3^A}.$$

The decision to fix $A_{\mathrm{id,D}}$ as the identity element was made because the group law in Theorem 6.2.3 serves as the starting point for further generalisations.

6.3 Further Generalisations

In this section, we will look at two examples on the cube law generalises to higher dimensions.

Definition 6.3.1. There is a natural bijection between the set of **binary cubic forms**, which are homogeneous polynomials of the form

$$px^3 + 3qx^2y + 3rxy^2 + sy^3 \text{ for some } p, q, r, s \in \mathbb{Z},$$

and the set of **triply-symmetric** cubes, which are cubes of the form

$$(p, q, q, r, q, r, r, s).$$

Let ι denote the map that sends a binary cubic form C to its corresponding triply-symmetric cube. The preimages of $A_{\text{id,D}}$ under ι (denoted by $C_{\text{id,D}}$) are given by

$$C_{\text{id,D}} = \begin{cases} 3x^2y + \dfrac{D}{4}y^3 & \text{if } D \equiv 0 \pmod 4 \\ 3x^2y + 3xy^2 + \dfrac{D+3}{4}y^3 & \text{if } D \equiv 1 \pmod 4. \end{cases} \tag{8}$$

Definition 6.3.2. The above bijection allows certain notions on cubes to be carried over to binary cubic forms as follows :

(i) A binary cubic form C is **projective** if the corresponding triply-symmetric cube $\iota(C)$ is projective.

(ii) Two binary cubic forms C_1 and C_2 are said to be $SL_2(\mathbb{Z})$**-equivalent** if $\iota(C_1)$ and $\iota(C_2)$ are Γ-equivalent. We let $\overline{C}$ denote the $SL_2(\mathbb{Z})$-equivalence class containing the binary cubic form C.

(iii) The **discriminant** of a binary cubic form C is the discriminant of the cube $\iota(C)$.

Remark 6.3.3. Let $C^3(D)$ denote the set of $SL_2(\mathbb{Z})$-equivalence classes of projective binary cubic forms of discriminant D. Let $\text{Sym}_3^+(D)$ denote the set of Γ-equivalence classes of projective cubes of discriminant D which contains a triply-symmetric cube. It follows from the definition that ι naturally induces a bijection from $C^3(D)$ to $\text{Sym}_3^+(D)$.

Theorem 6.3.4. Let D be an integer congruent to 0 or 1 modulo 4 and let $C_{\text{id,D}}$ be defined as in (8). There exists a unique group law on the set of $SL_2(\mathbb{Z})$-equivalence classes of projective binary cubic forms of discriminant D such that

(i) $\overline{C_{\text{id,D}}}$ is the identity element

(ii) The map $\varphi : C^3(D) \to C^+_{2\times 2\times 2}(D)$ defined by

$$\varphi\big(\overline{C}\big) = [\iota(C)].$$

is a group homomorphism.

Proof. If we can prove that $\mathrm{Sym}_3^+(D)$ is a subgroup of $C_2^+(D)$, then the existence and uniqueness of the group law follows immediately. This is because the bijection ι and the group structure on $\mathrm{Sym}_3^+(D)$ naturally induces a group structure on $C^3(D)$. By condition (ii), the group structure on $C^3(D)$ is in fact completely determined by the group structure on $\mathrm{Sym}_3^+(D)$. First we prove a lemma.

Lemma 6.3.5. Let $X \in C_{2\times 2\times 2}$ be a cube of non-zero discriminant. Then X is triply-symmetric if and only if $Q_1^X = Q_2^X = Q_3^X$.

Proof. If X is triply-symmetric, then a direct computation shows that

$$Q_1^X = Q_2^X = Q_3^X = (q^2 - pr)x^2 + (ps - qr)xy + (r^2 - qs)y^2.$$

On the other hand, suppose that we have

$$Q_1^X = Q_2^X = Q_3^X = Ax^2 + Bxy + Cy^2$$

for some $A, B, C \in \mathbb{Z}$. By using the explicit formulas given in Definition 6.1.2, we can obtain 6 equations in a, b, c, d, e, f, g, h. Solving for c, e, f, g in terms of a, b, d, h, we get two set of solutions :

$$c = b,\ e = b,\ f = d,\ g = d \ \text{ or } \ c = \frac{ad}{b},\ e = \frac{ah}{d},\ f = \frac{bh}{d},\ g = \frac{ah}{b}.$$

The latter case forces $\mathrm{disc}(X) = 0$. Thus we must have the former case which completes the proof of the lemma.

If $D = 0$, then $C_2^+(D)$ is trivial so $\mathrm{Sym}_3^+(D) = C_2^+(D)$ and we are done. Thus we assume $D \neq 0$.

Let $[X], [Y] \in \mathrm{Sym}_3^+(D)$. We have $[X] + [Y]^{-1} = [Z]$ for some $Z \in C_2^+(D)$. By the lemma, we have

$$[Q_1^X] = [Q_2^X] = [Q_3^X] \ \text{ and } \ [Q_1^Y] = [Q_2^Y] = [Q_3^Y].$$

It then follows that

$$[Q_1^Z] = [Q_2^Z] = [Q_3^Z].$$

Thus Z is Γ-equivalent to a cube Z' such that

$$Q_1^{Z'} = Q_2^{Z'} = Q_3^{Z'}.$$

By Proposition 6.3.4 again, we have that $[Z] \in \mathrm{Sym}_3^+(D)$ which completes the proof.

A completely analogous generalisation can be made by applying the same technique to doubly-symmetric cubes.

Definition 6.3.6. There is a natural bijection between the set of **pairs of classically integral binary quadratic forms**, which are of the form

$$(ax^2 + 2bxy + cy^2,\ dx^2 + 2exy + fy^2) \text{ for some } a, b, c, d, e, f \in \mathbb{Z},$$

and the set of **doubly-symmetric** cubes, which are cubes of the form

$$(a, b, b, c, d, e, e, f). \tag{9}$$

Let π denote the map that sends a pair of classically integral binary quadratic form to its corresponding doubly-symmetric cube. The preimages of $A_{\mathrm{id,D}}$ under π (denoted by $B_{\mathrm{id,D}}$ are given by

$$B_{\mathrm{id,D}} = \begin{cases} \left(2xy,\ x^2 + \dfrac{D}{4}\right) & \text{if } D \equiv 0 \pmod 4 \\ \left(2xy + y^2,\ x^2 + 2xy + \dfrac{D+3}{4}y^2\right) & \text{if } D \equiv 1 \pmod 4. \end{cases}$$

Remark 6.3.7. Notions of **projectivity**, $SL_2(\mathbb{Z})$**-equivalence** and **discriminant** are defined in a analogous manner to Definition 6.3.2. Let $C^{2\times 2}(D)$ denote the set of $SL_2(\mathbb{Z})$-equivalence classes of projective pairs of classically integral binary quadratic forms of discriminant D. Let $\mathrm{Sym}_2^+(D)$ denote the set of Γ-equivalence classes of projective cubes of discriminant D which contains a doubly-symmetric cube. Then we have an analogous theorem to Theorem 6.3.4.

Theorem 6.3.8. Let D be an integer congruent to 0 or 1 modulo 4 and let $B_{\mathrm{id,D}}$ be defined as in (9). There exists a unique group law on the set of $SL_2(\mathbb{Z})$-equivalence classes of projective pairs of classically integral binary quadratic forms of discriminant D such that

(i) $\overline{B_{\mathrm{id,D}}}$ is the identity element

(ii) The map $\varphi : C^{2\times 2}(D) \to \mathrm{Sym}_2^+(D)$ defined by

$$\varphi(\overline{C}) = [\pi(C)].$$

is a group homomorphism.

Proof. With the exception of the lemma stated below, the rest of the proof is exactly the same as in the case of binary cubic forms. Thus we will only prove the lemma.

Lemma 6.3.9. Let $X \in C_{2\times 2\times 2}$. Then X is doubly-symmetric if and only if $Q_2^X = Q_3^X$.

Proof. If X is doubly-symmetric, then a direct computation shows that

$$Q_2^X = Q_3^X = (bd - ae)x^2 + (af - cd)xy + (ce - bf)y^2.$$

On the other hand, suppose that we have

$$Q_2^X = Q_3^X = Ax^2 + Bxy + Cy^2$$

for some $A, B, C \in \mathbb{Z}$. Then again by using explicit formulas given in Definition 6.1.2, we obtain 3 equations in a, b, c, d, e, f, g, h. Solving for c and g in terms of a, b, d, e, f, h, we get

$$c = b \text{ and } g = f$$

which completes the proof.

6.4 Isomorphism between Cubes and Ideals in Quadratic Rings

In this section, we will prove Theorem 6.2.1 using the concept of quadratic rings in chapter 5. Let D be an integer congruent to 0 or 1 modulo 4 and let $S(D)$ be the unique quadratic ring of discriminant D. Recall that K is defined to be the tensor product $S(D) \otimes_{\mathbb{Z}} \mathbb{Q}$.

Definition 6.4.1. A triple (I_1, I_2, I_3) of oriented fractional ideals of S is **balanced** if it satisfies both properties :

(i) $I_1 I_2 I_3 \subseteq S$.

(ii) $N^{S(D)}(I_1)N^{S(D)}(I_2)N^{S(D)}(I_3) = 1$.

Definition 6.4.2. Two balanced triples (I_1, I_2, I_3) and (J_1, J_2, J_3) are **equivalent** if there exists $k_1, k_2, k_3 \in K$ such that $I_1 = k_1 J_1$, $I_2 = k_2 J_2$ and $I_3 = k_3 J_3$.

By the multiplicativity of ideal norm for principal ideals (Theorem 5.2.15), the above definition forces $N^{S(D)}(k_1 k_2 k_3) = 1$.

Theorem 6.4.3. There is a bijection between the set of non-degenerate Γ-equivalence classes of cubes and the set of equivalence classes of pairs $(S(D), (I_1, I_2, I_3))$ where $S(D)$ is a non-degenerate oriented quadratic ring and (I_1, I_2, I_3) is an equivalence class of balanced triples of oriented ideals of S. Under this bijection, the discriminant of the cube equals the discriminant of the corresponding quadratic ring.

Proof. Given a pair $(S(D), (I_1, I_2, I_3))$, we first show how to construct a corresponding cube $2 \times 2 \times 2$ cube. Let $\{1, \tau\}$ be the positively oriented regular basis for $S(D)$. Let $\langle \alpha_1, \alpha_2 \rangle$, $\langle \beta_1, \beta_2 \rangle$ and $\langle \gamma_1, \gamma_2 \rangle$ be $\mathbb{Z}$-bases for I_1, I_2 and I_3 respectively, where for each $i \in \{1, 2, 3\}$, the basis is positively oriented if I_i is positively oriented, and negatively oriented otherwise. We have $I_1 I_2 I_3 \subseteq S(D)$. Thus for all $1 \leq i, j, k \leq 2$, we may write

$$\alpha_i \beta_j \gamma_k = c_{ijk} + a_{ijk}\tau \quad \text{with } c_{ijk}, a_{ijk} \in \mathbb{Z}. \tag{10}$$

Define the cube $X \in C_{2\times 2\times 2}$ by

$$(a_{111}, a_{121}, a_{112}, a_{122}, a_{211}, a_{221}, a_{212}, a_{222}). \tag{11}$$

If $\langle \alpha'_1, \alpha'_2 \rangle$, $\langle \beta'_1, \beta'_2 \rangle$ and $\langle \gamma'_1, \gamma'_2 \rangle$ is another set of similarly-oriented $\mathbb{Z}$-bases for I_1, I_2 and I_3, then the change-of-basis matrices $M_1, M_2, M_3 \in GL_2(\mathbb{Z})$ must have determinant 1 since orientation is preserved. Thus $(M_1, M_2, M_3) \in \Gamma$. A direct computation shows that the new cube X' obtained via (11) can simply be obtained from the original cube X via the action of (M_1, M_2, M_3).

On the other hand, if (I_1, I_2, I_3) is replaced by an equivalent triple (k_1I_1, k_2I_2, k_3I_3) for some $k_1, k_2, k_3 \in K$, then observe that $\{k_1\alpha_1, k_1\alpha_2\}$, $\{k_2\beta_1, k_2\beta_2\}$ and $\{k_3\gamma_1, k_3\gamma_2\}$ are the new oriented $\mathbb{Z}$-bases. The equation in (10) becomes

$$(k_1k_2k_3)\alpha_i\beta_j\gamma_k = c'_{ijk} + a'_{ijk}\tau \text{ with } c'_{ijk}, a'_{ijk} \in \mathbb{Z}.$$

This means that the corresponding change on the cube X when (I_1, I_2, I_3) is replaced by (k_1I_1, k_2I_2, k_3I_3) is the same as if (I_1, I_2, I_3) is replaced by $(I_1, I_2, k_1k_2k_3I_3)$ instead. The determinant of the change-of-basis matrix M from $\{\gamma_1, \gamma_2\}$ to $\{k_1k_2k_3\gamma_1, k_1k_2k_3\gamma_2\}$ is precisely the norm of $k_1k_2k_3$, which is 1. Thus the cube X is transformed by the action of $(I_{2\times2}, I_{2\times2}, M) \in \Gamma$.

Thus the above construction produces a well-defined map from the set of equivalence classes of pairs $(S(D), (I_1, I_2, I_3))$ to the set of Γ-equivalence classes of cubes.

To show that the map is a bijection, we will show that given a cube X, there is exactly one pair $(S(D), (I_1, I_2, I_3))$ up to equivalence that produces the element X via the above map.

Let

$$X = (a_{1,1,1}, a_{1,2,1}, a_{1,1,2}, a_{1,2,2}, a_{2,1,1}, a_{2,2,1}, a_{2,1,2}, a_{2,2,2})$$

be an arbitrary non-degenerate cube. We first show that the oriented quadratic ring $S(D)$ is completely determined by X. By Theorem 5.1.11, it suffices to show that the discriminant of the oriented quadratic ring is completely determined by X. We will need the following lemma.

Lemma 6.4.4. The cube X obtained from $(S(D), (I_1, I_2, I_3))$ via equation (10) satisfies

$$\mathrm{disc}(X) = N(I_1)^2N(I_2)^2N(I_3)^2\mathrm{disc}(S).$$

Proof. When $I_1 = I_2 = I_3 = S(D)$. We have $\alpha_1 = \beta_1 = \gamma_1 = 1$ and $\alpha_2 = \beta_2 = \gamma_2 = \tau$. Then the resulting cube X is simply $A_{\mathrm{id,D}}$ so we have $\mathrm{disc}(X) = D = \mathrm{disc}(S(D))$ as desired.

Now suppose that I_1 is a general oriented fractional ideal of $S(D)$ with $\mathbb{Z}$-basis $\langle\alpha_1, \beta_1\rangle$. Let $M \in GL_2(\mathbb{Q})$ be the corresponding change-of-basis matrix from $\langle 1, \tau\rangle$ to $\langle\alpha_1, \beta_1\rangle$. The corresponding cube X is transformed by the action of $(M, I_{2\times2}, I_{2\times2})$. The quadratic form Q_2^X (or Q_3^X) is multiplied by a factor of $\det(M)$. By Proposition 5.2.8, we have

$$\det(M) = N^{S(D)}(I_1).$$

Thus the discriminant of X is multiplied by a factor of $N(I_1)^2$. Since the same argument applies for I_2 and I_3, we have proved that the equality holds for arbitrary oriented fractional ideals I_1, I_2, I_3.

The lemma, together with the additional restriction that $N(I_1)N(I_2)N(I_3) = 1$, gives

$$\operatorname{disc}(X) = \operatorname{disc}(S)$$

so the ring S is determined by X.

Next, since multiplication in the ring $S(D)$ is associative and commutative, we have

$$[\alpha_i\beta_j\gamma_k]\cdot[\alpha_{i'}\beta_{j'}\gamma_{k'}] = [\alpha_{i'}\beta_j\gamma_k]\cdot[\alpha_i\beta_{j'}\gamma_{k'}] = [\alpha_i\beta_{j'}\gamma_k]\cdot[\alpha_{i'}\beta_j\gamma_{k'}] = [\alpha_i\beta_j\gamma_{k'}]\cdot[\alpha_{i'}\beta_{j'}\gamma_k] \quad (12)$$

for $1 \leq i, i', j', k, k' \leq 2$. Equating these identities using (10), we get a system of 18 equations in the eight variables $c_{i,j,k}$ in terms of the $a_{i,j,k}$. This system of equations has a unique integral solution given by

$$\begin{aligned} c_{ijk} = {} & (i'-i)(j'-j)(k'-k) \\ & \cdot \Big[a_{i'jk}a_{ij'k}a_{ijk'} + \frac{1}{2}a_{ijk}\big(a_{ijk}a_{i'j'k'} - a_{i'jk}a_{ij'k'} - a_{ij'k}a_{i'jk'} - a_{ijk'}a_{i'j'k}\big)\Big] \\ & - \frac{1}{2}a_{ijk}\epsilon \end{aligned}$$

for all i, i', j, j', k, k' satisfying $\{i, i'\} = \{j, j'\} = \{k, k'\} = \{1, 2\}$ and $\epsilon = 0$ or 1 depending on whether $D \equiv 0$ or 1 (mod 4). An algorithm for solving the system is given in Appendix 7.2. Thus we conclude that the c_{ijk} in (10) are also completely determined by X.

Next, we prove that the pairs $\{\alpha_1, \alpha_2\}$, $\{\beta_1, \beta_2\}$ and $\{\gamma_1, \gamma_2\}$ are uniquely determined up to a invertible scaling factor in K. This is equivalent to proving that α_1/α_2, β_1/β_2 and γ_1/γ_2 are uniquely determined. The fact that α_1/α_2 is uniquely determined follows directly from

$$\begin{aligned} \alpha_1\beta_1\gamma_1(c_{211} + a_{211}\tau) &= \alpha_2\beta_1\gamma_1(c_{111} + a_{111}\tau) \\ \implies \frac{\alpha_1}{\alpha_2} &= \frac{c_{111} + a_{111}\tau}{c_{211} + a_{211}\tau} \end{aligned}$$

and the fact that the c_{ijk} are completely determined. Similar arguments apply to β_1/β_2 and γ_1/γ_2. With the restriction that $N(I_1)N(I_2)N(I_3) = 1$, the pair $\{\gamma_1, \gamma_2\}$ is completed determined once a choice of $\{\alpha_1, \alpha_2\}$ and $\{\beta_1, \beta_2\}$ has been made. Thus the triple (I_1, I_2, I_3) is completed determined up to equivalence.

Finally, we will show that $I_1 = \langle\alpha_1, \alpha_2\rangle$, $I_2 = \langle\beta_1, \beta_2\rangle$ and $I_3 = \langle\gamma_1, \gamma_2\rangle$ indeed form ideals of $S(D)$. Let Q_1^X, Q_2^X and Q_3^X be the three binary quadratic forms associated to X and write $Q_i^X = p_ix^2 + q_ixy + r_iy^2$ for $i \in \{1, 2, 3\}$. Then from Definition 6.1.2, the coefficients of Q_i^X can be written explicitly in terms of the coefficients of the 8 vertices of X. Since c_{ijk} can also be written explictly in terms of the a_{ijk}, we can perform an explicit computation in terms of the 8 variables a_{ijk}. This gives

$$\begin{aligned} \tau(c_{1,1,1} + a_{1,1,1}\tau) &= \frac{q_1 + \epsilon}{2}(c_{1,1,1} + a_{1,1,1}\tau) + p_1(c_{2,1,1} + a_{2,1,1}\tau) \\ -\tau(c_{2,1,1} + a_{2,1,1}\tau) &= r_1(c_{1,1,1} + a_{1,1,1}\tau) + \frac{q_1 - \epsilon}{2}(c_{2,1,1} + a_{2,1,1}\tau) \end{aligned}$$

which reduces to

$$\tau \cdot \alpha_1 = \frac{q_1 + \epsilon}{2} \cdot \alpha_1 + p_1 \cdot \alpha_2 \tag{13}$$

$$-\tau \cdot \alpha_2 = r_1 \cdot \alpha_1 + \frac{q_1 - \epsilon}{2} \cdot \alpha_2. \tag{14}$$

Analogous equations for $I_2 = \langle \beta_1, \beta_2 \rangle$ and $I_3 = \langle \gamma_1, \gamma_2 \rangle$ can be obtained by a similar computation. Regardless of whether $D \equiv 0$ or 1 (mod 4), note that $(q_1 + \epsilon)/2$ is always an integer so we conclude that I_1, I_2 and I_3 are indeed ideals of S.

Before we can state the second part of the main theorem, we need the following theorem.

Definition 6.4.5. A balanced triple (I_1, I_2, I_3) of ideals of $S(D)$ is **projective** if I_1, I_2 and I_3 are projective ideals.

Theorem 6.4.6. Let I be an oriented fractional ideal of a nondegenerate oriented quadratic ring $S(D)$. Then I is invertible if and only if I is projective.

Proof. Suppose that I is invertible. Since $II^{-1} = S(D)$, there exists $a_1, \cdots, a_n \in I$ and $b_1 \cdots, b_n \in I^{-1}$ such that $a_1 b_1 + \cdots + a_n b_n = 1_{S(D)}$. Then for any $x \in I$, we have

$$(xb_1)a_1 + \cdots + (xb_n)a_n = x.$$

Note that $xb_i \in S(D)$ for all i. Thus the set $\{a_1, \cdots, a_n\}$ generates I. Let F be the free $S(D)$-module of rank n, with basis $\{e_1, \cdots, e_n\}$. Define the surjective $S(D)$-linear map $\varphi : F \to I$ by

$$\varphi(e_i) = a_i.$$

Then define $\psi : I \to F$ by

$$\psi(x) = \sum_{i=1}^{n} (xb_i) \cdot e_i.$$

Then for any $x \in I$,

$$\varphi \circ \psi(x) = \varphi\left(\sum_{i=1}^{n} (xb_i) \cdot e_i \right) = \sum_{i=1}^{n} (xb_i) a_i = x.$$

so φ splits. Thus I is isomorphic to a direct summand of the free module F so it is projective.

Now suppose that I is projective. To prove that I is invertible, we will first need a few lemmas

Lemma 6.4.7. We have

$$I \otimes_{S(D)} K \cong S(D) \otimes_{S(D)} K \cong K$$

as K-modules. Furthermore, the inclusion map $\iota : I \otimes_{S(D)} K \to S(D) \otimes_{S(D)} K$ is a K-module isomorphism.

Proof. To prove that $S(D) \otimes_{S(D)} K \cong K$ as K-modules, observe that the following map $\psi : S(D) \otimes_{S(D)} K \to K$ defined by

$$\psi((s,k)) = s \cdot k$$

is a surjective K-module homomorphism. To show that ψ is injective, let $(s,k) \in \ker(\psi)$. We have

$$(s,k) = (1_{S(D)}, s \cdot k) = (1_{S(D)}, 0_K)$$

so ψ is indeed injective.

Now consider the short exact sequence

$$0 \longrightarrow I \longrightarrow S(D) \longrightarrow S(D)/I \longrightarrow 0.$$

Since $K = S(D) \otimes_{\mathbb{Z}} \mathbb{Q}$ is a localisation of $S(D)$, it is flat as an $S(D)$-module. Thus we get the following short exact sequence

$$0 \longrightarrow I \otimes_{S(D)} K \longrightarrow S(D) \otimes_{S(D)} K \longrightarrow S(D)/J \otimes_{S(D)} K \longrightarrow 0.$$

But $|S(D)/I| = |N^{S(D)}(I)|$ is finite. Let $n = |S(D)/I|$. Then observe that for any $(s', (s,q)) \in S(D)/I \otimes_{S(D)} K$, we have

$$\big(s', (s,q)\big) = \big(s', (ns, q/n)\big) = \big(ns', (s, q/n)\big) = \big(0_{S/I}, (s, q/n)\big).$$

Thus $S(D)/J \otimes_{S(D)} K$ is trivial so the inclusion map $\iota : I \otimes_{S(D)} K \to S(D) \otimes_{S(D)} K$ is an isomorphism.

Lemma 6.4.8. Every $S(D)$-linear map from I to $S(D)$ is of the form

$$x \mapsto \alpha x$$

for some $\alpha \in K$.

Proof. Let $f : I \to S(D)$ be a $S(D)$-module homomorphism. Then we have that $f \otimes_{S(D)} \mathrm{id} : I \otimes_{S(D)} K \to S(D) \otimes_{S(D)} K$ is a K-module homomorphism. By the previous lemma, we know that there exist K-module isomorphisms $\varphi_1 : K \to I \otimes_{S(D)} K$ and $\varphi_2 : S(D) \otimes_{S(D)} K \to K$. Let $g = f \otimes_{S(D)} \mathrm{id}$. Then the map $\varphi_2 \circ g \circ \varphi_1$ is a K-module homomorphism from K to itself.

Let $b = (\varphi_2 \circ g \circ \varphi_1)(1_K)$. Then for any $k \in K$, we have

$$(\varphi_2 \circ g \circ \varphi_1)(k) = k \cdot (\varphi_2 \circ g \circ \varphi_1)(1_K) = kb.$$

Then for any $i \in I \otimes_{S(D)} K$, we have that

$$\begin{aligned} g(i) &= \big(\varphi_2^{-1} \circ \varphi_2 \circ g \circ \varphi_1\big)\big(\varphi_1(i)\big) \\ &= \varphi_2^{-1}\big(b \cdot \varphi_1(i)\big) \\ &= \varphi_2^{-1}(b) \cdot (\varphi_2^{-1} \circ \varphi_1)(i) \\ &= b \cdot i. \end{aligned}$$

7 Appendix

7.1 Multiplication of Ideals

Theorem 7.1.1. Let D be an integer congruent to 0 or 1 modulo 4. Let $f = [A, B, CA']$ and $g = [A', B, CA]$ be two primitive binary quadratic forms of discriminant D. Let $I = \langle A, b_B + \tau\rangle$ and $J = \langle A', b_B + \tau\rangle$ be two ideals of $S(D)$, where τ satisfies $\tau^2 - D/4 = 0$ or $\tau^2 - \tau + (1 - D)/4 = 0$ depending on whether $D \equiv 0$ or 1 (mod 4). Then

$$IJ = \big\langle AA', b_B + \tau\big\rangle.$$

Proof. Let $\{x, y + z\tau\}$ be the standard basis for IJ. It suffices to prove that $x = |AA'|$, $z = 1$ and $y \equiv b_B \pmod{|AA'|}$.

To prove that $x = |AA'|$, we will prove that any integer in IJ is divisible by AA'. Let w be an integer in IJ. Then there exists $x_1, x_2, y_1, y_2 \in \mathbb{Z}$ such that

$$\begin{aligned}w &= [Ax_1 + (b_B + \tau)y_1][A'x_2 + (b_B + \tau)y_2]\\ &= AA'x_1x_2 + (b_B + \tau)(Ax_1y_2 + A'x_2y_1) + (b_B^2 + 2b_B\tau + \tau^2)y_1y_2\\ &= AA'x_1x_2 + b_BAx_1y_2 + b_BA'x_2y_1 + b_B^2y_1y_2 + \tau^2y_1y_2\\ &+ \tau(Ax_1y_2 + A'x_2y_1 + 2b_By_1y_2).\end{aligned}$$

If $D \equiv 0 \pmod 4$, then

$$\begin{aligned}w &= AA'x_1x_2 + b_BAx_1y_2 + b_BA'x_2y_1 + b_B^2y_1y_2 + \frac{Dy_1y_2}{4}\\ &+ \tau(Ax_1y_2 + A'x_2y_1 + 2b_By_1y_2).\end{aligned}$$

and so $Ax_1y_2 + A'x_2y_1 + 2b_By_1y_2 = 0$. We have

$$\begin{aligned}w &= AA'x_1x_2 + b_B(Ax_1y_2 + A'x_2y_1 + b_By_1y_2) + \frac{Dy_1y_2}{4}\\ &= AA'x_1x_2 - b_B^2y_1y_2 + \frac{Dy_1y_2}{4}\\ &= AA'x_1x_2 - y_1y_2\left(\frac{B^2 - D}{4}\right).\end{aligned}$$

If $D \equiv 1 \pmod 4$, then

$$\begin{aligned}w &= AA'x_1x_2 + b_BAx_1y_2 + b_BA'x_2y_1 + b_B^2y_1y_2 + \frac{(D-1)y_1y_2}{4}\\ &+ \tau(Ax_1y_2 + A'x_2y_1 + 2b_By_1y_2 + y_1y_2).\end{aligned}$$

so $Ax_1y_2 + A'x_2y_1 + 2b_By_1y_2 + y_1y_2 = 0$. We have

$$\begin{aligned} w &= AA'x_1x_2 + b_B(Ax_1y_2 + A'x_2y_1 + b_By_1y_2) + \frac{(D-1)y_1y_2}{4} \\ &= AA'x_1x_2 - b_B^2y_1y_2 - b_By_1y_2 + \frac{(D-1)y_1y_2}{4} \\ &= AA'x_1x_2 - y_1y_2\bigg(\Big(b_B + \frac{1}{2}\Big)^2 - \frac{D}{4}\bigg) \\ &= AA'x_1x_2 - y_1y_2\bigg(\frac{B^2-D}{4}\bigg). \end{aligned}$$

In both cases, $w = AA'x_1x_2 - y_1y_2AA'C$ which is divisible by AA'.

Next, observe that any element in IJ can be written as a $\mathbb{Z}$-linear combination of the 4 elements

$$\left\{AA' \ , \ \frac{AB}{2} + A\tau \ , \ \frac{A'B}{2} + A'\tau \ , \ \frac{B^2}{4} + \frac{D}{4} + B\tau\right\}$$

if $D \equiv 0 \pmod 4$ or

$$\left\{AA', \ \frac{A(B-1)}{2} + A\tau \ , \ \frac{A'(B-1)}{2} + A'\tau \ , \ \left(\frac{B-1}{2}\right)^2 + \frac{D-1}{4} + B\tau\right\}$$

if $D \equiv 1 \pmod 4$. Since $\gcd(A, A', B) = 1$, there exists $x \in \mathbb{Z}$ such that $x + \tau \in IJ$. Thus we must have $z = 1$.

Finally, we prove that $b_B \equiv y \pmod{|AA'|}$. Similar to the argument for proving that $x = |AA'|$, first observe that there exists $u_1, u_2, v_1, v_2 \in \mathbb{Z}$ such that

$$\begin{aligned} y + \tau = {} & AA'x_1x_2 + b_BAx_1y_2 + b_BA'x_2y_1 + b_B^2y_1y_2 + \tau^2y_1y_2 \\ & + \tau(Ax_1y_2 + A'x_2y_1 + 2b_By_1y_2) \end{aligned}$$

If $D \equiv 0 \pmod 4$, then $Ax_1y_2 + A'x_2y_1 + 2b_By_1y_2 = 1$ and we have

$$\begin{aligned} y &= AA'x_1x_2 + b_B(Ax_1y_2 + A'x_2y_1 + b_By_1y_2) + \frac{Dy_1y_2}{4} \\ &= AA'x_1x_2 + b_B - b_B^2y_1y_2 + \frac{Dy_1y_2}{4} \\ &= AA'x_1x_2 + b_B - y_1y_2\bigg(\frac{B^2-D}{4}\bigg). \end{aligned}$$

If $D \equiv 1 \pmod 4$, then $Ax_1y_2 + A'x_2y_1 + 2b_By_1y_2 + y_1y_2 = 1$.

$$\begin{aligned} y &= AA'x_1x_2 + b_B(Ax_1y_2 + A'x_2y_1 + b_By_1y_2) + \frac{(D-1)y_1y_2}{4} \\ &= AA'x_1x_2 + b_B - b_B^2y_1y_2 - b_By_1y_2 + \frac{(D-1)y_1y_2}{4} \\ &= AA'x_1x_2 + b_B - y_1y_2\bigg(\frac{B^2-D}{4}\bigg). \end{aligned}$$

In both cases, $y - b_B = AA'x_1x_2 - y_1y_2AA'C$ which is divisible by AA'.

7.2 Solving the system of 18 equations

From (6.3.4), we get 9 equations

$$\begin{aligned}
(c_{1,1,1}+a_{1,1,1}\tau)(c_{2,2,2}+a_{2,2,2}\tau) &= (c_{2,1,1}+a_{2,1,1}\tau)(c_{1,2,2}+a_{1,2,2}\tau)\\
(c_{1,1,1}+a_{1,1,1}\tau)(c_{2,2,2}+a_{2,2,2}\tau) &= (c_{1,2,1}+a_{1,2,1}\tau)(c_{2,1,2}+a_{2,1,2}\tau)\\
(c_{1,1,1}+a_{1,1,1}\tau)(c_{2,2,2}+a_{2,2,2}\tau) &= (c_{1,1,2}+a_{1,1,2}\tau)(c_{2,2,1}+a_{2,2,1}\tau)\\
(c_{1,1,1}+a_{1,1,1}\tau)(c_{1,2,2}+a_{1,2,2}\tau) &= (c_{1,2,1}+a_{1,2,1}\tau)(c_{1,1,2}+a_{1,1,2}\tau)\\
(c_{2,1,1}+a_{2,1,1}\tau)(c_{2,2,2}+a_{2,2,2}\tau) &= (c_{2,2,1}+a_{2,2,1}\tau)(c_{2,1,2}+a_{2,1,2}\tau)\\
(c_{1,1,1}+a_{1,1,1}\tau)(c_{2,1,2}+a_{2,1,2}\tau) &= (c_{2,1,1}+a_{2,1,1}\tau)(c_{1,1,2}+a_{1,1,2}\tau)\\
(c_{1,2,1}+a_{1,2,1}\tau)(c_{2,2,2}+a_{2,2,2}\tau) &= (c_{2,2,1}+a_{2,2,1}\tau)(c_{1,2,2}+a_{1,2,2}\tau)\\
(c_{1,1,1}+a_{1,1,1}\tau)(c_{2,2,1}+a_{2,2,1}\tau) &= (c_{2,1,1}+a_{2,1,1}\tau)(c_{1,2,1}+a_{1,2,1}\tau)\\
(c_{1,1,2}+a_{1,1,2}\tau)(c_{2,2,2}+a_{2,2,2}\tau) &= (c_{2,1,2}+a_{2,1,2}\tau)(c_{1,2,2}+a_{1,2,2}\tau).
\end{aligned}$$

Next, we compare the coefficients of 1 and τ. If $D \equiv 0 \pmod 4$, then $\tau^2 = \frac{D}{4}$ and so

$$0c_{1,1,1}c_{2,2,2}+\frac{D}{4}(a_{1,1,1}a_{2,2,2}) = c_{2,1,1}c_{1,2,2}+\frac{D}{4}(a_{2,1,1}a_{1,2,2}) \tag{15}$$

$$c_{1,1,1}a_{2,2,2}+c_{2,2,2}a_{1,1,1} = c_{2,1,1}a_{1,2,2}+c_{1,2,2}a_{2,1,1} \tag{16}$$

$$c_{1,1,1}c_{2,2,2}+\frac{D}{4}(a_{1,1,1}a_{2,2,2}) = c_{1,2,1}c_{2,1,2}+\frac{D}{4}(a_{1,2,1}a_{2,1,2}) \tag{17}$$

$$c_{1,1,1}a_{2,2,2}+c_{2,2,2}a_{1,1,1} = c_{1,2,1}a_{2,1,2}+c_{2,1,2}a_{1,2,1} \tag{18}$$

$$c_{1,1,1}c_{2,2,2}+\frac{D}{4}(a_{1,1,1}a_{2,2,2}) = c_{1,1,2}c_{2,2,1}+\frac{D}{4}(a_{1,1,2}a_{2,2,1}) \tag{19}$$

$$c_{1,1,1}a_{2,2,2}+c_{2,2,2}a_{1,1,1} = c_{1,1,2}a_{2,2,1}+c_{2,2,1}a_{1,1,2} \tag{20}$$

$$c_{1,1,1}c_{1,2,2}+\frac{D}{4}(a_{1,1,1}a_{1,2,2}) = c_{1,2,1}c_{1,1,2}+\frac{D}{4}(a_{1,2,1}a_{1,1,2}) \tag{21}$$

$$c_{1,1,1}a_{1,2,2}+c_{1,2,2}a_{1,1,1} = c_{1,2,1}a_{1,1,2}+c_{1,1,2}a_{1,2,1} \tag{22}$$

$$c_{2,1,1}c_{2,2,2}+\frac{D}{4}(a_{2,1,1}a_{2,2,2}) = c_{2,2,}c_{2,1,2}+\frac{D}{4}(a_{2,2,1}a_{2,1,2}) \tag{23}$$

$$c_{2,1,1}a_{2,2,2}+c_{2,2,2}a_{2,1,1} = c_{2,2,1}a_{2,1,2}+c_{2,1,2}a_{2,2,1} \tag{24}$$

$$c_{1,1,1}c_{2,1,2}+\frac{D}{4}(a_{1,1,1}a_{2,1,2}) = c_{2,1,1}c_{1,1,2}+\frac{D}{4}(a_{2,1,1}a_{1,1,2}) \tag{25}$$

$$c_{1,1,1}a_{2,1,2}+c_{2,1,2}a_{1,1,1} = c_{2,1,1}a_{1,1,2}+c_{1,1,2}a_{2,1,1} \tag{26}$$

$$c_{1,2,1}c_{2,2,2}+\frac{D}{4}(a_{1,2,1}a_{2,2,2}) = c_{2,2,1}c_{1,2,2}+\frac{D}{4}(a_{2,2,1}a_{1,2,2}) \tag{27}$$

$$c_{1,2,1}a_{2,2,2}+c_{2,2,2}a_{1,2,1} = c_{2,2,1}a_{1,2,2}+c_{1,2,2}a_{2,2,1} \tag{28}$$

$$c_{1,1,1}c_{2,2,1} + \frac{D}{4}(a_{1,1,1}a_{2,2,1}) = c_{2,1,1}c_{1,2,1} + \frac{D}{4}(a_{2,1,1}a_{1,2,1}) \tag{29}$$

$$c_{1,1,1}a_{2,2,1} + c_{2,2,1}a_{1,1,1} = c_{2,1,1}a_{1,2,1} + c_{1,2,1}a_{2,1,1} \tag{30}$$

$$c_{1,1,2}c_{2,2,2} + \frac{D}{4}(a_{1,1,2}a_{2,2,2}) = c_{2,1,2}c_{1,2,2} + \frac{D}{4}(a_{2,1,2}a_{1,2,2}) \tag{31}$$

$$c_{1,1,2}a_{2,2,2} + c_{2,2,2}a_{1,1,2} = c_{2,1,2}a_{1,2,2} + c_{1,2,2}a_{2,1,2} \tag{32}$$

$$a'h' - e'd' = \frac{D}{4}(ed - ah) \tag{33}$$

$$a'h - d'e - e'd + h'a = 0 \tag{34}$$

$$a'h' - b'g' = \frac{D}{4}(bg - ah) \tag{35}$$

$$a'h - b'g - g'b + h'a = 0 \tag{36}$$

$$a'h' - c'f' = \frac{D}{4}(cf - ah) \tag{37}$$

$$a'h - c'f - f'c + h'a = 0 \tag{38}$$

$$a'd' - b'c' = \frac{D}{4}(bc - ad) \tag{39}$$

$$a'd - b'c - c'b + d'a = 0 \tag{40}$$

$$e'h' - f'g' = \frac{D}{4}(fg - eh) \tag{41}$$

$$e'h - f'g - g'f + h'e = 0 \tag{42}$$

$$a'g' - c'e' = \frac{D}{4}(ce - ag) \tag{43}$$

$$a'g - c'e - e'c + g'a = 0 \tag{44}$$

$$b'h' - d'f' = \frac{D}{4}(df - bh) \tag{45}$$

$$b'h - d'f - f'd + h'b = 0 \tag{46}$$

$$a'f' - b'e' = \frac{D}{4}(be - af) \tag{47}$$

$$a'f - b'e - e'b + f'a = 0 \tag{48}$$

$$c'h' - d'g' = \frac{D}{4}(dg - ch) \tag{49}$$

$$c'h - d'g - g'd + h'c = 0 \tag{50}$$

where a, b, c, d, e, f, g, h are fixed constants and $a', b', c', d', e', f', g', h'$ are to be solved for, with

$$\begin{aligned} D = {} & a^2h^2 + b^2g^2 + c^2f^2 + d^2e^2 \\ & - 2(abgh + cdef + acfh + bdeg + aedh + bfcg) + 4(adfg + bceh) \end{aligned}$$

Inquiry : Is there a proper way to solve such a system of polynomial equations? (It is too big to solve naively using MATLAB)

Working steps

To ensure that $SL_2(\mathbb{Z}) \times SL_2(\mathbb{Z}) \times SL_2(\mathbb{Z})$ acts on the triple of ideals (I_1, I_2, I_3) and the triple of binary quadratic forms (Q_1, Q_2, Q_3) in the same way, we must have the bijection :

$$\begin{aligned}
a &= a_{1,1,1}\\
b &= a_{1,2,1}\\
c &= a_{1,1,2}\\
d &= a_{1,2,2}\\
e &= a_{2,1,1}\\
f &= a_{2,2,1}\\
g &= a_{2,1,2}\\
h &= a_{2,2,2}
\end{aligned}$$

Using (18), and comparing the coefficients of 1 and τ $\left(\text{where } \tau^2 - \frac{D}{4} = 0\right)$, we get

$$\begin{aligned}
&(c_{1,1,1} + a_{1,1,1}\tau)(c_{2,2,2} + a_{2,2,2}\tau) = (c_{2,1,1} + a_{2,1,1}\tau)(c_{1,2,2} + a_{1,2,2}\tau)\\
\implies\ & c_{1,1,1}c_{2,2,2} + \frac{D}{4}(a_{1,1,1}a_{2,2,2}) = c_{2,1,1}c_{1,2,2} + \frac{D}{4}(a_{2,1,1}a_{1,2,2})\\
& c_{1,1,1}a_{2,2,2} + c_{2,2,2}a_{1,1,1} = c_{2,1,1}a_{1,2,2} + c_{1,2,2}a_{2,1,1}
\end{aligned}$$

$$\begin{aligned}
&(c_{1,1,1} + a_{1,1,1}\tau)(c_{2,2,2} + a_{2,2,2}\tau) = (c_{1,2,1} + a_{1,2,1}\tau)(c_{2,1,2} + a_{2,1,2}\tau)\\
\implies\ & c_{1,1,1}c_{2,2,2} + \frac{D}{4}(a_{1,1,1}a_{2,2,2}) = c_{1,2,1}c_{2,1,2} + \frac{D}{4}(a_{1,2,1}a_{2,1,2})\\
& c_{1,1,1}a_{2,2,2} + c_{2,2,2}a_{1,1,1} = c_{1,2,1}a_{2,1,2} + c_{2,1,2}a_{1,2,1}
\end{aligned}$$

$$\begin{aligned}
&(c_{1,1,1} + a_{1,1,1}\tau)(c_{2,2,2} + a_{2,2,2}\tau) = (c_{1,1,2} + a_{1,1,2}\tau)(c_{2,2,1} + a_{2,2,1}\tau)\\
\implies\ & c_{1,1,1}c_{2,2,2} + \frac{D}{4}(a_{1,1,1}a_{2,2,2}) = c_{1,1,2}c_{2,2,1} + \frac{D}{4}(a_{1,1,2}a_{2,2,1})\\
& c_{1,1,1}a_{2,2,2} + c_{2,2,2}a_{1,1,1} = c_{1,1,2}a_{2,2,1} + c_{2,2,1}a_{1,1,2}
\end{aligned}$$

$$\begin{aligned}
&(c_{1,1,1} + a_{1,1,1}\tau)(c_{1,2,2} + a_{1,2,2}\tau) = (c_{1,2,1} + a_{1,2,1}\tau)(c_{1,1,2} + a_{1,1,2}\tau)\\
\implies\ & c_{1,1,1}c_{1,2,2} + \frac{D}{4}(a_{1,1,1}a_{1,2,2}) = c_{1,2,1}c_{1,1,2} + \frac{D}{4}(a_{1,2,1}a_{1,1,2})\\
& c_{1,1,1}a_{1,2,2} + c_{1,2,2}a_{1,1,1} = c_{1,2,1}a_{1,1,2} + c_{1,1,2}a_{1,2,1}
\end{aligned}$$

$$\begin{aligned}(c_{2,1,1}+a_{2,1,1}\tau)(c_{2,2,2}+a_{2,2,2}\tau) &= (c_{2,2,1}+a_{2,2,1}\tau)(c_{2,1,2}+a_{2,1,2}\tau)\\ \implies c_{2,1,1}c_{2,2,2}+\frac{D}{4}(a_{2,1,1}a_{2,2,2}) &= c_{2,2,}c_{2,1,2}+\frac{D}{4}(a_{2,2,1}a_{2,1,2})\\ c_{2,1,1}a_{2,2,2}+c_{2,2,2}a_{2,1,1} &= c_{2,2,1}a_{2,1,2}+c_{2,1,2}a_{2,2,1}\end{aligned}$$

$$\begin{aligned}(c_{1,1,1}+a_{1,1,1}\tau)(c_{2,1,2}+a_{2,1,2}\tau) &= (c_{2,1,1}+a_{2,1,1}\tau)(c_{1,1,2}+a_{1,1,2}\tau)\\ \implies c_{1,1,1}c_{2,1,2}+\frac{D}{4}(a_{1,1,1}a_{2,1,2}) &= c_{2,1,1}c_{1,1,2}+\frac{D}{4}(a_{2,1,1}a_{1,1,2})\\ c_{1,1,1}a_{2,1,2}+c_{2,1,2}a_{1,1,1} &= c_{2,1,1}a_{1,1,2}+c_{1,1,2}a_{2,1,1}\end{aligned}$$

$$\begin{aligned}(c_{1,2,1}+a_{1,2,1}\tau)(c_{2,2,2}+a_{2,2,2}\tau) &= (c_{2,2,1}+a_{2,2,1}\tau)(c_{1,2,2}+a_{1,2,2}\tau)\\ \implies c_{1,2,1}c_{2,2,2}+\frac{D}{4}(a_{1,2,1}a_{2,2,2}) &= c_{2,2,1}c_{1,2,2}+\frac{D}{4}(a_{2,2,1}a_{1,2,2})\\ c_{1,2,1}a_{2,2,2}+c_{2,2,2}a_{1,2,1} &= c_{2,2,1}a_{1,2,2}+c_{1,2,2}a_{2,2,1}\end{aligned}$$

$$\begin{aligned}(c_{1,1,1}+a_{1,1,1}\tau)(c_{2,2,1}+a_{2,2,1}\tau) &= (c_{2,1,1}+a_{2,1,1}\tau)(c_{1,2,1}+a_{1,2,1}\tau)\\ \implies c_{1,1,1}c_{2,2,1}+\frac{D}{4}(a_{1,1,1}a_{2,2,1}) &= c_{2,1,1}c_{1,2,1}+\frac{D}{4}(a_{2,1,1}a_{1,2,1})\\ c_{1,1,1}a_{2,2,1}+c_{2,2,1}a_{1,1,1} &= c_{2,1,1}a_{1,2,1}+c_{1,2,1}a_{2,1,1}\end{aligned}$$

$$\begin{aligned}(c_{1,1,2}+a_{1,1,2}\tau)(c_{2,2,2}+a_{2,2,2}\tau) &= (c_{2,1,2}+a_{2,1,2}\tau)(c_{1,2,2}+a_{1,2,2}\tau)\\ \implies c_{1,1,2}c_{2,2,2}+\frac{D}{4}(a_{1,1,2}a_{2,2,2}) &= c_{2,1,2}c_{1,2,2}+\frac{D}{4}(a_{2,1,2}a_{1,2,2})\\ c_{1,1,2}a_{2,2,2}+c_{2,2,2}a_{1,1,2} &= c_{2,1,2}a_{1,2,2}+c_{1,2,2}a_{2,1,2}\end{aligned}$$

Letting

$$\begin{aligned}a' &= c_{1,1,1}\\ b' &= c_{1,2,1}\\ c' &= c_{1,1,2}\\ d' &= c_{1,2,2}\\ e' &= c_{2,1,1}\\ f' &= c_{2,2,1}\\ g' &= c_{2,1,2}\\ h' &= c_{2,2,2}\end{aligned}$$

gives the desired result

When $D \equiv 1 \pmod 4$, $\tau^2 - \tau + \frac{1-D}{4} = 0 \implies \tau^2 = \tau - \frac{1-D}{4}$

$$\begin{aligned}(c_{1,1,1} + a_{1,1,1}\tau)(c_{2,2,2} + a_{2,2,2}\tau) &= (c_{2,1,1} + a_{2,1,1}\tau)(c_{1,2,2} + a_{1,2,2}\tau)\\ \implies c_{1,1,1}c_{2,2,2} + \frac{D-1}{4}(a_{1,1,1}a_{2,2,2}) &= c_{2,1,1}c_{1,2,2} + \frac{D-1}{4}(a_{2,1,1}a_{1,2,2})\\ c_{1,1,1}a_{2,2,2} + c_{2,2,2}a_{1,1,1} + a_{1,1,1}a_{2,2,2} &= c_{2,1,1}a_{1,2,2} + c_{1,2,2}a_{2,1,1} + a_{2,1,1}a_{1,2,2}\end{aligned}$$

$$\begin{aligned}(c_{1,1,1} + a_{1,1,1}\tau)(c_{2,2,2} + a_{2,2,2}\tau) &= (c_{1,2,1} + a_{1,2,1}\tau)(c_{2,1,2} + a_{2,1,2}\tau)\\ \implies c_{1,1,1}c_{2,2,2} + \frac{D-1}{4}(a_{1,1,1}a_{2,2,2}) &= c_{1,2,1}c_{2,1,2} + \frac{D-1}{4}(a_{1,2,1}a_{2,1,2})\\ c_{1,1,1}a_{2,2,2} + c_{2,2,2}a_{1,1,1} + a_{1,1,1}a_{2,2,2} &= c_{1,2,1}a_{2,1,2} + c_{2,1,2}a_{1,2,1} + a_{1,2,1}a_{2,1,2}\end{aligned}$$

$$\begin{aligned}(c_{1,1,1} + a_{1,1,1}\tau)(c_{2,2,2} + a_{2,2,2}\tau) &= (c_{1,1,2} + a_{1,1,2}\tau)(c_{2,2,1} + a_{2,2,1}\tau)\\ \implies c_{1,1,1}c_{2,2,2} + \frac{D-1}{4}(a_{1,1,1}a_{2,2,2}) &= c_{1,1,2}c_{2,2,1} + \frac{D-1}{4}(a_{1,1,2}a_{2,2,1})\\ c_{1,1,1}a_{2,2,2} + c_{2,2,2}a_{1,1,1} + a_{1,1,1}a_{2,2,2} &= c_{1,1,2}a_{2,2,1} + c_{2,2,1}a_{1,1,2} + a_{1,1,2}a_{2,2,1}\end{aligned}$$

$$\begin{aligned}(c_{1,1,1} + a_{1,1,1}\tau)(c_{1,2,2} + a_{1,2,2}\tau) &= (c_{1,2,1} + a_{1,2,1}\tau)(c_{1,1,2} + a_{1,1,2}\tau)\\ \implies c_{1,1,1}c_{1,2,2} + \frac{D-1}{4}(a_{1,1,1}a_{1,2,2}) &= c_{1,2,1}c_{1,1,2} + \frac{D-1}{4}(a_{1,2,1}a_{1,1,2})\\ c_{1,1,1}a_{1,2,2} + c_{1,2,2}a_{1,1,1} + a_{1,1,1}a_{1,2,2} &= c_{1,2,1}a_{1,1,2} + c_{1,1,2}a_{1,2,1} + a_{1,2,1}a_{1,1,2}\end{aligned}$$

$$\begin{aligned}(c_{2,1,1} + a_{2,1,1}\tau)(c_{2,2,2} + a_{2,2,2}\tau) &= (c_{2,2,1} + a_{2,2,1}\tau)(c_{2,1,2} + a_{2,1,2}\tau)\\ \implies c_{2,1,1}c_{2,2,2} + \frac{D-1}{4}(a_{2,1,1}a_{2,2,2}) &= c_{2,2,1}c_{2,1,2} + \frac{D-1}{4}(a_{2,2,1}a_{2,1,2})\\ c_{2,1,1}a_{2,2,2} + c_{2,2,2}a_{2,1,1} + a_{2,1,1}a_{2,2,2} &= c_{2,2,1}a_{2,1,2} + c_{2,1,2}a_{2,2,1} + a_{2,2,1}a_{2,1,2}\end{aligned}$$

$$\begin{aligned}(c_{1,1,1} + a_{1,1,1}\tau)(c_{2,1,2} + a_{2,1,2}\tau) &= (c_{2,1,1} + a_{2,1,1}\tau)(c_{1,1,2} + a_{1,1,2}\tau)\\ \implies c_{1,1,1}c_{2,1,2} + \frac{D-1}{4}(a_{1,1,1}a_{2,1,2}) &= c_{2,1,1}c_{1,1,2} + \frac{D-1}{4}(a_{2,1,1}a_{1,1,2})\\ c_{1,1,1}a_{2,1,2} + c_{2,1,2}a_{1,1,1} + a_{1,1,1}a_{2,1,2} &= c_{2,1,1}a_{1,1,2} + c_{1,1,2}a_{2,1,1} + a_{2,1,1}a_{1,1,2}\end{aligned}$$

$$\begin{aligned}(c_{1,2,1} + a_{1,2,1}\tau)(c_{2,2,2} + a_{2,2,2}\tau) &= (c_{2,2,1} + a_{2,2,1}\tau)(c_{1,2,2} + a_{1,2,2}\tau)\\ \implies c_{1,2,1}c_{2,2,2} + \frac{D-1}{4}(a_{1,2,1}a_{2,2,2}) &= c_{2,2,1}c_{1,2,2} + \frac{D-1}{4}(a_{2,2,1}a_{1,2,2})\\ c_{1,2,1}a_{2,2,2} + c_{2,2,2}a_{1,2,1} + a_{1,2,1}a_{2,2,2} &= c_{2,2,1}a_{1,2,2} + c_{1,2,2}a_{2,2,1} + a_{2,2,1}a_{1,2,2}\end{aligned}$$

$$
\begin{aligned}
(c_{1,1,1} + a_{1,1,1}\tau)(c_{2,2,1} + a_{2,2,1}\tau) &= (c_{2,1,1} + a_{2,1,1}\tau)(c_{1,2,1} + a_{1,2,1}\tau) \\
\implies c_{1,1,1}c_{2,2,1} + \frac{D-1}{4}(a_{1,1,1}a_{2,2,1}) &= c_{2,1,1}c_{1,2,1} + \frac{D-1}{4}(a_{2,1,1}a_{1,2,1}) \\
c_{1,1,1}a_{2,2,1} + c_{2,2,1}a_{1,1,1} + a_{1,1,1}a_{2,2,1} &= c_{2,1,1}a_{1,2,1} + c_{1,2,1}a_{2,1,1} + a_{2,1,1}a_{1,2,1}
\end{aligned}
$$

$$
\begin{aligned}
(c_{1,1,2} + a_{1,1,2}\tau)(c_{2,2,2} + a_{2,2,2}\tau) &= (c_{2,1,2} + a_{2,1,2}\tau)(c_{1,2,2} + a_{1,2,2}\tau) \\
\implies c_{1,1,2}c_{2,2,2} + \frac{D-1}{4}(a_{1,1,2}a_{2,2,2}) &= c_{2,1,2}c_{1,2,2} + \frac{D-1}{4}(a_{2,1,2}a_{1,2,2}) \\
c_{1,1,2}a_{2,2,2} + c_{2,2,2}a_{1,1,2} + a_{1,1,2}a_{2,2,2} &= c_{2,1,2}a_{1,2,2} + c_{1,2,2}a_{2,1,2} + a_{2,1,2}a_{1,2,2}
\end{aligned}
$$

$$a'h' - e'd' = \frac{D-1}{4}(ed - ah) \tag{51}$$

$$a'h - d'e - e'd + h'a = de - ah \tag{52}$$

$$a'h' - b'g' = \frac{D-1}{4}(bg - ah) \tag{53}$$

$$a'h - b'g - g'b + h'a = bg - ah \tag{54}$$

$$a'h' - c'f' = \frac{D-1}{4}(cf - ah) \tag{55}$$

$$a'h - c'f - f'c + h'a = cf - ah \tag{56}$$

$$a'd' - b'c' = \frac{D-1}{4}(bc - ad) \tag{57}$$

$$a'd - b'c - c'b + d'a = bc - ad \tag{58}$$

$$e'h' - f'g' = \frac{D-1}{4}(fg - eh) \tag{59}$$

$$e'h - f'g - g'f + h'e = fg - eh \tag{60}$$

$$a'g' - c'e' = \frac{D-1}{4}(ce - ag) \tag{61}$$

$$a'g - c'e - e'c + g'a = ce - ag \tag{62}$$

$$b'h' - d'f' = \frac{D-1}{4}(df - bh) \tag{63}$$

$$b'h - d'f - f'd + h'b = df - bh \tag{64}$$

$$a'f' - b'e' = \frac{D-1}{4}(be - af) \tag{65}$$

$$a'f - b'e - e'b + f'a = be - af \tag{66}$$

$$c'h' - d'g' = \frac{D-1}{4}(dg - ch) \tag{67}$$

$$c'h - d'g - g'd + h'c = dg - ch \tag{68}$$