Gauss Composition

Pan Jing Bin

Supervisor: A/P Chin Chee Whye

Department of Mathematics

National University of Singapore

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 $[f]$ 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 $C(\Delta)$ denote the set of $SL_2(\mathbb{Z})$-equivalence classes of primitive binary quadratic forms of discriminant Δ. Let $C_1, C_2 \in C(\Delta)$ 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 $\bullet : C(\Delta) \times C(\Delta) \to C(\Delta)$ by :

$$C_1 \bullet C_2 = C_3.$$

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

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

Example 2.2.6. We consider $C(-56)$. Note that -56 is a fundamental discriminant. Let $f = [2, 0, 7]$ and $g = [3, 2, 5]$. To compose $[f]$ and $[g]$, 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 $[f] \bullet [g]$ 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 it's 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 $MP^{-1} = P_1P_2 \cdots P_n$ is a product of prime ideals. It follows that $M = P_1P_2 \cdots P_nP$ 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

$$(r) = S_1S_2 \cdots S_t \text{ and } rF = (r)F = Q_1Q_2 \cdots Q_k$$

are products of prime ideals. Then $F = S_1^{-1}S_2^{-1} \cdots S_t^{-1}Q_1Q_2 \cdots Q_k$ 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 $I = \prod_{P \in \mathfrak{P}} P^{n_p}$ 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 $\left\{ a_i b_j \mid 1 \leq i \leq n, 1 \leq j \leq m \right\}$. 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

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

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^TM 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

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

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

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

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 **??** and Remark **??**). 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

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

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 Norm of an Ideal

We can now discuss the concept of fractional ideals in number rings. We develop the notion of norm of an ideal in the language of lattices. This will allow us to generalise the concept to arbitrary rings whose additive group is isomorphic to $\mathbb{Z}^n$, but may not be number rings.

Definition 4.7.1. 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 4.7.2. Since an algebraic number field is a finite dimensional $\mathbb{Q}$-vector space, every non-zero fractional ideal of a number ring is a lattice.

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 4.7.1.

Proposition 4.7.3. 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 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 **??**) 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 4.7.4. Let L be a lattice in V and $\varphi : V \to V$ 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 $\{x_1, \cdots, x_n\}$, φ can also be viewed as a $\mathbb{Z}$-linear automorphism $L \to L$. Thus φ can be represented by a $M_{n\times n}(\mathbb{Z})$ matrix A. By the Smith Normal Form, $\exists P, Q \in GL_n(\mathbb{Z})$ 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, $|\det(A)| = |a_1 \cdots a_n|$.

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

Proposition 4.7.5. 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, φ is an automorphism.

Corollary 4.7.6. 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 $|L_2/L_1| = |\det(\varphi)|$ which is clearly finite.

Remark 4.7.7. 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 4.7.8. 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

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

Proposition 4.7.8 gives us two immediate corollaries.

Corollary 4.7.9. If φ_1 and φ_2 are both $\mathbb{Q}$-linear automorphisms such that $\varphi_1(L_1) = \varphi_2(L_1) = L_2$, then $|\det(\varphi_1)| = |\det(\varphi_2)|$.

Corollary 4.7.10. If M_1 and M_2 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 4.7.11 (Norm)**.** Let R be a number ring corresponding to the number field K and I be a fractional ideal of R. Define the **norm** of a non-zero ideal I by

$$N^R(I) = \frac{|L/I|}{|L/R|}$$

where L is any lattice in K containing both I and R. The norm of the zero ideal is defined to be 0.

Remark 4.7.12. When I is an integral ideal of R, then by choosing $L = R$, we get

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

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

We shall state some useful properties about the norm of an ideal in the setting of number rings. For the rest of this section, let R be a number ring corresponding to the number field K.

Proposition 4.7.13. Let $I = (\alpha)$ be a principal fractional ideal of R. Then $N^R(I) = |N^R(\alpha)|$, where $N^R(\alpha)$ is defined as in **??**.

Proof. The statement trivially holds if $\alpha = 0$. Thus we may further assume $\alpha \neq 0$. By definition $N^R(\alpha) = \det(\varphi_\alpha)$, where $\varphi_\alpha : K \to K$ is the $\mathbb{Q}$-linear multiplication map

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

On the other hand, φ_α is an automorphism satisfying $\varphi_\alpha(R) = I$. For any lattice M in K containing I, we have by Proposition 4.7.8 :

$$N^R(I) = \frac{|M/I|}{|M/R|} = |\det(\varphi_\alpha)|.$$

Theorem 4.7.14 (Multiplicativity)**.** Let I and J be two fractional ideals of R. Then

$$N^R(I)N^R(J) = N^R(IJ).$$

Proof. Since the equation trivially holds if either I or J is the zero ideal, we assume that both I and J are non-zero.

We first prove that the equation holds if both I and J are integral ideals of R. It suffices to prove that $|R/I||R/J| = |R/IJ|$. Since a number ring is a Dedekind domain, J factors into a product of prime ideals. Thus we may further assume that J is prime. Since $IJ \subseteq I \subseteq R$, we have $|R/IJ| = |R/I||I/IJ|$.

We shall prove that $|I/IJ| = |R/J|$. When I/IJ is viewed as an R-module, we have $J \subseteq \mathrm{Ann}(I/IJ)$. Thus I/IJ is naturally also a R/J-module. Since J is prime, I/IJ is a R/J vector space. The subspaces of I/IJ are of the form K/IJ where K is an ideal of R satisfying $IJ \subseteq K \subseteq I$. But J is prime, and by formula (3) of Proposition 3.3.3, there are no ideals between I and IJ. Thus I/IJ is a one-dimensional vector space so $|I/IJ| = |R/J|$.

Now let I and J be fractional ideals of R. Then $\exists r_i, r_j \in R$ such that $r_i I$ and $r_j J$ are integral ideals.

We first note that if P, Q are any non-zero fractional ideals of R and $r \in R \setminus \{0\}$, then $|P/Q| = |rP/rQ|$ since the multiplication map $\varphi_r : P/Q \to rP/rQ$ is a well-defined isomorphism.

Let $r_i, r_j \in R \setminus \{0\}$ be such that $r_i I$ and $r_j J$ are integral ideals of R. Then the principal fractional ideal $(1/r_i r_j)$ contains both I and J.

$$\begin{aligned} N^R(I)N^R(J) &= \frac{|(1/(r_i r_j)/I|}{|(1/r_i r_j)/R|}\frac{|(1/r_i r_j)/J|}{|(1/r_i r_j)/R|} \\ &= \frac{|R/r_i r_j I|}{|R/(r_i r_j)|}\frac{|R/r_i r_j J|}{|R/(r_i r_j)|} \\ &= \frac{|R/(r_i^2 r_j^2 IJ)|}{|R/(r_i r_j)||R/(r_i r_j)|} \\ &= \frac{|R/(r_i r_j IJ)||R/(r_i r_j)|}{|R/(r_i r_j)||R/(r_i r_j)|} \\ &= \frac{|(1/r_i r_j)/IJ|}{|(1/r_i r_j)/R|} \\ &= N^R(IJ) \end{aligned}$$

Corollary 4.7.15. $N^R(I^{-1}) = N^R(I)^{-1}$.

Proof. Follows immediately from the observation that $N^R(R) = 1$.

Corollary 4.7.16. Let J be a non-zero fractional ideal of R and let $\alpha \in J$. Then $\dfrac{N^R(\alpha)}{N^R(J)} \in \mathbb{Z}$.

Proof. Recall that $N^R(\alpha) = N^R(I)$, where I is the principal ideal of R generated by α. Using the unique factorisation of Dedekind domains (Theorem **??**), we have

$$\begin{aligned} \frac{N^R(\alpha)}{N^R(J)} &= \frac{N^R(I)}{N^R(J)} \\ &= \frac{\prod_{\mathfrak{p}\in P}\left[N^R(\mathfrak{p})\right]^{n_\mathfrak{p}}}{\prod_{\mathfrak{p}\in P}\left[N^R(\mathfrak{p})\right]^{m_\mathfrak{p}}} \\ &= \prod_{\mathfrak{p}\in P}\left[N^R(\mathfrak{p})\right]^{n_\mathfrak{p}-m_\mathfrak{p}} \end{aligned}$$

where $n_\mathfrak{p}$ and $m_\mathfrak{p}$ denote the exponents of the prime ideal $\mathfrak{p}$ in I and J respectively. Since $I \subseteq J$, by formula (3) of Proposition 3.3.3, we have that $n_\mathfrak{p} \geq m_\mathfrak{p}$ for each $\mathfrak{p}$. Since the norm of all prime ideals are integers (prime ideals are integral ideals), we conclude that the product $\prod_{\mathfrak{p}\in P}\left[N^R(\mathfrak{p})\right]^{n_\mathfrak{p}-m_\mathfrak{p}}$ is also an integer.

5 Quadratic Number Fields

In this chapter, we will use the results proved in chapter 4 to study quadratic rings. After establishing some important properties about quadratic rings, we will end off by constructing an isomorphism between the narrow class group and the form class group.

Remark 5.0.1. For the purpose of our discussion, 1 will **not** be considered a square-free integer.

5.1 Classification of Quadratic Fields and Quadratic Rings

We start with some basic definitions.

Definition 5.1.1. A **quadratic algebraic number** is an algebraic number that is a root of a degree two polynomial with coefficients in $\mathbb{Q}$.

A quadratic algebraic number that is the root of a monic degree two polynomial with coefficients in $\mathbb{Z}$ is called a **quadratic integer**.

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

A **quadratic ring** is a number ring corresponding to a quadratic field.

We shall now proceed to classify all quadratic fields.

Proposition 5.1.2. Every quadratic field is of the form $\mathbb{Q}[\sqrt{d}]$, where d is a square-free integer.

Proof. Let $K = \mathbb{Q}[\alpha]$ be a quadratic field. Then α has degree two so we write $\alpha^2 = b\alpha + c$ for some $b, c \in \mathbb{Q}$. Solving, we get $\alpha = (b \pm \sqrt{b^2 + 4c})/2$. 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 $v^2 \mid nm$. Then d is square free and we have

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

as desired.

Proposition 5.1.3. 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. 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.

$\{1, \sqrt{d_1}\}$ is a $\mathbb{Q}$-basis for $\mathbb{Q}[\sqrt{d_1}]$ so $\exists a, b \in \mathbb{Q}$ such that $a_1 + b_1\sqrt{d_1} = \sqrt{d_2}$. Then $(a_1^2 + b_1^2 d_1 - d_2) + (2a_1 b_1 \sqrt{d_1}) = 0 \implies a_1 b_1 = 0$ by linear independence of $\{1, \sqrt{d_1}\}$. If $b_1 = 0$, then $\sqrt{d_2} = a_1$ which contradicts the $\mathbb{Q}$-linear independence of $\{1, \sqrt{d_2}\}$. Thus $a_1 = 0$ so we have $b_1\sqrt{d_1} = \sqrt{d_2} \implies b_1^2 d_1 = d_2$. Since d_2 is square-free, we have $b_1 = 1$ so $d_1 = d_2$.

Remark 5.1.4. From Proposition 5.1.2 and Proposition 5.1.3, we deduce that there is a bijection between the set of square-free integers (excluding 1) and the set of quadratic rings via

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

We now give a concrete characterisation of quadratic rings.

Theorem 5.1.5. Let $K = \mathbb{Q}[\sqrt{d}]$ be a quadratic field where d is a square-free integer. (In particular, $d \not\equiv 0 \pmod 4$) Let $R = \mathbb{A} \ \cap \ K$ be the corresponding quadratic ring. Then

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

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 $a = a'/2, b = b'/2$ for $a', b' \in \mathbb{Z}$ with $a' \equiv b' \equiv 1 \pmod 2$, then $2a \in \mathbb{Z}$. We also have $(a')^2 - d(b')^2 \equiv 0 \pmod 4 \implies a^2 - db^2 \in \mathbb{Z}$ so $f(x)$ 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 $\alpha = r \in \mathbb{Z}$ and we are done. If $s \neq 0$, then $m_\alpha(x) = x^2 - 2rx + r^2 - ds^2$. By Proposition **??**, $\alpha \in R \iff 2r \in \mathbb{Z}$ and $r^2 - ds^2 \in \mathbb{Z}$.

Then $4r^2 \in \mathbb{Z}$ and $4r^2 - 4ds^2 \in \mathbb{Z} \implies 4ds^2 = d(2s)^2 \in \mathbb{Z}$. Write $2s = p/q$ where $p, q \in \mathbb{Z}$ with $\gcd(p, q) = 1$. Then $q^2 \mid d \implies q = 1$ 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 $d \equiv 2 \pmod 4$ or $d \equiv 3 \pmod 4$, we must have $x \equiv y \equiv 0 \pmod 2 \implies r, s \in \mathbb{Z}$. On the other hand, if $d \equiv 1 \pmod 4$, we have $x \equiv y \pmod 2$. This completes the proof.

Definition 5.1.6 (Quadratic conjugate)**.** For a quadratic field $\mathbb{Q}[\sqrt{d}]$, there is only one non-trivial embedding $\sigma : \mathbb{Q}[\sqrt{d}] \to \mathbb{C}$, which is defined by

$$\sigma(a + b\sqrt{d}) = a - b\sqrt{d}.$$

For a quadratic algebraic number r, we use $\overline{r}$ to denote $\sigma(r)$.

We now give explicit formulas for computing trace, norm and discriminant. Let R be a quadratic ring correspond to the quadratic field $\mathbb{Q}[\sqrt{d}]$ where d is square-free.

Proposition 5.1.7. 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 **??**. A $\mathbb{Z}$-basis for R is given by $\{1, \sqrt{d}\}$ if $d \equiv 2$ or $3 \pmod 4$ and $\{1, \frac{1+\sqrt{d}}{2}\}$ 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, $\operatorname{tr}(\Phi_r) = 2a$ and $\det(\Phi_r) = a^2 - bd^2$.

Proposition 5.1.8. 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 $\{1, \sqrt{d}\}$,

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

If $d \equiv 1 \pmod 4$, then

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

Remark 5.1.9. By the previous proposition, there is a natural bijection between the set of fundamental discriminants (excluding 1) and the set of quadratic rings. For a fundamental discriminant D, we use $S(D)$ to denote the unique quadratic ring of discriminant D.

5.2 Narrow Class Group

Definition 5.2.1. Let $S(D)$ be the quadratic ring corresponding to the quadratic number field $\mathbb{Q}[\sqrt{d}]$, where $D = \operatorname{disc}(R)$. In Theorem 5.1.5, we have shown that the structure of $S(D)$ differs slightly depending on whether $D \equiv 0$ or $1 \pmod 4$. To handle both cases simultaneously, we define

$$\delta = \begin{cases} -\frac{\sqrt{D}}{2} & \text{if } D \equiv 0 \pmod 4 \\ \frac{1-\sqrt{D}}{2} & \text{if } D \equiv 1 \pmod 4. \end{cases}$$

Then δ is the root to $x^2 - \frac{D}{4}$ if $D \equiv 0 \pmod 4$ and the root to $x^2 - x + \frac{1-D}{4}$ if $D \equiv 1 \pmod 4$.

By Corollary **??**, every non-zero integral ideal I of R has a $\mathbb{Z}$-basis. We first define a canonical $\mathbb{Z}$-basis to make computations easier.

Remark 5.2.2. For $\alpha_1, \alpha_2 \in S(D)$, we use $\langle \alpha_1, \alpha_2 \rangle$ to denote $\{a\alpha_1 + b\alpha_2 \mid a, b \in \mathbb{Z}\}$.

Theorem 5.2.3. *Every non-zero integral ideal I of R has a unique $\mathbb{Z}$-basis $\{a, b + g\delta\}$ satisfying*

1. $a, b, g \in \mathbb{Z}$.
2. $0 \leq b < a$.
3. $0 < g \leq a$.
4. *g divides both a and b.*

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

Proposition 5.2.4. *I has a $\mathbb{Z}$-basis $\{a, b + g\delta\}$, where $a, b, g \in \mathbb{Z}$, $0 \leq b < a$ and $0 < g \leq a$.*

Proof. Let $\{\alpha_1, \alpha_2\}$ be any $\mathbb{Z}$-basis of I and write $\alpha_1 = a_1 + b_1\delta$, $\alpha_2 = a_2 + b_2\delta$ for $a_1, a_2, b_1, b_2 \in \mathbb{Z}$. 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, the two operations

$$\{\alpha_1, \alpha_2 - k\alpha_1\} \text{ and } \{\alpha_1 - k\alpha_2, \alpha_2\} \tag{3}$$

on the basis does not change the ideal I.

This allows us to perform 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, we have

$I = \langle a, b + g\delta \rangle$ for $a, b, g \in \mathbb{Z}$. Since we can subtract multiples of a and $a\delta$ from $b + g\delta$, we may further assume that $0 \leq b < a$ and $0 < g \leq a$. (Note that $g \neq 0$ since I is a free $\mathbb{Z}$-module of rank 2)

Proposition 5.2.5. Let $c \in \mathbb{Z} \cap I$. Then $a \mid c$.

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

Proposition 5.2.6. The basis given above is unique.

Proof. By Proposition 5.2.5, a is clearly unique. Let $I = \langle a, b + g\delta \rangle = \langle a, b' + g'\delta \rangle$. Then $\exists x_1, y_1, x_2, y_2 \in \mathbb{Z}$ such that

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

Observe that $g \mid g'$ and $g' \mid g \implies g = g'$ since both g and g' are positive. Thus $y_1 = y_2 = 1$ and since $0 \leq b, b' < a$, it follows that $x_1 = x_2 = 0$.

Proposition 5.2.7. In the basis given above, we have $g \mid a$ and $g \mid b$.

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

On the other hand, $(b + g\delta)\delta \in I \implies \exists x', y' \in \mathbb{Z}$ such that $ax' + (b + g\delta)y' = b\delta + g\delta^2$.

If $D \equiv 0 \pmod 4$, then $\delta^2 = \dfrac{D}{4} \implies gy' = b$.

If $D \equiv 1 \pmod 4$, then $\delta^2 = -\dfrac{1 - D}{4} + \delta \implies gy' = b + g$.

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

Propositions 5.2.4 to 5.2.7 prove Theorem 5.2.3.

While all non-zero 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 5.2.8. Let a, b, g be integers satisfying

1. $a > 0$.
2. $0 \leq b < a$.
3. $g > 0, \ g \mid b$ and $g \mid a$.
4. $a \mid N^{S(D)}(b + g\delta)$.

Then $\langle a, b + g\delta \rangle$ is an integral ideal with canonical basis $\{a, b + g\delta\}$.

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

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

has canonical basis $\{a, b + g\delta\}$. Since $g \mid b$ and $g \mid a$, we may without loss of generality assume $g = 1$. Let $\{t, r + s\delta\}$ be the canonical basis for I. Since $b + \delta \in I$, we must have $s = 1$. Next we need a lemma.

Lemma 5.2.9. Let $z \in I \cap \mathbb{Z}$. Then $a \mid z$.

Proof. Note that z is of the form

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

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

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

For z to be an integer, we have

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

and so

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

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

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

For z to be an integer, we have

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

and similarly,

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

which is also divisible by a.

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

Remark 5.2.10. Theorem 5.2.3 also generalises to fractional ideals like so : Let I be a fractional ideal of $S(D)$ and let $s \in S(D)$ be such that sI is an integral ideal. If $\{a, b+g\delta\}$ is the canonical basis for sI, then $\{a/s, (b+g\delta)/s\}$ is the canonical basis for I.

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

Theorem 5.2.11. Let $I = \langle \alpha_1, \alpha_2 \rangle$ be a non-zero fractional ideal of $S(D)$. Then

$$N^{S(D)}(I) = \frac{|\alpha_1\overline{\alpha_2} - \overline{\alpha_1}\alpha_2|}{\sqrt{D}}.$$

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

$$\begin{aligned} \frac{\left|\alpha_1\overline{(\alpha_2 - k\alpha_1)} - \overline{\alpha_1}(\alpha_2 - k\alpha_1)\right|}{\sqrt{D}} &= \frac{\left|\alpha_1(\overline{\alpha_2} - k\overline{\alpha_1}) - \overline{\alpha_1}(\alpha_2 - k\alpha_1)\right|}{\sqrt{D}} \\ &= \frac{|\alpha_1\overline{\alpha_2} - \overline{\alpha_1}\alpha_2|}{\sqrt{D}}. \end{aligned}$$

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 2 operations, (and swapping of α_1 with α_2), the definition is independent of the choice of basis.

We first prove for the case where I is an integral ideal. We will use the canonical basis $\{a, b+g\delta\}$. Under this basis, we have

$$\begin{aligned} N^{S(D)}(I) &= \frac{|a(b+g\overline{\delta}) - a(b+g\delta)|}{\sqrt{D}} \\ &= \frac{|ag(\overline{\delta}-\delta)|}{\sqrt{D}}. \end{aligned}$$

In both the cases $D \equiv 0 \pmod 4$ and $D \equiv 1 \pmod 4$, we have

$$\frac{|ag(\overline{\delta}-\delta)|}{\sqrt{D}} = ag.$$

On the other hand, the elements of the quotient group $S(D)/I$ are precisely

$$\left\{ x + y\delta + I \mid 0 \le x < a, 0 \le y < g \right\}$$

so $|S(D)/I| = ag$.

Now let I be a general fractional ideal with $\mathbb{Z}$-basis $\{\beta_1, \beta_2\}$. Then $\exists r \in R$ such that rI is an integral ideal and $\{r\beta_1, r\beta_2\}$ is a $\mathbb{Z}$-basis for rI. Then

$$\begin{aligned} N^{S(D)}(I) &= \frac{N^{S(D)}(rI)}{N^{S(D)}(r)} \\ &= \frac{|r\beta_1\overline{r}\overline{\beta_2} - \overline{r}\overline{\beta_1}r\beta_2|}{r\overline{r}\sqrt{D}} \\ &= \frac{|\beta_1\overline{\beta_2} - \overline{\beta_1}\beta_2|}{\sqrt{D}}. \end{aligned}$$

Definition 5.2.12. Let $\{\alpha_1, \alpha_2\}$ be the $\mathbb{Z}$-basis of a fractional ideal I. By the above proposition

$$\alpha_1\overline{\alpha_2} - \overline{\alpha_1}\alpha_2 = \pm N^{S(D)}(I)\sqrt{D}.$$

The basis is **positively oriented** if $\alpha_1\overline{\alpha_2} - \overline{\alpha_1}\alpha_2$ is positive or positive imaginary.

Definition 5.2.13. Let $P^+(S(D))$ denote the subgroup of all principal fractional ideals of $S(D)$ generated by elements having positive norm. 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 non-zero fractional ideals of $S(D)$.

5.3 Isomorphism Between Form Class Group and Narrow Class Group

We finally have all the tools to prove the main theorem of interest in this paper.

Theorem 5.3.1. Let Δ be a fundamental discriminant. Let $C(\Delta)$ denote the form class group of discriminant Δ. Let $Cl^+(\Delta)$ denote the narrow class group of the quadratic ring $S(\Delta)$. Then

$$Cl^+(\Delta) \cong C(\Delta)$$

as groups.

Proof. We will construct explicit isomorphisms from $Cl^+(\Delta)$ to $C(\Delta)$ and vice versa.

Let $J = \langle \alpha_1, \alpha_2 \rangle$ be an ideal of $S(\Delta)$, where $\{\alpha_1, \alpha_2\}$ is a positively oriented basis. Define $\Phi : Cl^+(\Delta) \to C(\Delta)$ by

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

Remark 5.3.2. There is slight abuse of notation here as J refers to both the ideal and the equivalence class containing J in $Cl^+(\Delta)$. Similarly, for a binary quadratic form f, f will refer to both the binary quadratic form as well as it's $SL_2(\mathbb{Z})$-equivalence class in $C(\Delta)$.

Propositions 5.3.3 to 5.3.5 will show that Φ is a well-defined map.

Proposition 5.3.3. $\Phi(J)$ is an integral binary quadratic form of discriminant Δ.

Proof. Expanding, we have

$$\Phi(J) = \frac{\alpha_1\overline{\alpha_1}x^2 + (\alpha_1\overline{\alpha_2} + \overline{\alpha}_1\alpha_2)xy + \alpha_2\overline{\alpha_2}y^2}{N^{S(\Delta)}(J)}.$$

By Corollary 4.7.16, $\dfrac{N(\alpha_1)}{N^{S(\Delta)}(J)}, \dfrac{N(\alpha_2)}{N^{S(\Delta)}(J)}$ and $\dfrac{N(\alpha_1 + \alpha_2)}{N^{S(\Delta)}(J)}$ are all integers. Thus

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

is an integer as well.

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

$$\begin{aligned}
&\left(\frac{\alpha_1\overline{\alpha_2}+\overline{\alpha_1}\alpha_2}{N^{S(\Delta)}(J)}\right)^2 - 4\left(\frac{\alpha_1\overline{\alpha_1}}{N^{S(\Delta)}(J)}\right)\left(\frac{\alpha_2\overline{\alpha_2}}{N^{S(\Delta)}(J)}\right)\\
&= \frac{\alpha_1^2\overline{\alpha_2}^2 - 2\alpha_1\overline{\alpha_1}\alpha_2\overline{\alpha_2} + \overline{\alpha_1}^2\alpha_2^2}{[N^{S(\Delta)}(J)]^2}\\
&= \frac{(\alpha_1\overline{\alpha_2} - \overline{\alpha_1}\alpha_2)^2}{[N^{S(\Delta)}(J)]^2}\\
&= \Delta
\end{aligned}$$

where the last equality is due to Theorem 5.2.11.

Proposition 5.3.4. If $\{\alpha_1, \alpha_2\}$ and $\{\beta_1, \beta_2\}$ are both positively oriented bases for J, then

$$\big[\alpha_1 x + \alpha_2 y\big]\big[\overline{\alpha_1}x + \overline{\alpha_2}y\big] \sim \big[\beta_1 x + \beta_2 y\big]\big[\overline{\beta_1}x + \overline{\beta_2}y\big].$$

Proof. First observe that for any $k \in \mathbb{Z}$,

$$\begin{aligned}
\alpha_1(\overline{\alpha_2 - k\alpha_1}) - \overline{\alpha_1}(\alpha_2 - k\alpha_1) &= \alpha_1(\overline{\alpha_2} - k\overline{\alpha_1}) - \overline{\alpha_1}(\alpha_2 - k\alpha_1)\\
&= \alpha_1\overline{\alpha_2} - \overline{\alpha_1}\alpha_2
\end{aligned}$$

so the orientation of the basis remains unchanged after the operation $\{\alpha_1, \alpha_2 - k\alpha_1\}$. By symmetry, the same applies for $\{\alpha_1 - k\alpha_2, \alpha_2\}$. In the proof of Proposition 5.2.4, we have shown that $\{\alpha_1, \alpha_2\}$ and $\{\beta_1, \beta_2\}$ can be reduced to either $\{a, b+g\delta\}$ or $\{b+g\delta, a\}$ via operations of the form (3). Since $\{\alpha_1, \alpha_2\}$ and $\{\beta_1, \beta_2\}$ are positively oriented and $\{b+g\delta, a\}$ is negatively oriented, the latter case is impossible.

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

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

which is $SL_2(\mathbb{Z})$-equivalent to $\alpha_1\overline{\alpha_1}x^2 + (\alpha_1\overline{\alpha_2} + \overline{\alpha_1}\alpha_2)xy + \alpha_2\overline{\alpha_2}y^2$ via the matrix S^{-k}. (Remark **??**)

Proposition 5.3.5. If J and J' are equivalent ideals, then $\Phi(J) = \Phi(J')$.

Proof. $\exists r \in S(\Delta) \setminus \{0\}$ such that $rJ = J'$. If $J = \langle \alpha_1, \alpha_2 \rangle$, then $J' = \langle r\alpha_1, r\alpha_2 \rangle$.

Let $I = (r)$. Using the fact that ideal norm is multiplicative and Proposition 4.7.13 :

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

We now define the other half of the isomorphism. For a binary quadratic form $f = [A, B, C]$, define $\Psi : C(\Delta) \to Cl^+(\Delta)$ by

$$\Psi(f) = \begin{cases} \big\langle A, b_B + \delta \big\rangle & \text{if } A > 0 \\ \big\langle A\delta, b_B\delta + \delta^2 \big\rangle & \text{if } A < 0 \end{cases}$$

where $b_B = \dfrac{B}{2}$ or $\dfrac{B-1}{2}$ depending on whether $\Delta \equiv 0$ or 1 (mod 4) respectively.

Note that regardless of whether $\Delta \equiv 0$ or 1 (mod 4), we have $b_B + \delta = \dfrac{B}{2} - \dfrac{\sqrt{\Delta}}{2}$ and $N^{S(D)}(b_B + \delta) = (B^2 - \Delta)/4$.

Propositions 5.3.6 and 5.3.7 will show that Ψ is well-defined.

Proposition 5.3.6. Let $f = [A, B, C]$ be a binary quadratic form of discriminant Δ, where Δ is a fundamental discriminant. Then $\langle A, b_B + \delta \rangle$ is an ideal of $S(\Delta)$ with canonical basis $\{|A|, b' + \delta\}$, where $b' \equiv b_B \pmod{|A|}$.

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

$\exists k \in \mathbb{Z}$ such that $0 \le b_B + kA < A$. Then $\langle A, b_B + \delta \rangle = \langle A, b_B + kA + \delta \rangle$. Using the formula $B^2 - \Delta = 4AC$, we have

$$\begin{aligned}N^{S(\Delta)}(b_B + kA + \delta) &= N^{S(\Delta)}\left(\frac{B + 2kA - \sqrt{\Delta}}{2}\right) \\ &= \frac{B^2 - \Delta + 4kAB + 4k^2A^2}{4} \\ &= AC + \frac{4kAB + 4k^2A^2}{4}\end{aligned}$$

which is divisible by A. By Theorem 5.2.9, $\langle A, b_B + kA + \delta\rangle$ is an ideal of $S(\Delta)$ with canonical basis $\{A, b_B + kA + \delta\}$ which completes the proof.

Proposition 5.3.7. Let $f, g \in C(\Delta)$ be $SL_2(\mathbb{Z})$-equivalent binary quadratic forms. Then $\Psi(f) = \Psi(g)$.

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 **??**) Note that $(T^{-1}S^TT)^{-1} = S$. Since S and T generate $SL_2(\mathbb{Z})$, so does S^T and T.

Generator T produces the equivalence $[A, B, C] \sim [C, -B, A]$. Let $h = [C, -B, A]$. Consider 2 cases :

Case 1 : $N^{S(\Delta)}(b_B + \delta) > 0$.

Since $B^2 - 4AC = \Delta$, we have $4AC > 0$ and so A and C are of like sign.

If both A and B are positive, then $\Psi(f) = \langle A, b_B + \delta\rangle$ is narrowly equivalent to

$$\left\langle A(b_B + \overline{\delta}), N^{S(\Delta)}(b_B + \delta)\right\rangle$$

since $N^{S(\Delta)}(b_B + \overline{\delta})$ is also positive. This is in turn narrowly equivalent to

$$\left\langle b_B + \overline{\delta}, \frac{B^2 - \Delta}{4A}\right\rangle = \langle C, b_B + \overline{\delta}\rangle.$$

Finally, since -1 is invertible in $\mathbb{Z}$, we have

$$\langle C, b_B + \overline{\delta}\rangle = \langle C, -b_B - \overline{\delta}\rangle.$$

If $\Delta \equiv 0 \pmod 4$, then

$$\langle C, -b_B - \overline{\delta}\rangle = \left\langle C, -\frac{B}{2} + \delta\right\rangle = \langle C, b_{-B} + \delta\rangle.$$

If $\Delta \equiv 1 \pmod 4$, then

$$\langle C, -b - \overline{\delta}\rangle = \left\langle C, -\frac{B-1}{2} - \frac{1+\sqrt{\Delta}}{2}\right\rangle = \left\langle C, \frac{-B-1}{2} + \frac{1-\sqrt{\Delta}}{2}\right\rangle = \left\langle C, b_{-B} + \delta\right\rangle.$$

which is exactly $\Psi(h)$.

If A and C are both negative, then we obtain the same narrow equivalence by carrying a factor of δ throughout and repeating the same argument as above.

Case 2 : $N^{S(\Delta)}(b_B+\delta)<0$.

Then $\Delta>0 \implies N^{S(\Delta)}(\delta)<0$. By multiplicativity of norm,

$$N^{S(\Delta)}\big[(b_B+\overline{\delta})\delta\big]>0 \text{ and } N^{S(\Delta)}\big[(b_B+\overline{\delta})/\delta\big]>0.$$

Since $B^2-4AC=\Delta$, A and C are of opposite sign. If A is positive and C is negative, then $\Psi(f)=\langle A, b_B+\delta\rangle$ is narrowly equivalent to

$$\big\langle A\delta(b_B+\overline{\delta}), \delta N^{S(\Delta)}(b_B+\delta)\big\rangle$$

and if A is negative and C is positive, then $\Psi(f)=\langle A\delta, b_B\delta+\delta^2\rangle$ is narrowly equivalent to

$$\big\langle A(b_B+\overline{\delta}), N^{S(\Delta)}(b_B+\delta)\big\rangle$$

By repeating the same argument as in case 1, we get the same narrow equivalence between $\Psi(f)$ and $\Psi(h)$.

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

$$\begin{aligned}\Psi(k)&=\langle A, b_{2A+B}+\delta\rangle\\&=\langle A, b_B+A+\delta\rangle\\&=\langle A, b_B+\delta\rangle\\&=\Psi(f).\end{aligned}$$

Proposition 5.3.8. Ψ and Φ are inverses of each other.

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

$$\Phi\circ\Psi(f)=\Phi(\langle A, b_B+\delta\rangle)$$

Note that $A\overline{(b_B+\delta)}-\overline{A}(b_B+\delta)=A(\overline{\delta}-\delta)=A\sqrt{D}$ so $\{A, b_B+\delta\}$ is positively oriented.

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

On the other hand, if I is an ideal with canonical basis $\{a, b+g\delta\}$,

$$\begin{aligned}\Psi\circ\Phi(I)&=\Psi\left(\frac{a^2x^2+[a(b+g\overline{\delta})+a(b+g\delta)]xy+(b+g\delta)(b+g\overline{\delta})y^2}{ag}\right)\\&=\Psi\left(\frac{a}{g}x^2+\left(\frac{2b}{g}+\delta+\overline{\delta}\right)xy+\left(\frac{(b+g\delta)(b+g\overline{\delta})}{ag}\right)y^2\right)\\&=\begin{cases}\big\langle a/g, \big(2b/g+\delta+\overline{\delta}\big)/2+\delta\big\rangle & \text{if } \Delta\equiv 0 \pmod 4\\ \big\langle a/g, (2b/g+\delta+\overline{\delta}-1)/2+\delta\big\rangle & \text{if } \Delta\equiv 1 \pmod 4).\end{cases}\end{aligned}$$

If $\Delta \equiv 0 \pmod 4$, then

$$\begin{aligned}\frac{2b/g + \delta + \overline{\delta}}{2} &= \frac{2b/g - \sqrt{\Delta}/2 + \sqrt{\Delta}/2}{2} \\ &= b/g\end{aligned}$$

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

$$\begin{aligned}\frac{2b/g + \delta + \overline{\delta} - 1}{2} &= \frac{2b/g + (1-\sqrt{\Delta})/2 + (1+\sqrt{\Delta})/2 - 1}{2} \\ &= b/g\end{aligned}$$

so in both cases, $\Psi \circ \Phi(I)$ is narrowly equivalent to $\langle a, b + g\delta\rangle$.

Proposition 5.3.9. Ψ and Φ are group homomorphisms.

Proof. Since we have already proven that Ψ and Φ are inverses of each other, it suffices to show that Ψ is a group homomorphism. Let $f, g \in C(\Delta)$. Then $\exists A, A', B, C \in \mathbb{Z}$ such that $f \sim [A, B, CA']$ and $g \sim [A', B, CA]$. We have $f \bullet g \sim [AA', B, C]$.

Let $I = \langle A, b_B + \delta\rangle$ and $J = \langle A', b_B + \delta\rangle$. Then I and J are ideals by Proposition 5.3.6. By a direct (but tedious) computation, we also have that $IJ = \langle AA', b_B + \delta\rangle$. (A proof is provided in Appendix 7.1)

Let P_δ denote the principal ideal generated by δ. If A and A' are both positive, then

$$\Psi(f \bullet g) = \langle AA', b_B + \delta\rangle = IJ = \Psi(f)\Psi(g).$$

If A is positive and A' is negative, then

$$\Psi(f \bullet g) = \langle AA'\delta, b_B\delta + \delta^2\rangle = I[P_\delta J] = \Psi(f)\Psi(g).$$

The case where A is negative and A' is positive is similar. If both A and A' are negative, then observe that $N^{S(\Delta)}(\delta^2) = \left[N^{S(\Delta)}(\delta)\right]^2 > 0$ since $N^{S(\Delta)}(\delta) \in \mathbb{Z}$. Thus $\Psi(f \bullet g) = \langle AA', b_B + \delta\rangle$ is narrowly equivalent to

$$\begin{aligned}\langle AA'\delta^2, b_B\delta^2 + \delta^3\rangle &= (P_\delta I)(P_\delta J) \\ &= \Psi(f)\Psi(g).\end{aligned}$$

6 Bhargava's Reformulation

6.1 Bhargava's Cube

Definition 6.1.1. Let $\mathcal{C}_2$ denote the space $\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2$. Each element of $\mathcal{C}_2$ can be represented as a vector (a, b, c, d, e, f, g, h). This can be viewed as a cube of integers

Insert Picture Here.

Any cube $X \in \mathcal{C}_2$ can be partitioned in 3 different ways as follows :

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

or

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

or

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

Definition 6.1.2. An element

$$\left[\begin{pmatrix} r_1 & s_1 \\ t_1 & u_1 \end{pmatrix} \ , \ \begin{pmatrix} r_2 & s_2 \\ t_2 & u_2 \end{pmatrix} \ , \ \begin{pmatrix} r_3 & s_3 \\ t_3 & u_3 \end{pmatrix} \right]$$

in the group $\Gamma = SL_2(\mathbb{Z}) \times SL_2(\mathbb{Z}) \times SL_2(\mathbb{Z})$ act on a cube $X \in C_2$ by replacing (M_i, N_i) with $(rM_i + sN_i, tM_i + uN_i)$ for each i.

Proposition 6.1.3. The action given above is well-defined.

Definition 6.1.4. For a cube $X \in \mathcal{C}_2$ 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 above, then explicit formulas for Q_1^X, Q_2^X and Q_3^X are given by

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

Definition 6.1.5. A cube $X \in \mathcal{C}_2$ is **projective** if Q_1^X, Q_2^X and Q_3^X are primitive binary quadratic forms.

Let $Cl(\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2; D)$ denote the set of projective cubes of discriminant D.

Remark 6.1.6. Since any common divisor of the entries of a cube X also divides the coefficients of Q_1^X, Q_2^X and Q_3^X, the greatest common divisor of the entries of a projective cube is necessarily 1.

Definition 6.1.7. For a cube $X \in \mathcal{C}_2$, a quick computation reveals that $\operatorname{disc}(Q_1) = \operatorname{disc}(Q_2) = \operatorname{disc}(Q_3)$. Define the **discriminant** of X by

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

If X is as in (), then an explicit formula for the discriminant of X is given by

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

6.2 Cube Law

Theorem 6.2.1. Let $D \equiv 0$ or $1 \pmod 4$ and let $Q_{\mathrm{id,D}}$ be a primitive binary quadratic form of discriminant D such that there is a cube X_0 with $Q_1^{X_0} = Q_2^{X_0} = Q_3^{X_0} = Q_{\mathrm{id,D}}$. 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 with the following properties

1. $[Q_{\mathrm{id,D}}]$ is the identity element.
2. For any cube $X \in Cl(\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2; D)$, $[Q_1^X] + [Q_2^X] + [Q_3^X] = [Q_{\mathrm{id,D}}]$.
3. For any 3 binary quadratic forms Q_1, Q_2, Q_3 with $[Q_1] + [Q_2] + [Q_3] = [Q_{\mathrm{id,D}}]$, there exists, up to Γ-equivalence, a unique cube $Y \in Cl(\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2; D)$ such that $Q_1^Y = Q_1,\ Q_2^Y = Q_2$ and $Q_3^Y = Q_3$.

Proof. Let $F(D)$ be the free group over the set of all primitive binary quadratic forms of discriminant D. Let $S(D)$ be the subgroup of $F(D)$ generated by the set

$$\{Q_{\mathrm{id,D}}\} \bigcup \{\ Q_1^X + Q_2^X + Q_3^X \mid X \in Cl(\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2; D)\ \}.$$

Lemma 6.2.2. Let P_1 and P_2 be two primitive binary quadratic forms of discriminant D. Then there exists $X \in CL(\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2; D)$ such that $Q_1^X = P_1$ and $Q_2^X = P_2$.

Proof. Since P_1 and P_2 are primitive, there exist $A, A', B, C \in \mathbb{Z}$ such that $P_1 \sim [A, B, CA']$ and $P_2 \sim [A', B, CA]$. We may without loss of generality assume that $P_1 = [A, B, CA']$ and $P_2 = [A', B, CA]$. Observe that the three quadratic forms associated with the cube X

$$(1, 0, 0, -a, 0, -c, -a', b) \tag{4}$$

is given by

$$\begin{aligned} Q_1^X &= [A, B, CA'] \\ Q_2^X &= [A', B, CA] \\ Q_3^X &= [C, B, AA']. \end{aligned}$$

Since $\gcd(A, B, CA') = \gcd(A', B, CA) = 1$, a direct computation reveals that Q_3^X is also primitive so X is projective. This completes the proof of the lemma.

Theorem 6.2.3. Let $D \equiv 0$ or $1 \pmod 4$ and let $A_{id,D}$ be defined as in (3). Then there exists a unique group law on the set of Γ-equivalence class of projective cubes of discriminant D such that

1. $[A_{id,D}]$ is the identity element
2. For $i \in \{1,2,3\}$, the map $\varphi_i : Cl(\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2; D) \to Cl(\mathrm{Sym}^2\mathbb{Z}^2; D)$ defined by
$$\varphi_i(A) = [Q_i^A]$$
is a group homomorphism.

Proof. Let $X, Y \in Cl(\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2; D)$. Then

$$([Q_1^X] + [Q_1^Y]) + ([Q_2^X] + [Q_2^Y]) + ([Q_3^X] + [Q_3^Y]) = [Q_{\mathrm{id,D}}]$$

in $Cl(\mathrm{Sym}^2\mathbb{Z}^2)$. By property (3) of Theorem 6.2.1, there exists, up to Γ-equivalence, a unique $Z \in Cl(\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2; D)$ such that $[Q_i^Z] = [Q_i^X] + [Q_i^Y]$ for $i \in \{1,2,3\}$. Define the composition of $[X]$ and $[Y]$ by $[X] + [Y] = [Z]$.

Next we prove uniqueness. If X' and Y' are 2 projective cubes, then we must have $[Q_i^{X'+Y'}] = [Q_i^X] + [Q_i^Y]$. The uniqueness of the group law follows from the uniqueness of a cube satisfying this property.

Remark 6.2.4. The proof for Theorem 6.2.3 remains valid if $A_{\mathrm{id,D}}$ is replaced with any projective cube I satisfying $[Q_1^I] = [Q_2^I] = [Q_3^I]$. Bhargava decided to fix $[A_{\mathrm{id,D}}]$ as the identity element because Theorem 6.2.3 serves as the starting point for further generalisations.

6.3 Quadratic rings

Definition 6.3.1. A commutative ring R with unity is a **quadratic ring** if the additive group of R is isomorphic to $\mathbb{Z}^2$.

Proposition 6.3.2. For all integers congruent to 0 or 1 mod 4, there exists (up to isomorphism) a unique quadratic ring of discriminant D, given by

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

Proof. Let $R = \langle 1, \tau\rangle$ be a quadratic ring of discriminant D. Then $\tau^2 = r\tau + s$ for some $r, s \in \mathbb{Z}$ and so we have $\tau^2 + r\tau + s = 0$, with $r^2 + 4s = D$. The kernel of the ring homomorphism $\varphi : \mathbb{Z}[x] \to R$ given by

$$\varphi\bigg(\sum_{i=0}^{n} a_i x^i\bigg) = \sum_{i=0}^{n} a_i \tau^i$$

is the principal ideal (x^2+rx+s). Thus we have the isomorphism $\mathbb{Z}[x]/(x^2+rx+s) \cong R$. Consider 3 cases.

Case 1 : $D = 0$.

Then r is even and $x^2 + rx + s = (x - r/2)^2$. We have $\mathbb{Z}[x]/\big((x - r/2)^2\big) \cong \mathbb{Z}[x]/(x^2)$ by sending 1 to 1 and $x - r/2$ to x.

Case 2 : $D \geq 1$ is a perfect square.

Then $x^2 + rx + s = (x - a)(x - b)$ for some $a, b \in \mathbb{Z}$ with $a - b = D$. Then $\mathbb{Z}[x]/\big((x-a)(x-b)\big) \cong \mathbb{Z}[x]/\big(x(x-D)\big)$ by fixing $\mathbb{Z}$ and sending x to $x + a$.

Case 3 : $D \neq 0$ and D is not a perfect square.

Then define $\varphi : \mathbb{Z}[x] \to \mathbb{Z}\left[\dfrac{-r+\sqrt{D}}{2}\right]$ by fixing $\mathbb{Z}$ and sending x to $\dfrac{-r+\sqrt{D}}{2}$. We have

$$\mathbb{Z}[x]/((x^2 + rx + s)) \cong \mathbb{Z}\left[\frac{-r+\sqrt{D}}{2}\right]$$

and since $r \equiv D \pmod 2$, we have $\mathbb{Z}\left[\dfrac{-r+\sqrt{D}}{2}\right] = \mathbb{Z}\left[\dfrac{D+\sqrt{D}}{2}\right]$.

Definition 6.3.3. Let $S(D)$ be a quadratic ring. A basis $\langle 1, \tau \rangle$ of S is **positively oriented** if $\pi(\tau) > 0$. If I be a $S(D)$-submodule of $K = S \otimes \mathbb{Q}$ having rank 2 as a $\mathbb{Z}$-module, then a $\mathbb{Z}$-basis $\langle \alpha, \beta \rangle$ of I is **positively oriented** if the change-of-basis matrix from the positively oriented basis $\langle 1, \tau \rangle$ to $\langle \alpha, \beta \rangle$ has positive determinant.

A $\mathbb{Z}$-basis of I that is not positively oriented is called **negatively oriented**.

Proposition 6.3.4. $\langle \alpha, \beta \rangle$ is positively oriented if and only if $\pi(\alpha'\beta) > 0$.

Proof. Let $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_{2\times 2}(\mathbb{Z})$ be such that $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 \\ \tau \end{pmatrix} = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$. Then

$$\begin{aligned} \pi(\alpha'\beta) &= \frac{\alpha'\beta - \alpha\beta'}{\sqrt{D}} \\ &= \frac{(a + b\tau')(c + d\tau) - (a + b\tau)(c + d\tau')}{\sqrt{D}} \\ &= \frac{(ad - bc)(\tau - \tau')}{\sqrt{D}} \end{aligned}$$

Since $\pi(\tau) > 0$, $\pi(\alpha'\beta)$ is positive if and only if $ad - bc > 0$.

Definition 6.3.5. A quadratic ring is **non-degenerate** if it's discriminant is nonzero. The six spaces introduced is nondegenerate if the discriminant is nonzero.

6.4 Isomorphism between triple of ideals and cubes

Theorem 6.4.1. There is a bijection between the set of non-degenerate Γ-equivalence classes of cubes and the set of equivalence classes of pairs $(S, (I_1, I_2, I_3))$ where S 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. We will construct an explicit bijection $\Phi : S \to Cl$.

Let $(S, (I_1, I_2, I_3))$ be such a pair. Let $\langle 1, \tau \rangle$ be a positively oriented basis 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 $1 \pmod 4$ respectively. Let $\langle \alpha_1, \alpha_2 \rangle$, $\langle \beta_1, \beta_2 \rangle$ and $\langle \gamma_1, \gamma_2 \rangle$ be the $\mathbb{Z}$-bases of I_1, I_2 and I_3 respectively, where for each $j \in \{1, 2, 3\}$, the basis is positively oriented if $\operatorname{sgn}(I_j) = 1$ and negatively oriented if $\operatorname{sgn}(I_j) = -1$. Since $I_1 I_2 I_3$ is contained in S, we can write

$$\alpha_i \beta_j \gamma_k = c_{i,j,k} + a_{i,j,k}\tau \tag{5}$$

for $1 \le i, j, k \le 2$. Define the cube X by

$$(a_{1,1,1}, a_{1,2,1}, a_{1,1,2}, a_{1,2,2}, a_{2,1,1}, a_{2,2,1}, a_{2,1,2}, a_{2,2,2}). \tag{6}$$

If $\langle \alpha_1', \alpha_2' \rangle$, $\langle \beta_1', \beta_2' \rangle$ and $\langle \gamma_1', \gamma_2' \rangle$ is another triple of positively oriented 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. A direct computation shows that the cube X' obtained from the new bases can be obtained from X via the action of (M_1, M_2, M_3).

Lemma 6.4.2. Let (I_1, I_2, I_3) and (I_1', I_2', I_3') be equivalent triples. Then $\Phi(S, (I_1, I_2, I_3)) = \Phi(S, (I_1', I_2', I_3'))$.

Proof. There exists $x_1, x_2, x_3 \in K$, with $N(x_1 x_2 x_3) = 1$, such that $I_j' = x_j I$ for $j \in \{1, 2, 3\}$. Then $\langle x_1\alpha_1, x_1\alpha_2 \rangle, \langle x_2\beta_1, x_2\beta_2 \rangle$ and $\langle x_3\gamma_1, x_3\gamma_2 \rangle$ are bases for I_1', I_2' and I_3' respectively. For $i \in \{1, 2, 3\}$, let $M \in SL_2(\mathbb{Q})$ be such that

$$M \begin{pmatrix} \alpha_1 \\ \alpha_2 \end{pmatrix} = \begin{pmatrix} x_1\alpha_1 \\ x_2\alpha_2 \end{pmatrix}.$$

Since α_1 and α_2 are linearly independent, M is also the matrix representing φ_{x_i}.

We now show that Φ is a bijection. 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 a cube. We first show that the ring S is determined by X. By Corollary, it suffices to show that the discriminant of S is determined by X.

Lemma 6.4.3. The cube X obtained from (S, I_1, I_2, I_3) via equation (5) satisfies

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

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

Now suppose that I_1 is a general fractional ideal of S 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 $(M, I_{2\times 2}, I_{2\times 2})$. The quadratic form Q_2^X (or Q_3^X) is multiplied by a factor of $\det(X) = N(I_1)$ by (cite here). Thus the discriminant of X is multiplied by a factor of $N(I_1)^2$. The same argument applies for I_2 and I_3. Thus we have proved that the equality holds for arbitrary I_1, I_2, I_3.

With the additional restriction that $N(I_1)N(I_2)N(I_3) = 1$, we have

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

so the ring S is determined by X.

Since multiplication in the ring S is associative and commutative, we have

$$[\alpha_i\beta_j\gamma_k]\cdot[\alpha_{i'}\beta_{j'}\gamma_{k'}] = [\alpha_{i'}\beta_j\gamma_k]\cdot[\alpha_i\beta_{j'}\gamma_{k'}] = [\alpha_i\beta_{j'}\gamma_k]\cdot[\alpha_{i'}\beta_j\gamma_{k'}] = [\alpha_i\beta_j\gamma_{k'}]\cdot[\alpha_{i'}\beta_{j'}\gamma_k] \quad (7)$$

for $1 \le i, i', j', k, k' \le 2$. Equating these identities using (5), 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 solution given by

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

with $\{i, i'\} = \{j, j'\} = \{k, k'\} = \{1, 2\}$ and $\epsilon = 0$ or 1 depending on whether $D \equiv 0$ or $1 \pmod 4$. An algorithm for solving the system and proving that the resulting solution is integral is given in the appendix. Thus we conclude that the c_{ijk} in (5) are uniquely determined by X.

Next, to prove that the pairs (α_1, α_2), (β_1, β_2) and (γ_1, γ_2) are uniquely determined up to a nonzero scaling factor in K, it suffices to prove that $\frac{\alpha_1}{\alpha_2}$, $\frac{\beta_1}{\beta_2}$ and $\frac{\gamma_1}{\gamma_2}$ are uniquely determined. The fact that $\frac{\alpha_1}{\alpha_2}$ is uniquely determined follows directly from

$$\begin{aligned} \alpha_1\beta_1\gamma_1(c_{2,1,1} + a_{2,1,1}\tau) &= \alpha_2\beta_1\gamma_1(c_{1,1,1} + a_{1,1,1}\tau) \\ \implies \frac{\alpha_1}{\alpha_2} &= \frac{c_{1,1,1} + a_{1,1,1}\tau}{c_{2,1,1} + a_{2,1,1}\tau}. \end{aligned}$$

and similar arguments apply to $\frac{\beta_1}{\beta_2}$ and $\frac{\gamma_1}{\gamma_2}$. With the restriction that $N(I_1)N(I_2)N(I_3) = 1$, the pair (γ_1, γ_2) is completed determined by (α_1, α_2) and (β_1, β_2). 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 $I_3 = \langle \gamma_1, \gamma_2 \rangle$ are ideals of S. Let Q_1^X, Q_2^X and Q_3^X be the three binary quadratic forms associated to X and write $Q_i^X = p_i x^2 + q_i xy + r_i y^2$ for $i \in \{1, 2, 3\}$. Then from Definition 6.1.4, the coefficients of Q_i^X can be written in terms of the coefficients of the 8 vertices of X. Since $c_{i,j,k}$ can also be written in terms of the $a_{i,j,k}$, an explicit computation in terms of the $a_{i,j,k}$ reveals that we have the following two equalities

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

which reduces to

$$\tau \cdot \alpha_1 = \frac{q_1 + \epsilon}{2} \cdot \alpha_1 + p_1 \cdot \alpha_2 \tag{8}$$

$$-\tau \cdot \alpha_2 = r_1 \cdot \alpha_1 + \frac{q_1 - \epsilon}{2} \cdot \alpha_2. \tag{9}$$

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. In both the cases of $D \equiv 0 \pmod 4$ and $D \equiv 1 \pmod 4$, $(q_1 + \epsilon)/2$ is an integer so we conclude that I_1, I_2 and I_3 are indeed ideals of S.

Definition 6.4.4. A balanced triple (I_1, I_2, I_3) of ideals of S is **projective** if I_1, I_2 and I_3 are projective ideals.

Proposition 6.4.5. *Let J be a projective ideal of S. Then every S-linear map from J to S is of the form $x \mapsto \alpha x$ for some $\alpha \in K$.*

Lemma 6.4.6. *$J \otimes_S K \cong S \otimes_S K \cong K$ as K-modules.*

Proof. To prove that $S \otimes_S K \cong K$ as K-modules, observe that the map $\psi : S \otimes_S K \to K$ given by

$$\psi((s, k)) = s \cdot k$$

is a surjective K-module homomorphism. To show that ψ is injective, let $(s, k) \in \ker(\psi)$. Then $s \cdot k = 0_K \implies (s, k) = (1_S, s \cdot k) = (1_S, 0_K) = 0_{S \otimes_S K}$. Thus ψ is injective.

Since J has full rank, S/J is finite. Consider the short exact sequence

$$0 \longrightarrow J \longrightarrow S \longrightarrow S/J \longrightarrow 0.$$

Since $K = S \otimes_{\mathbb{Z}} \mathbb{Q}$ is the localisation of S, it is flat as an S-module. Then we get the short exact sequence

$$0 \longrightarrow J \otimes_S K \longrightarrow S \otimes_S K \longrightarrow S/J \otimes_S K \longrightarrow 0.$$

But S/J is finite. Let $n = |S/J|$. Then for any $(s', (s, q)) \in S/J \otimes_S K$, we have $(s', (s, q)) = (s', (ns, q/n)) = (ns', (s, q/n)) = (0_{S/J}, (s, q/n))$. Thus $S/J \otimes_S K$ is the trivial ring so $J \otimes_S K \cong S \otimes_S K$ as K-modules.

Proof. Let $f : J \to S$ be a S-module homomorphism. Then $f \otimes_S \mathrm{id} : J \otimes_S K \to S \otimes_S K$ is a K-module homomorphism $J \otimes_S K$ to $S \otimes_S K$.

Theorem 6.4.7. The set of projective fractional ideals of S is an abelian group under ideal multiplication.

Proof. Associativity and commutativity of ideal multiplication follows directly from associativity and commutativity of ideal multiplication in the ring S.

It remains to show that the product of projective ideals must also be projective (i.e. the group operation is closed) and that every projective ideal of S is invertible. But it is clear that the product of invertible ideals is necessarily invertible. Thus it suffices to show that an ideal of S is projective if and only if it is invertible.

Let J be an invertible ideal of S. Since $JJ^{-1} = S$, there exists $a_1, \cdots, a_n \in J$ and $b_1 \cdots, b_n \in J^{-1}$ such that $a_1b_1 + \cdots + a_nb_n = 1_S$. Then for any $x \in J$, we have

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

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

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

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

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

Then for any $y \in J$,

$$\varphi \circ \psi(y) = \varphi\left(\sum_{i=1}^{n} (yb_i) \cdot e_i \right) = \sum_{i=1}^{n} yb_ia_i = y.$$

so φ splits. Thus J is isomorphic to a direct summand of the free module F so it is projective.

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 canonical 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 hat

$$\begin{aligned}w &= [Ax_1 + (b_B + \tau)y_1][A'x_2 + (b_B + \tau)y_2]\\ &= AA'x_1x_2 + (b_B + \tau)(Ax_1y_2 + A'x_2y_1) + (b_B^2 + 2b_B\tau + \tau^2)y_1y_2\\ &= AA'x_1x_2 + b_BAx_1y_2 + b_BA'x_2y_1 + b_B^2y_1y_2 + \tau^2y_1y_2\\ &\quad+ \tau(Ax_1y_2 + A'x_2y_1 + 2b_By_1y_2).\end{aligned}$$

If $D \equiv 0 \pmod 4$, then

$$\begin{aligned}w &= AA'x_1x_2 + b_BAx_1y_2 + b_BA'x_2y_1 + b_B^2y_1y_2 + \frac{Dy_1y_2}{4}\\ &\quad+ \tau(Ax_1y_2 + A'x_2y_1 + 2b_By_1y_2).\end{aligned}$$

and so $Ax_1y_2 + A'x_2y_1 + 2b_By_1y_2 = 0$. We have

$$\begin{aligned}w &= AA'x_1x_2 + b_B(Ax_1y_2 + A'x_2y_1 + b_By_1y_2) + \frac{Dy_1y_2}{4}\\ &= AA'x_1x_2 - b_B^2y_1y_2 + \frac{Dy_1y_2}{4}\\ &= AA'x_1x_2 - y_1y_2\bigg(\frac{B^2 - D}{4}\bigg).\end{aligned}$$

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

$$\begin{aligned}w &= AA'x_1x_2 + b_BAx_1y_2 + b_BA'x_2y_1 + b_B^2y_1y_2 + \frac{(D-1)y_1y_2}{4}\\ &\quad+ \tau(Ax_1y_2 + A'x_2y_1 + 2b_By_1y_2 + y_1y_2).\end{aligned}$$

so $Ax_1y_2 + A'x_2y_1 + 2b_By_1y_2 + y_1y_2 = 0$. We have

$$\begin{aligned} w &= AA'x_1x_2 + b_B(Ax_1y_2 + A'x_2y_1 + b_By_1y_2) + \frac{(D-1)y_1y_2}{4} \\ &= AA'x_1x_2 - b_B^2y_1y_2 - b_By_1y_2 + \frac{(D-1)y_1y_2}{4} \\ &= AA'x_1x_2 - y_1y_2\left(\left(b_B + \frac{1}{2}\right)^2 - \frac{D}{4}\right) \\ &= AA'x_1x_2 - y_1y_2\left(\frac{B^2-D}{4}\right). \end{aligned}$$

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

$$\left\{AA', \ \frac{A(B-1)}{2} + A\tau \ , \ \frac{A'(B-1)}{2} + A'\tau \ , \ \left(\frac{B-1}{2}\right)^2 - \frac{1-D}{4} + B\tau\right\}$$

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

$$\begin{aligned} y + \delta = AA'x_1x_2 &+ b_BAx_1y_2 + b_BA'x_2y_1 + b_B^2y_1y_2 + \tau^2y_1y_2 \\ &+ \tau(Ax_1y_2 + A'x_2y_1 + 2b_By_1y_2) \end{aligned}$$

If $D \equiv 0 \pmod 4$, then $Ax_1y_2 + A'x_2y_1 + 2b_By_1y_2 = 1$ and we have

$$\begin{aligned} y &= AA'x_1x_2 + b_B(Ax_1y_2 + A'x_2y_1 + b_By_1y_2) + \frac{Dy_1y_2}{4} \\ &= AA'x_1x_2 + b_B - b_B^2y_1y_2 + \frac{Dy_1y_2}{4} \\ &= AA'x_1x_2 + b_B - y_1y_2\left(\frac{B^2-D}{4}\right). \end{aligned}$$

If $D \equiv 1 \pmod 4$, then $Ax_1y_2 + A'x_2y_1 + 2b_By_1y_2 + y_1y_2 = 1$.

$$\begin{aligned} y &= AA'x_1x_2 + b_B(Ax_1y_2 + A'x_2y_1 + b_By_1y_2) + \frac{(D-1)y_1y_2}{4} \\ &= AA'x_1x_2 + b_B - b_B^2y_1y_2 - b_By_1y_2 + \frac{(D-1)y_1y_2}{4} \\ &= AA'x_1x_2 + b_B - y_1y_2\left(\frac{B^2-D}{4}\right). \end{aligned}$$

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 (7), 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

$$0c_{1,1,1}c_{2,2,2}+\frac{D}{4}(a_{1,1,1}a_{2,2,2}) = c_{2,1,1}c_{1,2,2}+\frac{D}{4}(a_{2,1,1}a_{1,2,2}) \tag{10}$$

$$c_{1,1,1}a_{2,2,2}+c_{2,2,2}a_{1,1,1} = c_{2,1,1}a_{1,2,2}+c_{1,2,2}a_{2,1,1} \tag{11}$$

$$c_{1,1,1}c_{2,2,2}+\frac{D}{4}(a_{1,1,1}a_{2,2,2}) = c_{1,2,1}c_{2,1,2}+\frac{D}{4}(a_{1,2,1}a_{2,1,2}) \tag{12}$$

$$c_{1,1,1}a_{2,2,2}+c_{2,2,2}a_{1,1,1} = c_{1,2,1}a_{2,1,2}+c_{2,1,2}a_{1,2,1} \tag{13}$$

$$c_{1,1,1}c_{2,2,2}+\frac{D}{4}(a_{1,1,1}a_{2,2,2}) = c_{1,1,2}c_{2,2,1}+\frac{D}{4}(a_{1,1,2}a_{2,2,1}) \tag{14}$$

$$c_{1,1,1}a_{2,2,2}+c_{2,2,2}a_{1,1,1} = c_{1,1,2}a_{2,2,1}+c_{2,2,1}a_{1,1,2} \tag{15}$$

$$c_{1,1,1}c_{1,2,2}+\frac{D}{4}(a_{1,1,1}a_{1,2,2}) = c_{1,2,1}c_{1,1,2}+\frac{D}{4}(a_{1,2,1}a_{1,1,2}) \tag{16}$$

$$c_{1,1,1}a_{1,2,2}+c_{1,2,2}a_{1,1,1} = c_{1,2,1}a_{1,1,2}+c_{1,1,2}a_{1,2,1} \tag{17}$$

$$c_{2,1,1}c_{2,2,2}+\frac{D}{4}(a_{2,1,1}a_{2,2,2}) = c_{2,2,}c_{2,1,2}+\frac{D}{4}(a_{2,2,1}a_{2,1,2}) \tag{18}$$

$$c_{2,1,1}a_{2,2,2}+c_{2,2,2}a_{2,1,1} = c_{2,2,1}a_{2,1,2}+c_{2,1,2}a_{2,2,1} \tag{19}$$

$$c_{1,1,1}c_{2,1,2}+\frac{D}{4}(a_{1,1,1}a_{2,1,2}) = c_{2,1,1}c_{1,1,2}+\frac{D}{4}(a_{2,1,1}a_{1,1,2}) \tag{20}$$

$$c_{1,1,1}a_{2,1,2}+c_{2,1,2}a_{1,1,1} = c_{2,1,1}a_{1,1,2}+c_{1,1,2}a_{2,1,1} \tag{21}$$

$$c_{1,2,1}c_{2,2,2}+\frac{D}{4}(a_{1,2,1}a_{2,2,2}) = c_{2,2,1}c_{1,2,2}+\frac{D}{4}(a_{2,2,1}a_{1,2,2}) \tag{22}$$

$$c_{1,2,1}a_{2,2,2}+c_{2,2,2}a_{1,2,1} = c_{2,2,1}a_{1,2,2}+c_{1,2,2}a_{2,2,1} \tag{23}$$

$$c_{1,1,1}c_{2,2,1} + \frac{D}{4}(a_{1,1,1}a_{2,2,1}) = c_{2,1,1}c_{1,2,1} + \frac{D}{4}(a_{2,1,1}a_{1,2,1}) \tag{24}$$

$$c_{1,1,1}a_{2,2,1} + c_{2,2,1}a_{1,1,1} = c_{2,1,1}a_{1,2,1} + c_{1,2,1}a_{2,1,1} \tag{25}$$

$$c_{1,1,2}c_{2,2,2} + \frac{D}{4}(a_{1,1,2}a_{2,2,2}) = c_{2,1,2}c_{1,2,2} + \frac{D}{4}(a_{2,1,2}a_{1,2,2}) \tag{26}$$

$$c_{1,1,2}a_{2,2,2} + c_{2,2,2}a_{1,1,2} = c_{2,1,2}a_{1,2,2} + c_{1,2,2}a_{2,1,2} \tag{27}$$

$$a'h' - e'd' = \frac{D}{4}(ed - ah) \tag{28}$$

$$a'h - d'e - e'd + h'a = 0 \tag{29}$$

$$a'h' - b'g' = \frac{D}{4}(bg - ah) \tag{30}$$

$$a'h - b'g - g'b + h'a = 0 \tag{31}$$

$$a'h' - c'f' = \frac{D}{4}(cf - ah) \tag{32}$$

$$a'h - c'f - f'c + h'a = 0 \tag{33}$$

$$a'd' - b'c' = \frac{D}{4}(bc - ad) \tag{34}$$

$$a'd - b'c - c'b + d'a = 0 \tag{35}$$

$$e'h' - f'g' = \frac{D}{4}(fg - eh) \tag{36}$$

$$e'h - f'g - g'f + h'e = 0 \tag{37}$$

$$a'g' - c'e' = \frac{D}{4}(ce - ag) \tag{38}$$

$$a'g - c'e - e'c + g'a = 0 \tag{39}$$

$$b'h' - d'f' = \frac{D}{4}(df - bh) \tag{40}$$

$$b'h - d'f - f'd + h'b = 0 \tag{41}$$

$$a'f' - b'e' = \frac{D}{4}(be - af) \tag{42}$$

$$a'f - b'e - e'b + f'a = 0 \tag{43}$$

$$c'h' - d'g' = \frac{D}{4}(dg - ch) \tag{44}$$

$$c'h - d'g - g'd + h'c = 0 \tag{45}$$

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

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

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

$$\begin{aligned}
&(c_{1,1,1} + a_{1,1,1}\tau)(c_{2,2,2} + a_{2,2,2}\tau) = (c_{2,1,1} + a_{2,1,1}\tau)(c_{1,2,2} + a_{1,2,2}\tau)\\
&\implies c_{1,1,1}c_{2,2,2} + \frac{D}{4}(a_{1,1,1}a_{2,2,2}) = c_{2,1,1}c_{1,2,2} + \frac{D}{4}(a_{2,1,1}a_{1,2,2})\\
&\qquad c_{1,1,1}a_{2,2,2} + c_{2,2,2}a_{1,1,1} = c_{2,1,1}a_{1,2,2} + c_{1,2,2}a_{2,1,1}
\end{aligned}$$

$$\begin{aligned}
&(c_{1,1,1} + a_{1,1,1}\tau)(c_{2,2,2} + a_{2,2,2}\tau) = (c_{1,2,1} + a_{1,2,1}\tau)(c_{2,1,2} + a_{2,1,2}\tau)\\
&\implies c_{1,1,1}c_{2,2,2} + \frac{D}{4}(a_{1,1,1}a_{2,2,2}) = c_{1,2,1}c_{2,1,2} + \frac{D}{4}(a_{1,2,1}a_{2,1,2})\\
&\qquad c_{1,1,1}a_{2,2,2} + c_{2,2,2}a_{1,1,1} = c_{1,2,1}a_{2,1,2} + c_{2,1,2}a_{1,2,1}
\end{aligned}$$

$$\begin{aligned}
&(c_{1,1,1} + a_{1,1,1}\tau)(c_{2,2,2} + a_{2,2,2}\tau) = (c_{1,1,2} + a_{1,1,2}\tau)(c_{2,2,1} + a_{2,2,1}\tau)\\
&\implies c_{1,1,1}c_{2,2,2} + \frac{D}{4}(a_{1,1,1}a_{2,2,2}) = c_{1,1,2}c_{2,2,1} + \frac{D}{4}(a_{1,1,2}a_{2,2,1})\\
&\qquad c_{1,1,1}a_{2,2,2} + c_{2,2,2}a_{1,1,1} = c_{1,1,2}a_{2,2,1} + c_{2,2,1}a_{1,1,2}
\end{aligned}$$

$$\begin{aligned}
&(c_{1,1,1} + a_{1,1,1}\tau)(c_{1,2,2} + a_{1,2,2}\tau) = (c_{1,2,1} + a_{1,2,1}\tau)(c_{1,1,2} + a_{1,1,2}\tau)\\
&\implies c_{1,1,1}c_{1,2,2} + \frac{D}{4}(a_{1,1,1}a_{1,2,2}) = c_{1,2,1}c_{1,1,2} + \frac{D}{4}(a_{1,2,1}a_{1,1,2})\\
&\qquad c_{1,1,1}a_{1,2,2} + c_{1,2,2}a_{1,1,1} = c_{1,2,1}a_{1,1,2} + c_{1,1,2}a_{1,2,1}
\end{aligned}$$

$$\begin{aligned}(c_{2,1,1}+a_{2,1,1}\tau)(c_{2,2,2}+a_{2,2,2}\tau) &= (c_{2,2,1}+a_{2,2,1}\tau)(c_{2,1,2}+a_{2,1,2}\tau)\\ \implies c_{2,1,1}c_{2,2,2}+\frac{D}{4}(a_{2,1,1}a_{2,2,2}) &= c_{2,2,}c_{2,1,2}+\frac{D}{4}(a_{2,2,1}a_{2,1,2})\\ c_{2,1,1}a_{2,2,2}+c_{2,2,2}a_{2,1,1} &= c_{2,2,1}a_{2,1,2}+c_{2,1,2}a_{2,2,1}\end{aligned}$$

$$\begin{aligned}(c_{1,1,1}+a_{1,1,1}\tau)(c_{2,1,2}+a_{2,1,2}\tau) &= (c_{2,1,1}+a_{2,1,1}\tau)(c_{1,1,2}+a_{1,1,2}\tau)\\ \implies c_{1,1,1}c_{2,1,2}+\frac{D}{4}(a_{1,1,1}a_{2,1,2}) &= c_{2,1,1}c_{1,1,2}+\frac{D}{4}(a_{2,1,1}a_{1,1,2})\\ c_{1,1,1}a_{2,1,2}+c_{2,1,2}a_{1,1,1} &= c_{2,1,1}a_{1,1,2}+c_{1,1,2}a_{2,1,1}\end{aligned}$$

$$\begin{aligned}(c_{1,2,1}+a_{1,2,1}\tau)(c_{2,2,2}+a_{2,2,2}\tau) &= (c_{2,2,1}+a_{2,2,1}\tau)(c_{1,2,2}+a_{1,2,2}\tau)\\ \implies c_{1,2,1}c_{2,2,2}+\frac{D}{4}(a_{1,2,1}a_{2,2,2}) &= c_{2,2,1}c_{1,2,2}+\frac{D}{4}(a_{2,2,1}a_{1,2,2})\\ c_{1,2,1}a_{2,2,2}+c_{2,2,2}a_{1,2,1} &= c_{2,2,1}a_{1,2,2}+c_{1,2,2}a_{2,2,1}\end{aligned}$$

$$\begin{aligned}(c_{1,1,1}+a_{1,1,1}\tau)(c_{2,2,1}+a_{2,2,1}\tau) &= (c_{2,1,1}+a_{2,1,1}\tau)(c_{1,2,1}+a_{1,2,1}\tau)\\ \implies c_{1,1,1}c_{2,2,1}+\frac{D}{4}(a_{1,1,1}a_{2,2,1}) &= c_{2,1,1}c_{1,2,1}+\frac{D}{4}(a_{2,1,1}a_{1,2,1})\\ c_{1,1,1}a_{2,2,1}+c_{2,2,1}a_{1,1,1} &= c_{2,1,1}a_{1,2,1}+c_{1,2,1}a_{2,1,1}\end{aligned}$$

$$\begin{aligned}(c_{1,1,2}+a_{1,1,2}\tau)(c_{2,2,2}+a_{2,2,2}\tau) &= (c_{2,1,2}+a_{2,1,2}\tau)(c_{1,2,2}+a_{1,2,2}\tau)\\ \implies c_{1,1,2}c_{2,2,2}+\frac{D}{4}(a_{1,1,2}a_{2,2,2}) &= c_{2,1,2}c_{1,2,2}+\frac{D}{4}(a_{2,1,2}a_{1,2,2})\\ c_{1,1,2}a_{2,2,2}+c_{2,2,2}a_{1,1,2} &= c_{2,1,2}a_{1,2,2}+c_{1,2,2}a_{2,1,2}\end{aligned}$$

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 $D \equiv 1 \pmod 4$, $\tau^2 - \tau + \frac{1-D}{4} = 0 \implies \tau^2 = \tau - \frac{1-D}{4}$

$$\begin{aligned}
(c_{1,1,1} + a_{1,1,1}\tau)(c_{2,2,2} + a_{2,2,2}\tau) &= (c_{2,1,1} + a_{2,1,1}\tau)(c_{1,2,2} + a_{1,2,2}\tau) \\
\implies c_{1,1,1}c_{2,2,2} + \frac{D-1}{4}(a_{1,1,1}a_{2,2,2}) &= c_{2,1,1}c_{1,2,2} + \frac{D-1}{4}(a_{2,1,1}a_{1,2,2}) \\
c_{1,1,1}a_{2,2,2} + c_{2,2,2}a_{1,1,1} + a_{1,1,1}a_{2,2,2} &= c_{2,1,1}a_{1,2,2} + c_{1,2,2}a_{2,1,1} + a_{2,1,1}a_{1,2,2}
\end{aligned}$$

$$\begin{aligned}
(c_{1,1,1} + a_{1,1,1}\tau)(c_{2,2,2} + a_{2,2,2}\tau) &= (c_{1,2,1} + a_{1,2,1}\tau)(c_{2,1,2} + a_{2,1,2}\tau) \\
\implies c_{1,1,1}c_{2,2,2} + \frac{D-1}{4}(a_{1,1,1}a_{2,2,2}) &= c_{1,2,1}c_{2,1,2} + \frac{D-1}{4}(a_{1,2,1}a_{2,1,2}) \\
c_{1,1,1}a_{2,2,2} + c_{2,2,2}a_{1,1,1} + a_{1,1,1}a_{2,2,2} &= c_{1,2,1}a_{2,1,2} + c_{2,1,2}a_{1,2,1} + a_{1,2,1}a_{2,1,2}
\end{aligned}$$

$$\begin{aligned}
(c_{1,1,1} + a_{1,1,1}\tau)(c_{2,2,2} + a_{2,2,2}\tau) &= (c_{1,1,2} + a_{1,1,2}\tau)(c_{2,2,1} + a_{2,2,1}\tau) \\
\implies c_{1,1,1}c_{2,2,2} + \frac{D-1}{4}(a_{1,1,1}a_{2,2,2}) &= c_{1,1,2}c_{2,2,1} + \frac{D-1}{4}(a_{1,1,2}a_{2,2,1}) \\
c_{1,1,1}a_{2,2,2} + c_{2,2,2}a_{1,1,1} + a_{1,1,1}a_{2,2,2} &= c_{1,1,2}a_{2,2,1} + c_{2,2,1}a_{1,1,2} + a_{1,1,2}a_{2,2,1}
\end{aligned}$$

$$\begin{aligned}
(c_{1,1,1} + a_{1,1,1}\tau)(c_{1,2,2} + a_{1,2,2}\tau) &= (c_{1,2,1} + a_{1,2,1}\tau)(c_{1,1,2} + a_{1,1,2}\tau) \\
\implies c_{1,1,1}c_{1,2,2} + \frac{D-1}{4}(a_{1,1,1}a_{1,2,2}) &= c_{1,2,1}c_{1,1,2} + \frac{D-1}{4}(a_{1,2,1}a_{1,1,2}) \\
c_{1,1,1}a_{1,2,2} + c_{1,2,2}a_{1,1,1} + a_{1,1,1}a_{1,2,2} &= c_{1,2,1}a_{1,1,2} + c_{1,1,2}a_{1,2,1} + a_{1,2,1}a_{1,1,2}
\end{aligned}$$

$$\begin{aligned}
(c_{2,1,1} + a_{2,1,1}\tau)(c_{2,2,2} + a_{2,2,2}\tau) &= (c_{2,2,1} + a_{2,2,1}\tau)(c_{2,1,2} + a_{2,1,2}\tau) \\
\implies c_{2,1,1}c_{2,2,2} + \frac{D-1}{4}(a_{2,1,1}a_{2,2,2}) &= c_{2,2,1}c_{2,1,2} + \frac{D-1}{4}(a_{2,2,1}a_{2,1,2}) \\
c_{2,1,1}a_{2,2,2} + c_{2,2,2}a_{2,1,1} + a_{2,1,1}a_{2,2,2} &= c_{2,2,1}a_{2,1,2} + c_{2,1,2}a_{2,2,1} + a_{2,2,1}a_{2,1,2}
\end{aligned}$$

$$\begin{aligned}
(c_{1,1,1} + a_{1,1,1}\tau)(c_{2,1,2} + a_{2,1,2}\tau) &= (c_{2,1,1} + a_{2,1,1}\tau)(c_{1,1,2} + a_{1,1,2}\tau) \\
\implies c_{1,1,1}c_{2,1,2} + \frac{D-1}{4}(a_{1,1,1}a_{2,1,2}) &= c_{2,1,1}c_{1,1,2} + \frac{D-1}{4}(a_{2,1,1}a_{1,1,2}) \\
c_{1,1,1}a_{2,1,2} + c_{2,1,2}a_{1,1,1} + a_{1,1,1}a_{2,1,2} &= c_{2,1,1}a_{1,1,2} + c_{1,1,2}a_{2,1,1} + a_{2,1,1}a_{1,1,2}
\end{aligned}$$

$$\begin{aligned}
(c_{1,2,1} + a_{1,2,1}\tau)(c_{2,2,2} + a_{2,2,2}\tau) &= (c_{2,2,1} + a_{2,2,1}\tau)(c_{1,2,2} + a_{1,2,2}\tau) \\
\implies c_{1,2,1}c_{2,2,2} + \frac{D-1}{4}(a_{1,2,1}a_{2,2,2}) &= c_{2,2,1}c_{1,2,2} + \frac{D-1}{4}(a_{2,2,1}a_{1,2,2}) \\
c_{1,2,1}a_{2,2,2} + c_{2,2,2}a_{1,2,1} + a_{1,2,1}a_{2,2,2} &= c_{2,2,1}a_{1,2,2} + c_{1,2,2}a_{2,2,1} + a_{2,2,1}a_{1,2,2}
\end{aligned}$$

$$
\begin{aligned}
&(c_{1,1,1} + a_{1,1,1}\tau)(c_{2,2,1} + a_{2,2,1}\tau) = (c_{2,1,1} + a_{2,1,1}\tau)(c_{1,2,1} + a_{1,2,1}\tau)\\
\implies &c_{1,1,1}c_{2,2,1} + \frac{D-1}{4}(a_{1,1,1}a_{2,2,1}) = c_{2,1,1}c_{1,2,1} + \frac{D-1}{4}(a_{2,1,1}a_{1,2,1})\\
&c_{1,1,1}a_{2,2,1} + c_{2,2,1}a_{1,1,1} + a_{1,1,1}a_{2,2,1} = c_{2,1,1}a_{1,2,1} + c_{1,2,1}a_{2,1,1} + a_{2,1,1}a_{1,2,1}
\end{aligned}
$$

$$
\begin{aligned}
&(c_{1,1,2} + a_{1,1,2}\tau)(c_{2,2,2} + a_{2,2,2}\tau) = (c_{2,1,2} + a_{2,1,2}\tau)(c_{1,2,2} + a_{1,2,2}\tau)\\
\implies &c_{1,1,2}c_{2,2,2} + \frac{D-1}{4}(a_{1,1,2}a_{2,2,2}) = c_{2,1,2}c_{1,2,2} + \frac{D-1}{4}(a_{2,1,2}a_{1,2,2})\\
&c_{1,1,2}a_{2,2,2} + c_{2,2,2}a_{1,1,2} + a_{1,1,2}a_{2,2,2} = c_{2,1,2}a_{1,2,2} + c_{1,2,2}a_{2,1,2} + a_{2,1,2}a_{1,2,2}
\end{aligned}
$$

$$a'h' - e'd' = \frac{D-1}{4}(ed - ah) \tag{46}$$
$$a'h - d'e - e'd + h'a = de - ah \tag{47}$$

$$a'h' - b'g' = \frac{D-1}{4}(bg - ah) \tag{48}$$
$$a'h - b'g - g'b + h'a = bg - ah \tag{49}$$

$$a'h' - c'f' = \frac{D-1}{4}(cf - ah) \tag{50}$$
$$a'h - c'f - f'c + h'a = cf - ah \tag{51}$$

$$a'd' - b'c' = \frac{D-1}{4}(bc - ad) \tag{52}$$
$$a'd - b'c - c'b + d'a = bc - ad \tag{53}$$

$$e'h' - f'g' = \frac{D-1}{4}(fg - eh) \tag{54}$$
$$e'h - f'g - g'f + h'e = fg - eh \tag{55}$$

$$a'g' - c'e' = \frac{D-1}{4}(ce - ag) \tag{56}$$
$$a'g - c'e - e'c + g'a = ce - ag \tag{57}$$

$$b'h' - d'f' = \frac{D-1}{4}(df - bh) \tag{58}$$
$$b'h - d'f - f'd + h'b = df - bh \tag{59}$$

$$a'f' - b'e' = \frac{D-1}{4}(be - af) \tag{60}$$
$$a'f - b'e - e'b + f'a = be - af \tag{61}$$

$$c'h' - d'g' = \frac{D-1}{4}(dg - ch) \tag{62}$$
$$c'h - d'g - g'd + h'c = dg - ch \tag{63}$$