Abstract

This is a self-contained notes on the theory of class groups. We develop the theory of ideal class group and class group of binary quadratic forms. We end by showing the isomorphism of the two notions of class groups.

1 A Crash Course in Rings and Modules

1.1 Ring Theory

Definition 1.1. *A* ring $(R, +, \cdot)$ is a set R with two binary operations (addition and multiplication) satisfying the following three axioms:

(i) $(R, +)$ is an abelian group with identity element 0_R

(ii) The operation $\cdot$ is associative., commutative and has an identity 1_R, such that $1_R \cdot a = a$, for all $a \in R$

(iii) Multiplication distributes over addition: for all $a, b, c \in R$, we have $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ and $(b + c) \cdot a = (b \cdot a) + (c \cdot a)$.

Example 1.2. $(\mathbb{Z}, +, \cdot), (\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot), (\mathbb{C}, +, \cdot)$ are all rings ($+, \cdot$ are the usual addition and multiplication).

Example 1.3. For any integer D which is not a perfect square, $\mathbb{Z}[\sqrt{D}] = \{a + b\sqrt{D} \mid a, b \in \mathbb{Z}\}$ is a ring with respect to the addition and multiplication induced by those in $\mathbb{R}$.

Remark 1.4. A ring $(R, +, \cdot)$ is called a **commutative** ring if $a \cdot b = b \cdot$ a for all $a, b \in R$ It is said to be with **identity** if there exists an element $1 \neq 0$ in R such that $1 \cdot a = a = a \cdot 1$ for all $a \in R$. This element 1 is called the **identity** of R.

Definition 1.5. A **subring** of R is a subset $S \subseteq R$ that is closed under addition, additive inverses, and multiplication. This makes S a ring in its own right under the operations inherited from R, with $1_S = 1_R$. if R is a ring with identity 1_R.

Definition 1.6. Let R be a ring. An ideal $I \subseteq R$ is an additive subgroup that absorbs multiplication: if $a \in R$ and $x \in I$, then $ax \in I$.

Example 1.7. Let $I = \mathbb{Z} \cdot 7 + \mathbb{Z}(3 + \sqrt{-5})$ Then I is an idea in $\mathbb{Z}[\sqrt{-5}]$. It suffices to check that $\sqrt{-5}I \subseteq I$, which we check on the generators:

$$\sqrt{-5} \cdot 7 = (-3) \cdot 7 + 7(3 + \sqrt{-5}) \in I$$
$$\sqrt{-5} \cdot (3 + \sqrt{-5}) = -5 + 3\sqrt{-5} = -2 \cdot 7 + 3(3 + \sqrt{-5}) \in I$$

Definition 1.8. Given rings R and S, a function $\varphi : R \to S$ is a ring homomorphism if it meets the following conditions for any $a, b \in R$:
$(a)\varphi(a + b) = \varphi(a) + \varphi(b)$
$(b)\varphi(ab) = \varphi(a)\varphi(b)$
$(c)\varphi(1_R) = 1_S$
If φ is one-to-one and onto, it is called a ring isomorphism. If an isomorphism exists between two rings R and S, we say they are isomorphic and write $R \cong S$.

Proposition 1.9. *Let I be an ideal of a ring R. The expressions*

$$(a + I) + (b + I) = (a + b) + I$$
$$(a + I)(b + I) = (ab) + I$$

are well-defined operations that make R/I into a ring. The function $\pi : R \to R/I$ defined by $\pi(a) = a + I$ is a surjective ring homomorphism.

Definition 1.10. An ideal I of R is a **principal ideal** if $I = Ra$ for some $a \in R$. Any such a is called a **generator** of I

Definition 1.11. For two ideals I and J of R, we define the following sets, each of which is itself an ideal:

$$I + J = \{x + y : x \in I, y \in J\}$$
$$I \cap J = \{x : x \in I \text{ and } x \in J\}$$
$$IJ = \left\{ \sum_{i=1}^{m} x_i y_i : x_i \in I, y_i \in J \right\}$$

Definition 1.12. If $I + J = R$, we say that I and J are **relatively prime ideals**. This happens if and only if there exist $x \in I$ and $y \in J$ with $x + y = 1$.

1.2 Module Theory

Definition 1.13. Let R be a ring (not necessarily commutative nor with 1). A left $R-$module or a left module over R is a set M together with

1. a binary operation $+$ on M under which M is an abelian group, and
2. an action of R on M (that is, a map $R \times M \to M$) denoted by rm, for all $r \in R$ and for all $m \in M$ which satisfies
   (i) $(r + s)m = rm + sm$, for all $r, s \in R, m \in M$
   (ii) $(rs)m = r(sm)$, for all $r, s \in R, m \in M$, and
   (iii) $r(m + n) = rm + rn$, for all $r \in R, m, n \in M$.
   If the ring R has a 1 we impose the additional axiom:
   (iv) $1m = m$, for all $m \in M$

Remark 1.14. The description "left" in the above definition indicates that the ring elements appear on the left; "right" $R-$modules can be defined analogously. If the ring R is commutative and M is a left $R-$module we can make M into a right $R-$module by defining $mr = rm$ for $m \in M$ and $r \in R$.

Remark 1.15. When R is a field F the axioms for an $R-$module are precisely the same as those for a vector space over F, so that modules over a field F and vector spaces over F are the same.

Definition 1.16. Let R be a ring and let M be an $R-$module. A subset N of M is a submodule of M if
(1) $N \neq \emptyset$, and
(2) $x + ry \in N$ for all $r \in R$ and for all $x, y \in N$

Example 1.17. ($\mathbb{Z}-$modules) Let R = $\mathbb{Z}$, let A be any abelian group (finite or infinite) and write the operation of A as $+$. Make A into a $\mathbb{Z}-$module as follows: for any $n \in \mathbb{Z}$ and $a \in A$ define

$$na = \begin{cases} a + a + \cdots + a (n \text{ times }) & \text{if } n > 0 \\ 0 & \text{if } n = 0 \\ -a - a - \cdots - a (-n \text{ times }) & \text{if } n < 0 \end{cases}$$

(here 0 is the identity of the additive group A). This definition of an action of the integers on A makes A into a $\mathbb{Z}$ -module, and the module axioms show that this is the only possible action of $\mathbb{Z}$ on A making it a (unital) $\mathbb{Z}$ -module. Thus every abelian group is a $\mathbb{Z}$ -module. Conversely, if M is any $\mathbb{Z}-$module, a fortiori M is an abelian group, so $\mathbb{Z}-$modules are the same as abelian groups. Furthermore, it is immediate from the definition that $\mathbb{Z}-$submodules are the same as subgroups.

Definition 1.18. Let M be an $R-$module and let $N_1, \ldots, N_n$ be submodules of M.

1. The sum of $N_1, \ldots, N_n$ is the set of all finite sums of elements from the sets N_i : $\{a_1 + a_2 + \cdots + a_n \mid a_i \in N_i \text{ for all } i\}$. Denote this sum by $N_1 + \cdots + N_n$
2. For any subset A of M let

$$RA = \left\{ r_1 a_1 + r_2 a_2 + \cdots + r_m a_m \mid r_1, \ldots, r_m \in R, a_1, \ldots, a_m \in A, m \in \mathbb{Z}^+ \right\}$$

(where by convention $RA = \{0\}$ if $A = \emptyset$). If A is the finite set $\{a_1, a_2, \ldots, a_n\}$ we shall write $Ra_1 + Ra_2 + \cdots + Ra_n$ for RA. Call RA the submodule of M generated by A. If N is a submodule of M (possibly $N = M$) and $N = RA$ for some subset A of M, we call A a set of generators or generating set for N and we say N is generated by A

3. A submodule N of M (possibly $N = M$) is finitely generated if there is some finite subset A of M such that $N = RA$, that is, if N is generated by some finite subset.

4. A submodule N of M (possibly $N = M$) is *cyc* lic if there exists an element $a \in M$ such that $N = Ra$, that is, if N is generated by one element:

$$N = Ra = \{ra \mid r \in R\}$$

Example 1.19. Let $R = \mathbb{Z}$ and let M be any $R-$module, that is, any abelian group. If $a \in M$, then $\mathbb{Z}a$ is just the cyclic subgroup of M generated by $a : \langle a \rangle$. More generally, M is generated as a $\mathbb{Z}-$module by a set A if and only if M is generated as a group by A (that is, the action of ring elements in this instance produces no elements that cannot already be obtained from A by addition and subtraction).

2 Quadratic Number Fields

Definition 2.1. A quadratic field is a field of the form

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

where $N \in \mathbb{Z}$ is not a perfect square. The field $\mathbb{Q}[\sqrt{N}]$ is called **imaginary** if $N < 0$, and **real** if $N > 0$.

Definition 2.2. Let $\alpha \in \mathbb{Q}[\sqrt{N}]$. The **conjugate** of $\alpha = a + b\sqrt{N}$ is $\bar{\alpha} = a - b\sqrt{N}$. We define the **trace** and the **norm** of α by

$$\mathrm{Tr}\,\alpha = \alpha + \bar{\alpha}, \quad \mathrm{N}\alpha = \alpha\bar{\alpha}.$$

The conjugate $\overline{I}$ of any subset $I \subseteq \mathbb{Q}[\sqrt{N}]$ is the set

$$\overline{I} = \{\overline{\alpha} \mid \alpha \in I\}.$$

Definition 2.3. Let $\alpha \in \mathbb{Q}[\sqrt{N}]$. The **minimal polynomial** of α is the least degree polynomial $f \in \mathbb{Z}[x]$ with coprime coefficients such that $f(\alpha) = 0$ and the leading coefficient of f is positive.

Definition 2.4. Let $K = \mathbb{Q}[\sqrt{N}]$ be a quadratic field. We defined an **order** $\mathcal{O}$ in K to be a subset of K such that
1. $\mathcal{O}$ is a subring of K
2. $\mathcal{O}$ is a finitely generated $\mathbb{Z}-$module,
3. $\mathcal{O}$ contains a $\mathbb{Q}-$basis of K.

Remark 2.5. Since K is a vector space over $\mathbb{Q}$, thus condition 3 in above definition makes sense.

Remark 2.6. Let $\mathcal{O}$ be an order of K. Since K as a $\mathbb{Q}-$module is generated by 1 and $\sqrt{N}$, thus $\mathcal{O}$ is also generated over $\mathbb{Z}$ (condition 2) by two elements of K, say α, β. Thus any order can be defined using the two generators. We denote $\mathcal{O} = \alpha\mathbb{Z} + \beta\mathbb{Z}$ by $[\alpha, \beta]$.

Definition 2.7. The **ring of integers** of $K = \mathbb{Q}[\sqrt{N}]$ is the set

$$\begin{aligned}\mathcal{O}_K &= \left\{\alpha \in \mathbb{Q}[\sqrt{N}] : \alpha^2 - t\alpha + n = 0 \text{ for some } t, n \in \mathbb{Z}\right\} \\ &= \{\alpha \in \mathbb{Q}[\sqrt{N}] : \mathrm{Tr}\,\alpha, \mathrm{N}\alpha \in \mathbb{Z}\}.\end{aligned}$$

Define the **discriminant** d_K of K as follows:

$$d_K = \begin{cases} N & \text{if } N \equiv 1 \bmod 4 \\ 4N & \text{otherwise} \end{cases}$$

Remark 2.8. Let $\mathbb{O}$ be the **maximal order** in K in the sense that if $\mathcal{O}$ is any other order in K then $\mathcal{O} \subseteq \mathbb{O}$. Then one can show that $\mathbb{O} = \mathcal{O}_K$.

For any order $\mathcal{O}$ of K, the **conductor** of $\mathcal{O}$ is the index $[\mathcal{O}_K : \mathcal{O}] = \frac{|O_K|}{|O|} = f$. Define the discriminant of the order $\mathcal{O} = [\alpha, \beta]$ to be

$$D(\alpha, \beta) = \left(\det \begin{pmatrix} \alpha & \bar{\alpha} \\ \beta & \bar{\beta} \end{pmatrix} \right)^2.$$

It is easy to show that the discriminant of an order is independent of the choice of the basis. That is, if $\mathcal{O} = [\alpha, \beta] = [\alpha', \beta']$ then $D(\alpha, \beta) = D(\alpha', \beta')$. We will denote the discriminant of $\mathcal{O}$ simply by D.

Theorem 2.9. *$\mathcal{O}_K = [1, \omega_K]$ where $\omega_K = \frac{d_K + \sqrt{d_K}}{2}$. If f is the conductor of $\mathcal{O}$ then $\mathcal{O} = [1, f\omega_K]$.*

Remark 2.10. Observe that $D = f^2 d_K$ since $\mathcal{O} = [1, f\omega_K]$. This observation points out that if D is the discriminant of the order $\mathcal{O}$ then $K = \mathbb{Q}[\sqrt{D}]$. Also observe that $D \equiv 0, 1 (\text{mod } 4)$.

Definition 2.11. Let K be a quadratic field.

1. An ideal I of an order $\mathcal{O}$. We say that I is a **proper ideal** if $\mathcal{O} = \{\beta \in K : \beta I \subset I\}$
2. A **fractional ideal** $\mathscr{I}$ of $\mathcal{O}$ is an $\mathcal{O}-$module such that $\omega I \subseteq \mathcal{O}$ for some $\omega \in \mathcal{O}$. We can define **proper fractional ideal** in a similar way.
3. Given a fractional ideal $\mathscr{I}$, we say that it is **invertible** if there exists a fractional ideal $\mathscr{J}$ such that $\mathscr{I}\mathscr{J} = \mathcal{O}$.

Example 2.12. Let $K = \mathbb{Q}[\sqrt{-7}]$. Then $d_K = -7$. By Theorem 2.9 we have

$$\mathcal{O}_K = [1, \omega_K] = \mathbb{Z} + \frac{-7 + \sqrt{-7}}{2}\mathbb{Z} = \mathbb{Z} + \frac{1 + \sqrt{-7}}{2} \cdot \mathbb{Z}.$$

Let $\mathcal{O} = \mathbb{Z}[\sqrt{-7}] \subseteq \mathcal{O}_K$ be an order of K where $\mathbb{Z}[\sqrt{-7}]$ is defined similar to K as

$$\mathbb{Z}[\sqrt{D}] = \{a + b\sqrt{D} : a, b \in \mathbb{Z}\}.$$

One easily checks that the conductor f of $\mathcal{O}$ is 2 since $2\omega_K = -7 + \sqrt{-7}$ and $\mathcal{O}$ is generated by 1 and $2\omega_K$. $I = 2\mathbb{Z} + (1 + \sqrt{-7})\mathbb{Z}$ is an ideal of $\mathcal{O}$. One easily verifies that $I \subseteq \mathcal{O}$ is indeed a proper ideal of $\mathcal{O}$.

Example 2.13. For $K = \mathbb{Q}[\sqrt{-5}]$, $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$. The ideal $\mathscr{I} = \mathbb{Z}[\sqrt{-5}] \cdot \frac{1+\sqrt{-5}}{3}$ is a fractional ideal of $\mathcal{O}_K$.

Proposition 2.14. *Let $\mathcal{O}$ be any order of a quadratic field K. For any ideal $I \subseteq \mathcal{O}$, there exist $a, b, d \in \mathbb{Z}$ such that the following are true:*
$(a) I = d(\mathbb{Z}a + \mathbb{Z}(-b + \omega_K))$, and
(b) $b^2 - tb + n \equiv 0 (\text{mod } a)$, or, equivalently, $a \mid \text{N}(-b + \omega_K)$
Conversely, any $I \subseteq \mathcal{O}$ satisfying (a) and (b) is an ideal.

Proposition 2.15. *An $\mathscr{I} \subseteq F$ is a fractional ideal if and only if there exists an $e \in \mathbb{Z}$ such that $e\mathscr{I}$ is an ideal of $\mathcal{O}$*

Combining Proposition 2.15 and 2.14 we have

Corollary 2.16. *Fractional ideals are precisely the subsets of K of the form $q(\mathbb{Z}a + \mathbb{Z}(-b + \omega_K))$ for some $q \in \mathbb{Q}^\times$ and $a, b \in \mathbb{Z}$ satisfying $a \neq 0$ and*

$$b^2 - tb + n \equiv 0 (\text{mod } a).$$

Remark 2.17. In view of Proposition 2.14 and Corollary 2.16, we will denote any ideal or fractional ideal of an order $\mathcal{O}$ by $[\alpha, \beta]$.

Definition 2.18. (Ideal Norm) The norm of an ideal $I \neq 0$ of $\mathcal{O}$ is the natural number $\text{N}(I) = |\mathcal{O}/I|$.

Proposition 2.19. *Let $I = [\alpha, \beta]$ be any ideal or fractional ideal of $\mathcal{O} = [1, \tau]$ where $\tau = f\omega_K$ with f being the conductor of $\mathcal{O}$ in $\mathcal{O}_K$. Then we have that*

$$N(I) = \text{abs}\left(\begin{vmatrix} \alpha & \bar{\alpha} \\ \beta & \bar{\beta} \end{vmatrix} \frac{1}{\sqrt{|D|}}\right)$$

where D is the discriminant of $\mathcal{O}$.

Remark 2.20. If $\alpha = a_1 + a_2\tau, \beta = b_1 + b_2\tau$, then

$$N(I) = \text{abs}\left(\begin{vmatrix} a_1 & a_2 \\ b_1 & b_2 \end{vmatrix}\right)$$

Theorem 2.21. *Let I, J be a nonzero ideals of $\mathcal{O}$.*

1. *$N(IJ) = N(I) \cdot N(J)$.*
2. *If $I \subseteq J$ are ideals of $\mathcal{O}$ and $\mathrm{N}(I) = \mathrm{N}(J)$, then $I = J$.*
3. *$I\bar{I} = \mathcal{O} \cdot \mathrm{N}(I)$, the principal ideal generated by $\mathrm{N(I)}$ viewed as an element of $\mathcal{O}$.*

Proposition 2.22. *Let I be an ideal of $\mathcal{O}$. Then $N(I) = gcd(N\alpha \mid \alpha \in I)$.*

Theorem 2.23. *Let $K = \mathbb{Q}[\tau]$ be a quadratic field and $ax^2 + bx + c$ the minimal polynomial of τ. Then $[1, \tau]$ is a proper fractional ideal for the order $[1, a\tau]$ of K.*

Theorem 2.24. *Let $\mathcal{O}$ be an order in a quadratic field K and let $\mathscr{I}$ be a fractional $\mathcal{O}-$ideal. Then $\mathscr{I}$ is proper if and only if $\mathscr{I}$ is invertible.*

Definition 2.25. Let $\mathcal{O}$ be an order of a quadratic field K. Let $\mathscr{I}(\mathcal{O})$ denote the set of invertible fractional ideals of $\mathcal{O}$, and $P(\mathcal{O})$ be the set of non-zero principal ideals (Definition 1.10) of $\mathcal{O}$.

Remark 2.26. It is clear that $\mathscr{I}(\mathcal{O})$ is an abelian group and that $P(\mathcal{O}) \subset \mathscr{I}(\mathcal{O})$.

Definition 2.27. Let $\mathcal{O}$ be an order of a quadratic field K. We define the **ideal class group** of $\mathcal{O}$ to be $C(\mathcal{O}) = \mathscr{I}(\mathcal{O})/P(\mathcal{O})$.

We make the following observations:

(a) Let $\mathscr{I}$ and $\mathscr{J}$ be fractional ideals. A typical element of $C(\mathcal{O})$ is a coset $[\mathscr{I}] = \mathcal{P}(\mathcal{O})\mathscr{I}$, which we call the **ideal class** of $\mathscr{I}$. By the definition of a quotient group, $[\mathscr{I}] = [\mathscr{J}]$ if and only if $\mathscr{I} = (\mathcal{O}\alpha)\mathscr{J} = \alpha\mathscr{J}$ for some $\alpha \in K \setminus \{0\}$. Two ideals are in the same class precisely when they're proportional. In particular, the identity of $C(\mathcal{O})$ is $[\mathcal{O}]$, the class of principal fractional ideals.

(b) By Proposition 2.15, for any fractional ideal $\mathscr{I}$ there exists $k \in \mathbb{Z}$ such that $I = k\mathscr{I} \subseteq \mathcal{O}$ is an ideal. Then $[\mathscr{I}] = [k\mathscr{I}] = [I]$, so that every ideal class is represented by an ideal. We can define ideal classes without leaving $\mathcal{O} : [I] = [J]$ for ideals I, J of $\mathcal{O}$ if and only if there exist $\beta, \gamma \in \mathcal{O}$ such that $\gamma I = \beta J$

(c) The inverse in $C(\mathcal{O})$ is given by conjugation. The identity $I\bar{I} = \mathcal{O} \cdot \mathrm{NI}$ (Theorem 2.21) translates to $[I][\bar{I}] = [\mathcal{O}]$, or $[I]^{-1} = [\bar{I}]$.

3 Correspondence of Class Group and Ideal Class Group

3.1 Class Group

Definition 3.1. A **binary quadratic form** is a function $q : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ given by $q(x, y) = mx^2 + rxy + ny^2$ where $m, r, n \in \mathbb{Z}$. The integer $D = r^2 - 4mn$ is called the **discriminant** of $q(x, y)$. The binary quadratic form $q(x, y)$ is called

(i) **primitive** if $\gcd(m, r, n) = 1$.

(ii) **positive definite** if $D < 0$ and $m > 0$.

(iii) **reduced** if $|r| \leq |m| \leq |n|$ and $r \geq 0$ when $|m| = |r|$ or $|m| = |n|$.

Consider the set of all primitive, positive definite binary quadratic forms with fixed discriminant D and denote it by $\mathcal{Q}_D$. The next Theorem gives an action of $SL_2(\mathbb{Z})$ on $\mathcal{Q}_D$.

Theorem 3.2. *For* $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ *and* $q(x, y) \in \mathcal{Q}_D$*, the map* $SL_2(\mathbb{Z}) \times \mathcal{Q}_D \longrightarrow \mathcal{Q}_D$ *given by*

$$(M, q) \mapsto (M \circ q)(x, y) = q(ax + cy, bx + dy).$$

is a group action of $SL_2(\mathbb{Z})$ *on the set* $\mathcal{Q}_D$*.*

Definition 3.3. The set $C(D) = \mathcal{Q}_D/SL_2(\mathbb{Z})$ is called the **class group** and the cardinality $h(D) = |C(D)|$ is called the **class number**.

We recall the Dirichlet composition of forms.

Theorem 3.4. *Let* $[m_1, r_1, n_1]$ *and* $[m_2, r_2, n_2]$ *be two members of class group* $C(D)$*. Let* $e = gcd\left(n_1, n_2, \frac{r_1+r_2}{2}\right)$*. Then there is a unique integer* R *modulo* $2n_2n_2/e^2$ *such that:*

$$R \equiv r_1 \ mod \ \frac{2n_1}{e}, \quad R \equiv r_2 \ mod \ \frac{2n_2}{e}, \quad R^2 \equiv D \ mod \ \frac{4n_1n_2}{e^2}$$

Moreover, we have the following class group composition

$$[m_1, r_1, n_1] * [m_2, r_2, n_2] = \left[\frac{e^2(R^2 - D)}{4n_1n_2}, R, \frac{n_1n_2}{e^2}\right]. \tag{1}$$

3.2 The Correspondence

Let $\mathscr{I} = [\alpha, \beta]$ be a fractional ideal of an order $\mathcal{O}$ of discriminant D of the quadratic field $K = \mathbb{Q}[\sqrt{D}]$. The expression

$$q_{\mathscr{I},\alpha,\beta}(x, y) = \frac{\mathrm{N}(x\alpha - y\beta)}{\mathrm{N}\mathscr{I}} = \frac{\mathrm{N}\alpha}{\mathrm{N}\mathscr{I}}x^2 - \frac{\mathrm{Tr}(\bar{\alpha}\beta)}{\mathrm{N}\mathscr{I}}xy + \frac{\mathrm{N}\beta}{\mathrm{N}\mathscr{I}}y^2 \tag{2}$$

has coefficients in $\mathbb{Z}$ by Proposition 2.22. Moreover it is easy to show that the discriminant of the quadratic form $q_{\mathscr{I},\alpha,\beta}$ is same as the discriminant of $\mathcal{O}$ which is D.

Conversely if $q(x, y) = ax^2 + bxy + cy^2$ is a quadratic form with discriminant D then the ideal given by

$$\left[a, \frac{-b + \sqrt{D}}{2}\right]$$

is a proper ideal of the order $\mathcal{O}$ with discriminant D of the quadratic field $\mathbb{Q}[\sqrt{D}]$. It turns out that these two maps are inverses of each other and satisfy group homomorphism rules. Thus we get an isomorphism of the ideal class group and the class group of binary quadratic forms. To prove this isomorphism, we will differentiate between the cases $D < 0$ and $D > 0$. The former case is slightly easier. In what follows we assume $D < 0$.

Theorem 3.5. *Let* $D < 0$ *and* $\mathcal{O} = [1, f\omega_K]$ *an order with discriminant* D *of the quadratic field* $K = \mathbb{Q}[\sqrt{D}]$*, where* f *is the conductor of* $\mathcal{O}$ *and* $\omega_K = \frac{d_K+\sqrt{d_K}}{2}$ *with* d_K *the discriminant of* K

1. *If* $q(x, y) = ax^2 + bxy + cy^2$ *is a binary quadratic form with discriminant* D *then* $\left[a, \frac{-b+\sqrt{D}}{2}\right]$ *is a proper ideal of* $\mathcal{O}$
2. $C(D)$ *is a group and the map sending* $q(x, y)$ *to* $\left[a, \frac{-b+\sqrt{D}}{2}\right]$ *induces an isomorphism between* $C(D)$ *and* $C(\mathcal{O})$*. Hence the order of* $C(\mathcal{O})$ *is the class number* $h(D)$

Proof. Proof of 1.
Since $D < 0,$ and $a > 0$, let $\tau = \frac{-b+\sqrt{D}}{2a}$ be the unique root of $q(x, 1)$ with positive imaginary part. Then

$$\left[a, \frac{-b+\sqrt{D}}{2}\right] = [a, a\tau] = a[1, \tau].$$

By Theorem 2.23 we have that $a[1, \tau]$ is a proper ideal of $[1, a\tau]$. We will now show that $\mathcal{O} = [1, a\tau]$. One easily sees that

$$a\tau = -\frac{b + fd_K}{2} + f\omega_K.$$

This shows that $[1, a\tau] = [1, f\omega_K] = \mathcal{O}$.

Sketch of Proof of 2.

Step 1. The map sending $q(x, y) = ax^2 + bxy + cy^2$ to $\left[a, \frac{-b+\sqrt{D}}{2}\right]$ is well defined

Indeed if $q(x, y) \backsim q'(x, y)$ by the matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ then a simple computation shows that the solutions τ, τ' to the equations $q(x, 1) = 0$ and $q'(x, 1) = 0$ is related by

$$\tau' = \frac{a\tau + c}{b\tau + d}.$$

With this observation, one can show that

$$(b\tau + d)[1, \tau'] = [1, \tau].$$

Thus by Observation 2 above, we see that the map is well defined.

Step 2. Injectivity
Suppose q maps to $a[1, \tau]$ and q' maps to $a'[1, \tau']$ such that $[a[1, \tau]] = [a'[1, \tau']]$ then $[1, \tau] = \alpha[1, \tau']$ for some $\alpha \in K^\times$. Then we have $\alpha\tau' = a\tau + b$ and $\alpha = c\tau + d$ for some $a, b, c, d \in \mathbb{Z}$ such that the matrix $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is invertible (since we can also write τ and 1 in terms of $\alpha\tau', \alpha$) so that $\det(A) = \pm 1$. We have

$$\tau' = \frac{\alpha\tau'}{\alpha} = \frac{a\tau + b}{c\tau + d}.$$

Since τ' has positive imaginary part $A \in SL_2(\mathbb{Z})$. Now it is easy to see that $q = A^T \circ q'$.

Step 3. Surjectivity
For any fractional ideal $\mathscr{I} = [\alpha, \beta]$ of $\mathcal{O}$, define the quadratic form $q_{\mathscr{I},\alpha,\beta}(x, y)$ as in Eq. (2). Then $q_{\mathscr{I},\alpha,\beta}(x, y)$ maps precisely to $\mathscr{I}$. Thus we have a bijection $C(D) \longleftrightarrow C(\mathcal{O})$.

Step 4. Group homomorphism
Let $[a, b, c]$ and $[a', b', c']$ be two classes of binary quadratic forms of discriminant D. Then by Theorem 3.4 under the above bijection their images are

$$\left[a, \frac{-b+\sqrt{D}}{2}\right], \left[a', \frac{-b'+\sqrt{D}}{2}\right], \left[\frac{aa'}{e^2} \text{ and } \frac{-B+\sqrt{D}}{2}\right]$$

respectively where

$$e = \gcd\left(a, a', \frac{b+b'}{2}\right) \text{ and } B = \frac{1}{e}\left(n_1 ab' + n_2 a'b + n_3 \frac{bb' + D}{2}\right)$$

for some $n_1, n_2, n_3 \in \mathbb{Z}$ such that

$$n_1 a + n_2 a' + n_3 \frac{b+b'}{2} = e.$$

To show that the above bijection is a group homomorphism, we need to show that

$$\left[a, \frac{-b+\sqrt{D}}{2}\right]\left[a', \frac{-b'+\sqrt{D}}{2}\right] = \left[aa', a\frac{-b'+\sqrt{D}}{2}, a'\frac{-b+\sqrt{D}}{2}, \frac{\frac{1}{2}(bb'+D)-\frac{1}{2}(b+b')\sqrt{D}}{2}\right]$$
$$= \left[\frac{aa'}{e^2}, \frac{-B+\sqrt{D}}{2}\right].$$

In above Equation, by $[\alpha, \beta]$ we mean the equivalence class in $C(\mathcal{O})$. We claim that

$$\left[a, \frac{-b+\sqrt{D}}{2}\right]\left[a', \frac{-b'+\sqrt{D}}{2}\right] = \left[\frac{aa'}{e}, \frac{-B+\sqrt{D}}{2}e\right].$$

Using Proposition 2.19, it is easy to see that

$$N\left(\left[a, \frac{-b+\sqrt{D}}{2}\right]\right) = a,\ N\left(\left[a', \frac{-b'+\sqrt{D}}{2}\right]\right) = a'\ N\left(\left[\frac{aa'}{e}, \frac{-B+\sqrt{D}}{2}e\right]\right) = aa'.$$

, Next using (i) of Theorem 2.21 we have

$$N\left(\left[aa', a\frac{-b'+\sqrt{D}}{2}, a'\frac{-b+\sqrt{D}}{2}, \frac{\frac{1}{2}(bb'+D)-\frac{1}{2}(b+b')\sqrt{D}}{2}\right]\right) = aa' = N\left(\left[\frac{aa'}{e}, \frac{-B+\sqrt{D}}{2}e\right]\right),$$

Using the congruences in Theorem 3.4 and the fact $e \mid a, e \mid a', e \mid \frac{b+b'}{2}$ we can show that

$$\left[a, \frac{-b+\sqrt{D}}{2}\right]\left[a', \frac{-b'+\sqrt{D}}{2}\right] \subseteq \left[\frac{aa'}{e}, \frac{-B+\sqrt{D}}{2}e\right]$$

Indeed we have

$$a\frac{-b'+\sqrt{D}}{2} = n\frac{aa'}{e} + me\frac{-B+\sqrt{D}}{2} \in \left[\frac{aa'}{e}, \frac{-B+\sqrt{D}}{2}e\right],$$

where $m = \frac{a}{e}$ and n is such that

$$\frac{a}{e}B = \frac{a}{e}b' + 2n\frac{aa'}{2^2}.$$

Similarly we can show that other generators

$$a'\frac{-b+\sqrt{D}}{2}, \frac{\frac{1}{2}(bb'+D)-\frac{1}{2}(b+b')\sqrt{D}}{2} \in \left[\frac{aa'}{e}, \frac{-B+\sqrt{D}}{2}e\right].$$

By Theorem 2.21 we have

$$\left[a, \frac{-b+\sqrt{D}}{2}\right]\left[a', \frac{-b'+\sqrt{D}}{2}\right] = \left[\frac{aa'}{e}, \frac{-B+\sqrt{D}}{2}e\right].$$

But $\left[\frac{aa'}{e}, \frac{-B+\sqrt{D}}{2}e\right] = \frac{1}{e}\left[\frac{aa'}{e^2}, \frac{-B+\sqrt{D}}{2}\right]$, hence they are in the same ideal class. This completes the proof. □