# BINARY QUADRATIC FORMS AND IDEAL CLASS GROUPS

OLIVER CAI

Abstract. We can define an equivalence relation on primitive positive definite binary quadratic forms, which gives rise to class groups of forms. Similarly, we can define an equivalence relation on the ideals of a number ring, which creates the ideal class group. A key theorem of algebraic number theory is that the ideal class group is finite. In this paper, we investigate the connection between class groups of binary quadratic forms and ideal class groups of quadratic number rings with negative discriminant to prove this theorem.

## 1. Introduction

Binary quadratic forms were first studied extensively by Gauss in his *Disquisitiones Arithmeticae*, of which a large portion is dedicated to this study. These forms, which are quadratics in two variables, have been studied extensively by Lagrange and Gauss; Gauss himself contributing greatly to the study with his formulation of the composition of two forms. They arise naturally in the study of primes of the form $x^2 + ny^2$, as Fermat worked on.

On the other hand, the study of quadratic number fields grew out of the study of binary quadratic forms by Gauss. This work was later extended by Kummer to cyclotomic fields in the efforts to prove Fermat's Last Theorem. Finally, Dedekind introduced the concept of ideals, unifying the concepts laid down by Gauss and Kummer and giving rise to the ideal class group.

For a more detailed summary of the history of these concepts in number theory, see [SO85].

The ideal class group can be obtained by defining an equivalence relation on the ideals of a number ring. Our goal in this paper is to explain the theory of quadratic form class groups, ideal class groups, and show the following theorem linking binary quadratic forms and the ideal class groups of quadratic number rings:

**Theorem 1.1.** *For a negative discriminant $D$, the class group for quadratic forms with discriminant $D$ is isomorphic to the ideal class group of the ring of integers of $\mathbb{Q}(\sqrt{D})$.*

We will also show that the ideal class groups of quadratic number rings with negative discriminant are finite.

In Section 2, we discuss binary quadratic forms and their group of equivalence classes; in section 3, we provide a brief summary of necessary ring theory; in Section 4, we develop ideal class groups; and in Section 5, we bring binary quadratic forms and ideal class groups to show Theorem 1.1.

---

*Date*: July 14, 2024.

Acknowledgements

The author would like to thank Simon Rubinstein-Salzedo and Emma Cardwell for both mathematical assistance and help with writing this paper.

## 2. Binary Quadratic Forms

The first objects that we would like to study are binary quadratic forms, which are a special type of function in two variables.

**Definition 2.1.** An integral **binary quadratic form** is a function of the form $f(x, y) = ax^2 + bxy + cy^2$, for integers $a$,$b$,$c$.

We can have $a, b, c \notin \mathbb{Z}$, but this paper focuses on the integral case. We will sometimes abbreviate "binary quadratic form" to just "form".

**Definition 2.2.** A binary quadratic form **represents** an integer $n$ if we have $f(x, y) = n$ for some $x, y \in \mathbb{Z}$. $f(x, y)$ **properly represents** $n$ if we have $f(x, y) = n$ for relatively prime $x, y$.

**Example 2.1.** Suppose we have $f(x, y) = x^2+2xy+3y^2$. Then, we can say $f(x, y)$ represents 3 since we have $f(0, 3) = 3$. We can also say $f(x, y)$ properly represents 43 since $f(2, 3) = 43$.

Right now, our definition of a binary quadratic form is pretty loose; we could pull out any three integers and make a form. We will define some restrictions on these forms so that they satisfy useful properties, and so that we can eventually put them into equivalence classes.

**Definition 2.3.** A binary quadratic form $ax^2+bxy+cy^2$ is **reduced** if $|b| \leq a \leq c$, and $a = c$ or $a = |b|$ implies $b \geq 0$.

**Definition 2.4.** A binary quadratic form $ax^2+bxy+cy^2$ is **primitive** if $\gcd(a, b, c) = 1$.

**Definition 2.5.** The quadratic form $f(x, y) = ax^2+bxy+cy^@$ is **positive definite** if $f(x, y) \geq 0$, $a > 0$, and $f(x, y) = 0 \iff x = y = 0$.

We usually discuss primitive positive definite binary quadratic forms; we will show later that this is equivalent to simply being reduced. Now, to further help classify binary quadratic forms, we introduce the discriminant, and group forms with equal discriminant together. The definition of the discriminant should be reminiscent of quadratic polynomials.

**Definition 2.6.** The **discriminant** of a binary quadratic form $f(x) = ax^2+bxy+cy^2$, denoted $D_f$, is $b^2 - 4ac$.

And now, our sense of equivalence for forms. This will allow us to talk about classes of equivalent forms later.

**Definition 2.7.** A form $f(x, y)$ is **properly equivalent** to a form $g$ if we have $f(x, y) = g(px+qy, rx+sy)$ and $ps-qr = 1$ (as opposed to $\pm 1$ for just "equivalent") for $p, q, r, s \in \mathbb{Z}$.

It turns out that proper equivalence preserves the discriminant:

**Proposition 2.1.** *If two forms $f(x, y)$ and $g(x, y)$ are properly equivalent, then they have equal discriminant.*

*Proof.* Let $f(x,y) = ax^2 + bxy + cy^2$, and let $g(x,y) = f(px+qy, rx+sy)$ for integers $a,b,c,p,q,r,s$, and $ps - qr = 1$. Note that the discriminant of $f(x,y)$ is $b^2 - 4ac$. We have

$$g(x,y) = \left(ap^2 + bpq + cq^2\right)x^2 + (2apr + bps + brq + 2ps)xy + \left(ar^2 + brs + cs^2\right)y^2.$$

After a lot of algebra, we can indeed verify that the discriminant of $g(x,y)$ is also $b^2 - 4ac$. □

Now, all of these conditions for primitive, reduced, and properly representing quadratic forms seem sort of arbitrary, but it turns out that these restrictions are enough for some very convenient results.

**Theorem 2.1.** *Primitive positive definite forms are properly equivalent to a unique reduced form.*

*Proof.* First, show that we can find a reduced form that $f(x,y)$ equivalent to. That is, we will show the existence of such a form.

(1) We can find $f(x,y) = ax^2 + bxy + cy^2$ with minimal $|b|$.
(2) We can verify that $a \geq |b|$ and $c \geq |b|$ via contradiction.
(3) Now, if $a > c$, we preform the transformation $(x,y) \mapsto (-y,x)$ (proper equivalence), which swaps $a$ and $c$, and changes the sign of $b$. This works since $x^2$ and $y^2$ are nonnegative anyways.

We still need to verify that if $|b| = a$ or $a = c$ we can guarantee $b \geq 0$. So if we have a not reduced form, we have $b < 0$ and $a = -b$ or $a = c$; in either case $ax^2 - bxy + cy^2$ is reduced. So we just need to show that $ax^2 \pm bxy + cy^2$ are properly equivalent (via more transformations, one for each case):

- If we have $a = -b$, then we have $f(x,y) = ax^2 - axy + cy^2$. We apply $(x,y) \mapsto (x+y,y)$ to flip the sign on $xy$.
- If we have $a = c$, then we have $f(x,y) = ax^2 + bxy + ay^2$. Applying $(x,y) \mapsto (-y,x)$ flips the sign on $xy$.

We will make a few key observations before we show uniqueness.

Let $f(x,y) = ax^2 + bxy + cy^2$ be reduced, so $|b| \leq a \leq c$. We claim that

$$f(x,y) \geq (a - |b| + c)\min\left(x^2, y^2\right). \tag{2.1}$$

Note that we have $x^2 \geq \left(x^2,y^2\right)$, $y^2 \geq \left(x^2,y^2\right)$, and $|xy| \geq \left(x^2,y^2\right)$, so we have $f(x,y) \geq (a + |b| + c)\min\left(x^2,y^2\right) \geq (a - |b| + c)\min\left(x^2,y^2\right)$ as claimed.

Now, we have $f(x,y) \geq a - |b| + c$ whenever neither $x$ nor $y$ are zero. Then, we know that $a$ is the smallest positive value properly represented by $f$, since we have $f(1,0) = a$. In the case that $c > a$, we also have $c = f(0,1)$ be the next smallest properly represented number.

Suppose that $f(x,y)$ is reduced and satisfies $|b| < a < c$. We know that $a < c < a - |b| + c$ are the three smallest numbers that are properly represented by $f(x,y)$, since $f(x,y) \geq (a - |b| + c)\min\left(x^2,y^2\right)$ and we know that $a, c$ are the two smallest values properly represented by $f(x,y)$. We claim that

$$f(x,y) = a, \gcd(x,y) = 1 \iff (x,y) = (\pm 1, 0).$$

Note that $f(\pm 1, 0) = a$ trivially. Now, suppose that $f(x,y) = a$. By Equation 2.1, we have $a \geq (a - |b| + c)\min\left(x^2,y^2\right)$. Furthermore, since $c > |b|$, we have $a - |b| + c >$

$a$, so we must have $\min\left(x^2, y^2\right) = 0$, so one of $x$ and $y$ must be zero. $x$ must be nonzero, so we must have $x = \pm 1, y = 0$. Similarly, we can show that

$$f(x, y) = c, \gcd(x, y) = 1 \iff (x, y) = (0, \pm 0).$$

We now show uniqueness when the above strict inequality holds; the proof with nonstrict inequalities is a bit more involved with edge cases.

Suppose $g(x, y)$ is reduced and equivalent to $f(x, y)$. Then, they represent the same numbers, so in particular, their first coefficients must be equal to $a$. Then, we look at the last coefficient of $g(x, y)$; let it be $c'$. Since $g(x, y)$ is reduced, we have $a \leq c'$. However, if we have $a = c'$, then we would have

$$g(x, y) = a \iff (x, y) = (\pm 1, 0), (0, \pm 1).$$

This is a contradiction since we know $f(x, y)$ is equivalent to $g(x, y)$, and we must have $f(x, y) = a \iff (x, y) = (\pm 1, 0)$ only. Therefore $a < c'$, and $c = c'$. Thus we have $g(x, y) = ax^2 \pm bxy + cy^2$ since $f(x, y)$ and $g(x, y)$ must have the same discriminant. □

This tells us that the number of *classes* of primitive positive definite forms with discriminant $D$ under proper equivalence is also the number of reduced forms with discriminant $D$. We have a special name for this.

**Definition 2.8.** The **class number** of $D$, denoted $h(D_f)$, is the number of primitive, positive definite, binary quadratic forms with discriminant $D_f$.

**Example 2.2.** We have $h(-4) = 1$ since the only reduced, positive definite form with discriminant $-4$ is $x^2 + y^2$.

On the other hand, $h(-20) = 2$; we have $x^2 + 5y^2$ and $2x^2 + 2xy + 3y^2$ with discriminant $-20$.

Keep the class number in mind; it will come up again very soon. It turns out that reduced forms with discriminant $D$ form a group. The group operation is known as composition, and it turns out to be quite involved.

**Definition 2.9.** Given two primitive positive definite binary quadratic forms $f(x, y)$ and $g(z, w)$, a form $F(x, y)$ is their **composition** given that there exist bilinear forms

$$B_i(x, y : z, w) = a_i xz + b_i xw + c_i yz + d_i yw$$

such that

$$f(x, y)g(z, w) = F(B_1(x, y : z, w), B_2(x, y : z, w)),$$

for integers $a_i, b_i, c_i, d_i$.

It turns out that this definition is a bit too loose; given two forms, there are many ways we can compose them together. Therefore we must restrict composition. In practice, we use a direct formula known as Dirichlet composition.

**Definition 2.10.** Let $f(x, y) = ax^2 + bxy + cy^2$ and $g(x, y) = a'x^2 + b'xy + c'y^2$ be primitive positive definite quadratic forms with negative discriminant $D$. Further, let $\gcd\left(a, a', \frac{b+b'}{2}\right) = 1$.

It turns out that there is a unique integer $B$ modulo $2aa'$ such that

$$\begin{aligned} B &\equiv b \pmod{2a}, \\ B &\equiv b' \pmod{2a'}, \\ B^2 &\equiv D \pmod{4aa'}. \end{aligned}$$

To see this, convert and multiply the first two congruences modulo $4aa'$, then substitute into the third. We can then simplify the resulting congruence, modify the first two congruences, and then use the Chinese Remainder Theorem to solve the system uniquely [Cox22, Chapter 3].

Then, the **Dirichlet composition** (which we will abbreviate to "composition" when it is clear) of $f(x, y)$ and $g(x, y)$ is

$$aa'x^2 + Bxy + \frac{B^2 - D}{4aa'}y^2.$$

Despite having restrictions on the coefficients of our quadratic forms, Dirichlet composition is much more useful than the more general (and much more complex) Gauss composition. Furthermore, we can usually find properly equivalent forms that Dirichlet composition works on. Dirichlet and Gauss compositions are also identical on forms they are defined on. Apart from the equivalence with Gauss composition, Dirichlet composition also satisfies some properties that we should expect.

**Proposition 2.2.** *Define $f(x, y)$ and $g(x, y)$ as in Definition 2.10. Let $F(x, y)$ be the Dirichlet composition of $f(x, y)$ and $g(x, y)$. Then, $F(x, y)$ is primitive, positive definite, and has the same discriminant $D$ as $f(x, y)$ and $g(x, y)$.*

*Proof.* We can directly compute the discriminant of $F(x, y)$ to be $D$ using a lot of algebra. Let $f(x, y) = ax^2 + bxy + cy^2$ and $g(x, y) = a'x^2b'xy + c'y^2$. Then, we have $F(x, y) = aa'x^2 + Bxy + \frac{B^2-D}{4aa'}y^2$, so its discriminant is

$$B^2 - 4aa'\frac{B^2 - D}{4aa'} = D.$$

It follows that $F(x, y)$ is positive definite. As a lemma,

**Lemma 2.1.** *If a binary quadratic form $f(x, y) = ax^2 + bxy + cy^2$ is positive definite, its discriminant $b^2 - 4ac$ is negative.*

*Proof.* We will first show that a positive definite form has negative discriminant. Consider $f(x, 0) = ax^2$, $f(0, y) = cy^2$, and

$$f(x, kx) = ax^2 + bkx^2 + k^2x^2 = (a + bk + ck^2)x^2$$

for nonzero integers $x, y, k$. Since $f(x, y)$ is positive definite, we must have $c > 0$ and $a + bk + k^2 > 0$. In particular, this means that we must have $b^2 - 4ac$ for the second inequality to hold. This completes the proof of the lemma. □

This tells us that we have $D < 0$. We now return to the proof of Theorem 2.2. Note that

$$F(ky, y) = \left(aa'k^2 + Bk + \frac{B^2 - D}{4aa'}\right)y^2$$

for arbitrary integers $k$, and that the portion inside parentheses is either all positive or all negative. Further, since $aa' > 0$, it must be positive. Also, note that $F(0, 0) = 0$ and $F(x, 0) = aa' > 0$. Thus $F(x, y)$ is positive definite.

Finally, we show that $F(x, y)$ is primitive. Note that $F(x, y)$ takes the form $f(x, y) \cdot g(z, w)$. Since both $f(x, y)$ and $g(w, z)$ are primitive, the greatest common divisor of numbers they represent is 1.

We claim that the greatest common divisor of the numbers represented by $f(x, y) \cdot g(z, w)$ is also one. Suppose not; then there is some prime $p$ that divides either $f(x, y)$ or $g(z, s)$ for all pairs $(x, y)$ and $(w, z)$. Since $(x, y)$ and $(w, z)$ are independent, we must have $p$ divide $f(x, y)$ for all $(x, y)$, contradicting the fact that $f(x, y)$ is primitive.

Then, the greatest common divisor of the numbers represented by $F(x, y)$ is one. If $F(x, y)$ was not primitive, then note that some prime $q$ must divide each coefficient. Then, $q$ would divide all numbers represented by $F(x, y)$, contradicting the fact that their greatest common divisor is 1. Thus $F(x, y)$ is primitive. □

**Theorem 2.2.** *Let the set of reduced forms with discriminant $D$ be $C(D)$ with $D \equiv 0, 1 \pmod 4$ negative. Then $C(D)$ forms an abelian group of order $h(D)$ under composition, known as the* ***class group*** *for binary quadratic forms with discriminant $D$.*

*Proof.* Let $f(x, y) = ax^2 + bxy + cy^2$ and $g(x, y)$ be representatives of two classes in $C(D)$. We will show that $g(x, y)$ is properly equivalent to another form such that we can use Dirichlet composition on it and $f(x, y)$.

**Lemma 2.2.** *Given a reduced form $f(x, y)$ and $M \in \mathbb{Z}$, $f(x, y)$ can properly represent at least one integer relatively prime to $M$.*

*Proof.* Let $f(x, y) = ax^2 + bxy + cy^2$. Then, note that $f(1, 0) = a$, $f(0, 1) = c$, and $f(1, 1) = a + b + c$.

Let $p$ be any prime. We will show that $p$ must be relatively prime to at least one of $f(1, 0)$, $f(0, 1)$, and $f(1, 1)$. Suppose not. Then there exists some prime $q$ such that $q \mid a$, $q \mid c$, and $q \mid (a + b + c)$. In particular, this implies that $q \mid ((a+b+c)-a-c) \implies q \mid b$, so we do not have $\gcd(a, b, c) = 1$, a contradiction.

Now, let $q$ be a prime such that $q \nmid M$, so $q$ and $M$ are relatively prime. Then, we showed above that $q$ must be relatively prime to one of $f(1, 0)$, $f(0, 1)$, and $f(1, 1)$, so $f(x, y)$ indeed properly represents an integer (in fact, a prime) relatively prime to $M$. □

**Lemma 2.3.** *A form $f(x, y)$ properly represents $m \in \mathbb{Z}$ if and only if we have $f(x, y)$ properly equivalent to $mx^2 + b'xy + c'y^2$ for some integers $b', c'$.*

*Proof.* First, note that if $mx^2 + bxy + cy^2$ properly represents $m$ by taking $(x, y) = (1, 0)$.

Now, suppose that $f(p, q) = m$ for some relatively prime $p, q$. Then, we can find $r, s \in \mathbb{Z}$ such that $ps - qr = 1$ (so that we have proper equivalence). Substituting the proper equivalence yields:

$$\begin{aligned} f(px+ry, qx+sy) =& a(px+ry)^2 + b(px+ry)(qx+sy) + c(qx+sy)^2, \\ =& \left(ap^2+bpq+cq^2\right)x^2 \\ &+ (2apr+bps+brq+2ps)xy \\ &+ \left(ar^2+brs+cs^2\right)y^2, \\ =& f(p,q)x^2 + (2apr+bps+brq+2ps)xy + f(r,s)y^2, \\ =& mx^2 + b'xy + c'y^2, \end{aligned}$$

completing our proof of this lemma. □

We return to the proof of Theorem 2.2.

By Lemma 2.2, we can find an integer $a'$ that $g(x,y)$ represents such that $a'$ is relatively prime to $a$. Then, by Lemma 2.3, we know $g(x,y)$ is in fact properly equivalent to some form $a'x^2+b'xy+c'y^2$.

Now, Dirichlet composition applies to the pair of forms $f(x,y)$ and $a'x^2+b'xy+c'y^2$ since $\gcd(a,a') = 1 \implies \gcd\left(a, a', \frac{b+b'}{2}\right) = 1$. Since we have found a way to convert forms in $C(D)$ to properly equivalent forms that allow Dirichlet composition, we have shown that composition in general is defined for any two classes in $C(D)$.

We can check that Dirichlet composition is both well-defined for classes from Proposition 2.2. We can easily verify identity and inverses. □

The following theorem demonstrates that we have finitely many reduced forms with a given negative discriminant.

**Theorem 2.3.** *$h(D)$ is finite for $D < 0$.*

**Remark.** We have $D < 0$ for all reduced forms. If $f(x,y) = ax^2+bxy+cy^2$ is reduced, then we have $|b| \le a \le c$, so $b^2 - 4ac \le ac - 4ac = -3ac \le 0$. Observe that $a \le c$, so we have $-3ac < 0$. Thus $b^2 - 4ac < 0$.

As a result, $h(D)$ is only defined if $D < 0$. Thus, we can restate Theorem 2.3 as "$h(D)$ is finite for $D$ such that it is defined".

*Proof.* Let $ax^2+bxy+c$ be reduced, and let $D < 0$. Then, we have $|b| \le a \implies b^2 \le a^2$. So, $-D = 4ac-b^2 \ge 4ac-a^2$. Since $a \le c$, we can say that $-D \ge 4a^2-a^2 = 3a^2$, which implies

$$a \le \sqrt{\frac{-D}{3}}.$$

Now, note that $|b| \le a$ and that $a, b, c$ are all integers. Therefore, we have finitely many choices for $a$ and $b$. Once we nail down $a$ and $b$, $D = b^2 - 4ac$ allows us to determine $c$. Thus, the number of reduced forms with discriminant $D$ is finite, and the above theorem also guarantees that the number of equivalence classes (under proper equivalence) is finite. □

We can use binary quadratic forms to study quadratic number rings; those that take the form $\mathbb{Z}[\sqrt{D}]$.

## 3. A Primer on Ring Theory

We will need some basic definitions from ring theory to explain the ideal class group.

**Definition 3.1.** A **ring** (specifically, a commutative ring) is a set $R$ along with two binary operations, known as addition $(+)$ and multiplication $(\cdot)$, satisfying the following:

(1) $(R, +)$ forms an abelian group. The additive identity is called 0.
(2) Multiplication is associative and commutative.
(3) There exists a multiplicative identity 1.
(4) The distributive law applies: $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$.

Note that we do not require multiplicative inverses to exist.

Note that a ring with multiplicative inverses of nonzero elements is just a field.

**Example 3.1.** The integers $\mathbb{Z}$ under addition and multiplication form a ring. This is since $(\mathbb{Z}, +)$ forms an abelian group, and the usual multiplication is associative and commutative. Note that multiplication does *not* need to be invertible, so we are fine.

**Example 3.2.** On the other hand, $\mathbb{Q}$ under addition and multiplication forms not only a ring, but a field, since multiplication is invertible for all nonzero rationals.

Something important we'd like to define are ideals:

**Definition 3.2.** Let $R$ be a ring. A nonempty subset $I \subseteq R$ is an **ideal** of $R$ if:

(1) $I$ is closed under addition: for all $a, b \in I$, we have $a + b \in I$.
(2) $I$ is closed under multiplication with elements of $R$: for all $a \in I$, $r \in R$, we have $ar \in I$.

A specific kind of ideal is a principal ideal:

**Definition 3.3.** The **principal ideal** generated by $a \in R$ is the ideal $(a) = \{ar : r \in R\}$. If every ideal of $R$ takes this form, then we say that $R$ is a **principal ideal domain**, or a PID for short.

As always, it is helpful to think about $\mathbb{Z}$ as an example of a ring.

**Example 3.3.** The multiples of 2 form an ideal in the ring $\mathbb{Z}$. This is since the sum of two even integers is even, and the product of any integer and an even integer is even. It turns out that this is also a principal ideal, since it is generated by the element $2 \in \mathbb{Z}$.

We care about our number rings being PIDs since they have unique factorization, which we will show after we introduce ideals. Here are a few examples demonstrating unique and non-unique factorization.

**Example 3.4.** Consider the ring $\mathbb{Z}[\sqrt{-5}]$. This ring does *not* have unique factorization, as we can write

$$6 = (1 - \sqrt{-5})(1 + \sqrt{-5}) = (2)(3),$$

where all four factors are irreducible.

**Example 3.5.** On the other hand, the ring $\mathbb{Z}[\omega]$, where $\omega = \frac{1}{2} + \frac{\sqrt{3}}{2}i$ (known as the Eisenstein Integers), does indeed have unique factorization. This fact follows from the fact that we can define a division algorithm, from which unique factorization follows.

We typically denote ideals using Gothic/Fraktur letters. The reasoning behind ideals is that they just work better than individual elements.

The idea of a prime ideal is very natural to come up with, as ideals are already related to the idea of "is a multiple of".

**Definition 3.4.** An ideal $\mathfrak{p} \subsetneq R$ is a **prime ideal** if whenever $ab \in \mathfrak{p}$, then we have $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$.

We require that $\mathfrak{p} \subsetneq R$ so that we cannot identify $R$ as a prime ideal of itself.

Something very similar to prime ideals is the idea of a maximal ideal. In fact, maximal ideals are prime as well.

**Definition 3.5.** A **maximal ideal** $\mathfrak{m} \subsetneq R$ is an ideal such that there are no ideals $\mathfrak{a}$ or $R$ such that $\mathfrak{m} \subsetneq \mathfrak{a} \subsetneq R$. In other words, there are no ideals "between" $\mathfrak{m}$ and $R$.

We are now ready to prove that principal ideal domains have unique factorization.

**Proposition 3.1.** *Elements of a principal ideal domain factor uniquely into irreducibles; it is a* ***unique factorization domain****.*

*Proof.* Let $S$ be a PID. We will first show existence of a factorization into irreducibles.

Let $a_0 \in S$ be both nonzero and not a unit. If $a$ is irreducible, then we have factored $a_0$ into irreducibles. Otherwise, we have $a_0 = a_1 b_1$ for $a_1$, $b_1$ not units. Note that we have $(a_0) \subsetneq (a_1)$; if we had $(a_0) = (a_1)$, then we must have $b_1$ a unit. We can then continue the procedure, resulting in a strictly increasing chain of ideals

$$(a_0) \subsetneq (a_1) \subsetneq (a_2) \subsetneq \cdots .$$

We will show that this chain must end at some $(a_n)$.

One can verify that $A = \cup(a_i)$ is itself an ideal of $S$. Since $S$ is a PID, we have $A = (a)$ for some $a \in S$, and $a \in (a_r)$ for $r$ a positive integer. Note that, for any $s \geq r$, $(a) \subseteq (a_r) \subseteq (a_s) \subseteq A = (a)$. This implies that $(a_r) = (a_s)$. Therefore, at some point, our chain of $(a_i)$ becomes constant, so it must terminate. This final principal ideal is an irreducible factor of $a_0$. Thus we have shown that $a_0 = p_1 c_1$ for irreducible $p_1$ and $c_1$ not a unit.

We can follow a similar procedure for $c_1$ to eventually demonstrate that $a_0$ can be factored into irreducibles.

We will now show that this factorization into irreducibles is unique.

Suppose to the contrary that we have $n \in S$ such that

$$n = p_1 p_2 \cdots p_t = q_1 q_2 \cdots q_s$$

for irreducibles $p_i, q_i$, and without loss of generality let $t \leq s$. Then, we have $p_1 \mid (q_1 q_2 \cdots q_s)$, which implies that $p_1 \mid q_j$ for some $j$. Without loss of generality assume that we have $p_1 \mid q_1$. Since $p_1$ and $q_1$ are both irreducible, we have $q_1 = p_1 u_1$ for a unit $u_1$. Substituting for $q_1$ and cancelling out $p_1$ yields

$$p_2 p_3 \cdots p_t = u_1 q_2 q_3 \cdots q_s.$$

We can repeat this process with $p_2, p_3$, and so on, yielding

$$1 = u_1 u_2 \dots u_t q_{t+1} \dots q_s.$$

Now, since each of the $q_i$ are irreducibles, we must have $t = s$, so the two factorizations are indeed equal. □

Finally, we will distinguish between primes and irreducibles.

**Definition 3.6.** A **unit** is an element that divides 1. For instance, in $\mathbb{Z}$, the units are $\pm 1$, and in $\mathbb{Z}[i]$, the units are $\pm 1, \pm i$.

We say $n \in R$ is **irreducible** if whenever $n = ab$, either $a$ or $b$ must be a unit.

On the other hand, $x \in R$ is **prime** if it is not a unit and whenever $x|ab$, we have $x|a$ or $x|b$. That is, if $ab$ is a multiple of $x$, then either $a$ or $b$ is already a multiple of $x$.

## 4. The Ideal Class Group

With basic ring theory out of the way, we can not begin setting up the ideal class group. The key objects of interest are number rings and number fields.

We first define algebraic numbers and algebraic integers.

**Definition 4.1.** A number $\alpha$ is **integral** over the rationals or the integers if it is the root of some irreducible (not factorable) polynomial with rational or integral coefficients. For instance, $\sqrt{2}$ is integral over $\mathbb{Z}$ since it is a root of $x^2 - 2$.

As a special case, we say a complex number is an **algebraic integer** if it is the root of a monic polynomial with integral coefficients.

Now that we have the proper setup, we can now discuss number fields, which are like extended rational numbers.

**Definition 4.2.** A **number field** is a subfield of $\mathbb{C}$, with finite degree as an extension of $\mathbb{Q}$. One can show that all number fields uniquely take the form $\mathbb{Q}(\alpha)$ for algebraic $\alpha \in \mathbb{C}$. So if $\alpha$ is the root of a degree $n$ polynomial, we have

$$\mathbb{Q}(\alpha) = \{a_0 + a_1\alpha + \dots + a_{n-1}\alpha^{n-1} : a_i \in \mathbb{Q}\}.$$

We can adjoin more $\alpha$, but it's equivalent to adjoining one element.

Of particular interest to us are **quadratic fields**, those that take the form of $\mathbb{Q}(\sqrt{m})$, for $m \in \mathbb{Z}$ squarefree. However, we would like to talk about rings that look like $\mathbb{Z}[\sqrt{m}]$ or $\mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right]$, which are known as **quadratic number rings**.

**Definition 4.3.** The **ring of integers** or **number ring** $\mathcal{O}_K$ of a number field $K$ is the set of algebraic integers in $K$.

Equivalently, letting $\mathbb{A}$ be the set of algebraic integers in $\mathbb{C}$, we can write $\mathcal{O}_K = K \cap \mathbb{A}$.

It's called a ring, but is it? We will first show this for quadratic number rings, then in general.

**Theorem 4.1.** *If $f$ is a monic polynomial with integral coefficients, with an algebraic integer as a root, then $f$ is irreducible over $\mathbb{Q}$.*

As a corollary, we have:

**Corollary 4.1.** *Algebraic integers in $\mathbb{Q}$ are just $\mathbb{Z}$.*

The following corollary is extremely important, as it characterizes the ring of integers.

**Corollary 4.2.** *Let $m$ be a squarefree (not divisible by the square of a prime) integer. Then, the set of algebraic integers in $\mathbb{Q}(\sqrt{m})$ is:*

$$\mathbb{Z}[\sqrt{m}] = \{a + b\sqrt{m} : a, b \in \mathbb{Z}\}, m \equiv 2, 3 \pmod 4,$$
$$\mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right] = \left\{\frac{a+b\sqrt{m}}{2} : a, b \in \mathbb{Z}, a \equiv b \pmod 2\right\}, m \equiv 1 \pmod 4.$$

*Proof.* Suppose $\alpha = r + s\sqrt{m}$ for rational $r$ and $s$. Then, note that $f(x) = (x - \alpha)(x + \alpha) = x^2 - 2rx + r^2 - ms^2$ is a monic polynomial that is irreducible over $\mathbb{Q}$ with $\alpha$ as a root. If $2r$ and $r^2 - ms^2$, $f(x)$ in fact has integral coefficients, so $\alpha$ is an algebraic integer in that case. What is left is to find the non-integral $r$ and $s$ such that the above condition holds.

If $r, s \in \mathbb{Z}$, then $\alpha$ is clearly an algebraic integer. Otherwise, we must have $r = \frac{n}{2}$ for some $n \in \mathbb{Z}$ since we want $2r \in \mathbb{Z}$. Also rewrite $s = \frac{k}{2}$ for some $k \in \mathbb{Z}$. So we would like $r^2 - ms^2 = \frac{n^2}{4} - \frac{mk^2}{4} \in \mathbb{Z}$. Thus $n^2 - mk^2 \equiv 0 \pmod 4$. We proceed by cases on $m \pmod 4$. Note that $m \not\equiv 0 \pmod 4$ as $m$ is squarefree.

Suppose $m \equiv 1 \pmod 4$. Then, we have

$$n^2 - k^2 \equiv 0 \pmod 4 \implies n^2 \equiv k^2 \pmod 4 \implies n \equiv k \pmod 2.$$

This implies that, in this case, the set of algebraic integers in $\mathbb{Q}(\sqrt{m})$ is indeed

$$\left\{\frac{a+b\sqrt{m}}{2} : a, b \in \mathbb{Z}, a \equiv b \pmod 2\right\}.$$

Now, suppose $m \equiv 2 \pmod 4$. Then, we have $n^2 \equiv 2k^2 \pmod 4$. Recalling that $x^2 \equiv 0, 1 \pmod 4$ for integer $x$, we must have $n^2 \equiv k^2 \equiv 0 \pmod 4$, so $n, k$ are even, so we just have $r, s \in \mathbb{Z}$.

Finally, suppose $m \equiv 3 \pmod 4$. Then, we have $n^2 \equiv 3k^2 \pmod 4$. We also must have $n^2 \equiv k^2 \pmod 4$, so as in the $2 \pmod 4$ case, we have $r, s \in \mathbb{Z}$. These two cases complete our proof. □

This gives us a specific set for the algebraic integers of $\mathbb{Q}(\sqrt{m})$, and it is easy to check that they also form a ring. To show that the algebraic integers of any number field form a ring, we need to establish that the sum and product of algebraic integers are themselves algebraic integers. We will do this a a corollary of this next theorem.

**Definition 4.4.** A group $G$ is **finitely generated** if there is some finite set $S$ (known as the generating set) such that every element in $G$ can be written as the combination of elements in $S$ and their inverses.

**Theorem 4.2.** *For $\alpha \in C$, the following statements are equivalent:*

1. *$\alpha$ is an algebraic integer,*
2. *The additive group for $\mathbb{Z}[\alpha]$ is finitely generated,*
3. *$\alpha$ is in some subring of $\mathbb{C}$ with a finitely generated additive group,*
4. *$\alpha A = \{\alpha a : a \in A\} \subseteq A$ for a finitely generated additive subgroup $A \subseteq \mathbb{C}$.*

*Proof.* We will show that (1) $\implies$ (2) $\implies$ (3) $\implies$ (4) $\implies$ (1).

To show that (1) $\implies$ (2), note that $\alpha$ is the root of some polynomial in $\mathbb{Z}$ with degree $n$, so the additive group of $\mathbb{Z}[\alpha]$ can be generated with the values $1, \alpha, \ldots, \alpha^{n-1}$.

Note that (2) $\implies$ (3) trivially, as $\mathbb{Z}[\alpha]$ is a subring of $\mathbb{C}$.

Similarly, (3) $\implies$ (4) trivially, as we can let $A$ be the subring with finitely generated additive group that $\alpha$ is a member of.

Finally, we show (4) $\implies$ (1). Let $A$ be generated by $a_1, \ldots, a_n$. Then, we can write the $\alpha a_i$ as some linear combination of $a_1, \ldots, a_n$ with integral coefficients. Rewriting this in matrix and vector notation, we have

$$\alpha \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = M \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$$

for an $n \times n$ matrix $M$ over $\mathbb{Z}$ that encodes the linear combinations for each $\alpha a_i$. We can rewrite this equation as

$$(\alpha I - M) \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = \mathbf{0},$$

where $I$ is the $n \times n$ identity matrix. Since we know the $a_i$ are not all zero, we know $\alpha I - M$ must have zero determinant. Evaluating this determinant gives

$$\alpha^n + \text{lower-degree terms} = 0,$$

which is a monic polynomial with integral coefficients with $\alpha$ as a root. □

**Example 4.1.** To clarify the proof of (4) $\implies$ (1), suppose we have $A = \mathbb{Z}[\sqrt{2}]$ and $\alpha = 3 + \sqrt{2}$. Note that $\alpha A \subseteq A$ and that $A$ is generated by $1, \sqrt{2}$. Then, we can write

$$\alpha \begin{pmatrix} 1 \\ \sqrt{2} \end{pmatrix} = \begin{pmatrix} 3 & 1 \\ 2 & 3 \end{pmatrix} \begin{pmatrix} 1 \\ \sqrt{2} \end{pmatrix}.$$

Moving everything to one side, we have

$$\left( \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix} - \begin{pmatrix} 3 & 1 \\ 2 & 3 \end{pmatrix} \right) \begin{pmatrix} 1 \\ \sqrt{2} \end{pmatrix} = \begin{pmatrix} \alpha - 3 & -1 \\ 2 & \alpha - 3 \end{pmatrix} \begin{pmatrix} 1 \\ \sqrt{2} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}.$$

Taking the determinant of the matrix gives $\alpha^2 - 6\alpha + 11 = 0$, which we can verify has $3 + \sqrt{2}$ as a root via the quadratic formula.

This theorem implies that the algebraic integers of any number field do indeed form a ring.

**Corollary 4.3.** *If $\alpha, \beta$ are algebraic integers, then so are $\alpha + \beta$ and $\alpha\beta$.*

Since addition and multiplication are commutative and associative, and this result tells us that addition and multiplication are indeed binary operations, we know that the ring of integers is indeed a ring.

*Proof.* Note that $\mathbb{Z}[\alpha]$ and $\mathbb{Z}[\beta]$ have finitely generated additive groups by characterization (1). Then, so does $\mathbb{Z}[\alpha, \beta]$, since it is generated by linear combinations of products of the generators for $\mathbb{Z}[\alpha]$ and $\mathbb{Z}[\beta]$.

Now, we note that $\mathbb{Z}[\alpha, \beta]$ must contain $\alpha + \beta$ and $\alpha\beta$ in order to be a ring extension, so by characterization (3), they are both algebraic integers. □

We will now set up Dedekind domains, which satisfy very useful properties. To do that, we will first set up integral domains.

**Definition 4.5.** An **integral domain** is a ring where the product of any two nonzero elements is nonzero.

**Definition 4.6.** A **Dedekind domain** $R$ is an integral domain satisfying the following:

(1) Ideals are finitely generated,
(2) Nonzero prime ideals are maximal,
(3) $R$ is integrally closed in its field of fractions $K = \{\alpha/\beta : \alpha, \beta \in R, \beta \neq 0\}$. So if $\alpha/\beta \in K$ is a root of a monic polynomial with coefficients in $R$, then we have $\alpha/\beta \in R$.

It turns out that the first condition is equivalent to the following:

- Every increasing sequence of ideals $I_1 \subseteq I_2 \subseteq \cdots$ is eventually constant; all $I_n$ are equal for sufficiently large $n$.
- Every nonempty set of ideals has a (not necessarily unique) maximal member. That is, there is some $M \in S$ such that whenever $M$ is a subset of an ideal $I$, then $M = I$.

**Example 4.2.** Again, $\mathbb{Z}$ is a Dedekind domain.

Ideals are finitely generated since all ideals are principal.

Prime ideals are also maximal, since for each prime $p$ there is no set $\{kn : k \in \mathbb{Z}\}$ for some $n \in \mathbb{Z}$ that is a subset of $(p)$.

Finally, $\mathbb{Z}$ is closed over its field of fractions $\mathbb{Q}$. Let $f(x)$ be a polynomial with integer coefficients with $\alpha \in \mathbb{Q}$ as a root. Then, we must have $\alpha \in \mathbb{Z}$ by the rational root theorem.

It turns out that all number rings are Dedekind domains, so our statements about Dedekind domains also apply to number rings. We will now set up the definition of the ideal class group.

**Definition 4.7.** Define an equivalence relation $\sim$ on the set of ideals of $\mathcal{O}$ by $\mathfrak{a} \sim \mathfrak{b}$ if and only if $\alpha\mathfrak{a} = \beta\mathfrak{b}$ for some $\alpha, \beta \in \mathcal{O}$. The number of equivalence classes of ideals under $\sim$ is the **class number** of $\mathcal{O}$, denoted $h$. These equivalence classes also form a group under multiplication of ideals, which is known as the **ideal class group**. Its elements are known as **ideal classes**.

We also have a second, equivalent definition, involving fractional ideals.

**Definition 4.8.** A **fractional ideal** of a number ring $R$ takes the form $\alpha\mathfrak{a}$ for $\alpha$ in the field of fractions of $R$, which takes the form $\{\beta/\gamma : \beta, \gamma \in R, \gamma \neq 0\}$, and $\mathfrak{a}$ an ideal of $R$, with $\alpha, \mathfrak{a}$ nonzero.

We can think of a fractional ideal as representing fractions with denominators in $\mathfrak{a}$.

And now, the definition itself.

**Definition 4.9.** The **ideal class group** of an algebraic number field $K$ is the quotient group $J_K/P_K$, where $J_K$ is the the group of fractional ideas of the ring of integers of $K$, and $P_K$ is the subgroup of the principal ideals of $J_K$. Its elements are also known as **ideal classes**.

Let's break down the second definition of the ideal class group.

We take the fractional ideals and mod out by the principal ideals $P_K$, so the elements of $J_K/P_K$ are cosets of the form $\alpha\mathfrak{a}P_K$ for all fractional ideal $\alpha\mathfrak{a} \in J_K$.

Each of our cosets can be thought of as the products of a fractional ideal with all principal ideals.

It turns out that Definitions 4.7 and 4.9 are equivalent. This mostly boils down to the cosets in Definition 4.9 in fact being the equivalence classes in Definition 4.7. For instance, let's just consider the identity element of both groups. Under the equivalence relation, they are simply the principal ideals (proved later). The identity element of our quotient group is the "denominator" of the quotient group, which are the principal ideals.

Now, why do we care about this ideal class group so much? Well, if our ideal class group is trivial, our number ring has unique factorization.

**Theorem 4.3.** *If a number ring $R$ has a trivial ideal class group, then it has unique factorization.*

*Proof.* Recall that a trivial group consists of the identity and nothing else. Further, recall that the principal ideals form the identity for the ideal class groups. Thus, a trivial ideal class group implies that all ideals are principal, so $R$ is a principal ideal domain, and thus has unique factorization. □

We also have the following theorem that implies the ideal classes of a Dedekind domain form a group.

**Theorem 4.4.** *For every ideal $\mathfrak{a}$ of a Dedekind domain $R$, there exists an ideal $\mathfrak{b}$ such that $\mathfrak{ab}$ is principal.*

See [Mar18, Chapter 3] for a complete proof of this theorem.

**Corollary 4.4.** *The ideal classes in a Dedekind domain form a group under multiplication of ideals.*

*Proof.* Let $R$ be a Dedekind domain.

Observe that multiplication is associative since normal multiplication (on real numbers) is. Similarly, the identity is the class containing (1), the principal ideal generated by the multiplicative identity.

We claim that all principal ideals are in the same class. This is true since for $\alpha, \beta \in R$, we have $\beta(\alpha) = \alpha(\beta)$.

Now, we show inverses exist. Let $\mathfrak{a}$ be an ideal that represents an equivalence class. Then, by Theorem 4.4, there exists some ideal $\mathfrak{b}$ such that $\mathfrak{ab}$ is a principal ideal, which we showed above is a representative of our identity element. □

## 5. Putting it together

It is possible to prove that the ideal class group is finite for all number rings; this proof involves thinking about number rings as lattices and volumes on that lattice. However, we choose to prove the case with quadratic rings, as they have a nice connection with binary quadratic forms.

First, we will define a discriminant for quadratic number ring, which is an invariant related to an integral basis of the ring.

**Definition 5.1.** Let $R$ be the ring of integers of a number field $K$. An **integral basis** of $R$ is a set $\{\beta_1, \ldots, \beta_n\} \in R$ such that every $\alpha \in R$ can be uniquely represented by

$$m_1\beta_1 + \cdots + m_n\beta_n, m_i \in \mathbb{Z}.$$

The set $\{\beta_1, \ldots, \beta_n\}$ is also known as a basis for $R$ over $\mathbb{Z}$, or a basis for $K$ over $\mathbb{Q}$.

Also, we have the **discriminant** of the integral basis be

$$\operatorname{disc}(\beta_1, \ldots, \beta_n) = |\sigma_i(\alpha_j)|^2,$$

where the $\sigma_i$ denote embeddings of $K \in \mathbb{C}$, and $\sigma_i(\alpha_j)$ is the matrix where the entry in the $i$th row and $j$th column is $\sigma_i(\alpha_j)$.

**Definition 5.2.** The **discriminant** of a number ring is the unique discriminant of its integral bases. In the case of the number ring being $\mathbb{A} \cap Q(\sqrt{D})$, it can be shown to be

$$\begin{cases} d, & d \equiv 1 \pmod 4, \\ 4d, & d \equiv 2, 3 \pmod 4. \end{cases}$$

See [Mar18, Chapter 2] for an in-depth explanation of integral bases and the equivalence claimed in this definition.

**Theorem 5.1.** *The class group for quadratic forms with discriminant $D$ is isomorphic to the ideal class group of the ring of integers of $\mathbb{Q}(\sqrt{D})$ for $D < 0$.*

*In particular, the isomorphism takes the primitive positive definite binary quadratic form $ax^2 + bxy + cy^2$ to the ideal generated by the set $\left\{a, \frac{-b+\sqrt{D}}{2}\right\}$.*

*Proof.* See [Cox22, Chapter 5]. □

**Corollary 5.1.** *The ideal class group of the ring of integers of the quadratic number field $\mathbb{Q}(\sqrt{D})$ is finite for $D < 0$.*

*Proof.* Let the ring of integers of $\mathbb{Q}(\sqrt{D})$ be $\mathcal{O}$. By Theorem 5.1, we know the ideal class group of $\mathcal{O}$ has the same cardinality as the class group for quadratic forms with discriminant $D$, which we know by Theorem 2.3 to be finite. □

## References


[Cox22] David A. Cox. *Primes of the form $x^2 + ny^2$. Fermat, class field theory, and complex multiplication. Third edition with solutions. With contributions by Roger Lipsett*, volume 387 of *AMS Chelsea Publ.* Providence, RI: American Mathematical Society (AMS), 3rd edition edition, 2022.

[Mar18] Daniel A. Marcus. *Number fields.* Universitext. Cham: Springer, 2nd edition edition, 2018.

[SO85] Winfried Scharlau and Hans Opolka. *From Fermat to Minkowski. Lectures on the theory of numbers and its historical development. Transl. from the German by Walter Kaufmann- Bühler and Gary Cornell.* Undergraduate Texts Math. Springer, Cham, 1985.