Class Groups of Quadratic Forms

Wilson Chen

June - July 2022

Abstract

Quadratic Forms and Number Fields are completely different fields in abstract algebra, how can they be connected? In this paper, we will discuss several characteristics of quadratic forms including primitive, reduced, positive definite as well as its connection with algebraic number theory such as the ring theory, number fields, ideal class groups and class numbers. We will also introduce the Minkowski's Theorem and Bound and prove it. In the end, we will cover the general procedure and include an example of using the MinKowski Bound to compute the class number of quadratic number field.

1 Introduction

The theory of quadratic has a long history and its origin could be traced back during ancient Babylonia between 1900 and 1600 BC, which then taken up again by Brahmagupta in the Seventh Century, and thousands years later by the great genius Fermat, followed by a succession of extraordinary mathematicians, including Euler, Lagrange, and Gauss, who brought the subject closer to its modern form. The work of Minkowski in the late Nineteenth Century, coupled with the extension of his work by Hasse in the early Twentieth Century, led to a great broadening and deepening of the theory that has served as the foundation for an enormous amount of research that continues today.

This paper's goal is to give a heuristic description of the concept of quadratic forms and class groups to those with limited background in number theory. This paper is dedicated to show how the idea originally developed and how it implies the more common definition found in today's texts.

The organization of the paper is as following:

In 2, we introduce the basic definition and characteristics of quadratic forms.
In 3, we discuss the basic concept of algebraic numbers such as rings, number fields, ideals
In 4, we discuss the bijection among class groups and quadratic form

In 5, we discuss the geometry of numbers and introduce the Minkowski Theoreom and Bound
In 6, we provide the general procedure of finding class number of quadratic number field with an example
In 7, we recognize help and advise from various people.

2 Quadratic Forms

2.1 Basic Definition

An integral binary quadratic form is a polynomial of the type $f(x,y) = ax^2 + bxy + cy^2$, where a, b, and c are integers. A form is primitive if the integers a, b, and c are relatively prime. Note that any form is an integer multiple of a primitive form. Throughout, we will assume that all forms are primitive. We say that a form f represents an integer n if $f(x,y) = n$ has an integer solution; the representation is proper if the integers x, y are relatively prime. A form is positive definite if it represents only positive integers.

The discriminant of $f = ax^2 + bxy + cy^2$ is defined as $\Delta = b^2 - 4ac$. Observe that $4af(x,y) = (2ax + by)^2 - \Delta y^2$. Thus, if $\Delta < 0$, the form represents only positive integers or only negative integers, depending on the sign of a. In particular, if $\Delta < 0$ and $a > 0$ then $f(x,y)$ is positive definite. Moreover, $\Delta = b^2 - 4ac$ implies that $\Delta \equiv b^2 (\mathrm{mod} 4)$. Thus we have $\Delta \equiv 0 (\mathrm{mod} 4)$ or $\Delta \equiv 1 (\mathrm{mod} 4)$, depending on whether b is even or odd.

2.2 Reduced Quadratic Form

Definition: A positive definite binary quadratic form $f(x,y) = ax^2 + bxy + cy^2$ is said to be Reduced if one of the following inequalities hold:
1) $-a < b \leq a < c$
2) $0 < b \leq a = c$
Let:

$$M_1 = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \quad , \quad M_2 = \begin{bmatrix} 1 & m \\ 0 & 1 \end{bmatrix}$$

Observe that $det(M_1) = 1$ and $det(M_2) = 1$. If $f(x,y) = ax^2 + bxy + cy^2$ then under M_1 we have:

$$\begin{aligned} f(0x - 1y, 1x + 0y) &= f(-y, x) \\ &= a(-y)^2 + b(-y)(x) + c(x)^2 \\ &= ay^2 - bxy + cx^2 \\ &= cx^2 - bxy + ay^2 \\ &= a'x^2 + b'xy + c'y^2 \end{aligned} \tag{1}$$

where $a' = c, b' = -b$, and $c' = a$. So if $a > c$ then $a' = c < a = c'$. So if $f(x, y)$ is such that the coefficient of x^2 is greater than the coefficient of y^2 then applying M_1 to $f(x, y)$ gives us an equivalent binary quadratic form where the coefficient of x^2 is less than the coefficient of y^2.

If $f(x, y) = ax^2 + bxy + cy^2$ then under M_2 we have:

$$\begin{aligned} f(1x + my, 0x + 1y) &= f(x + my, y) \\ &= a(x + my)^2 + b(x + my)(y) + c(y)^2 \\ &= a\left(x^2 + 2mxy + m^2y^2\right) + b\left(xy + my^2\right) + cy^2 \\ &= ax^2 + 2amxy + am^2y^2 + bxy + bmy^2 + cy^2 \\ &= ax^2 + (2am + b)xy + (am^2 + bm + c)y^2 \\ &= a'x^2 + b'xy + c^{prime}y^2 \end{aligned} \tag{2}$$

where $a' = a, b' = 2am + b$, and $c' = am^2 + bm + c$. If $b > a$ then m can be chosen such that:

$$-a' = -a < 2am + b = b' < a = a'$$

Therefore, if $f(x, y)$ is such that the coefficient of xy is greater than the coefficient of x^2 then applying M_2 to $f(x, y)$ gives us an equivalent binary quadratic form such that the coefficient of xy is less than the coefficient of x^2.

Theorem 1: Let $f(x, y) = ax^2 + bxy + cy^2$ be a reduced binary quadratic form with discriminant $d \in Z$ where d is not a perfect square.

a) If f is indefinite then $0 < |a| \leq \frac{1}{2}\sqrt{d}$.

b) If f is positive definite then $0 < a \leq \sqrt{\frac{-d}{3}}$.

Proof of a):

Proof. Suppose that f is indefinite and is a reduced binary quadratic form. Then $d > 0$ and $-a < b \leq a < c$. If a and c have the same signs then $ac > 0$. So $ac > a^2$.[MzK04] Hence:

$$d = b^2 - 4ac \leq a^2 - 4ac \leq a^2 - 4a^2 = -3a^2 < 0$$

Which is a contradiction. So a and c must have different signs, and hence $-4ac = 4|ac|$. Thus:

$$d = b^2 - 4ac = b^2 + 4|ac| \geq 4|ac| \geq 4a^2$$

Dividing both sides by 4 and taking the squareroot of both sides of the inequality gives us:

$$|a| \leq \frac{1}{2}\sqrt{d}$$

If $a = 0$ then the inequality $0 < b \leq a = c$ cannot be satisfied, and so:

$$0 < |a| \leq \frac{1}{2}\sqrt{d}$$

□

Proof of b)

Proof. Suppose that f is positive definite and is a reduced binary quadratic form. Then $d < 0$ and $a, c > 0$, and $-a < b \leq a < c$. So:

$$d = b^2 - 4ac \leq a^2 - 4ac \leq a^2 - 4a^2 = -3a^2$$

Dividing both sides by -3 and taking the squareroot of both sides gives us that:

$$|a| \leq \sqrt{\frac{-d}{3}}$$

The absolute value bars on a are removed since $a > 0$, and so:

$$0 < a \leq \sqrt{\frac{d}{-3}}$$

□

2.3 Representation of Integers by Binary Quadratic Forms

The earliest investigations concerning the representation of integers by binary quadratic forms were due to Fermat. In correspondence to Pascal and Marsenne, he claimed to have proved the following:

1) Every prime number of the form 4k + 1 can be represented by $x^2 + y^2$

2) Every prime number of the form 3k + 1 can be represented by $x^2 + 3y^2$

3) Every prime number of the form 8k + 1 or 8k + 3 can be represented by $x^2 + 2y^2$

In general, an integer n is represented by the binary quadratic form $ax^2 + bxy + cy^2$ if there exist integers r and s such that $n = ar^2 + brs + cs^2$. In the seventeenth century Fermat showed the first such result, that the primes represented by the binary quadratic form $x^2 + y^2$ are 2 and those primes $\equiv 1 (\bmod 4)$, and thence determined all integers that are the sum of two squares. One can similarly ask for the integers represented by $x^2 + 2y^2$, or $x^2 + 3y^2$, or $2x^2 + 3y^2$, or any binary quadratic form $ax^2 + bxy + cy^2$.

The integers n that are represented by $x^2 + 2xy + 2y^2$ are the same as those represented by $x^2 + y^2$, for if $n = u^2 + 2uv + 2v^2$ then $n = (u + v)^2 + v^2$, and if

$n = r^2 + s^2$ then $n = (r-s)^2 + 2(r-s)s + 2s^2$. Thus we call these two forms equivalent. In general, binary quadratic form f is equivalent to $F(X,Y) = f(\alpha X + \beta Y, \gamma X + \delta Y)$ whenever $\alpha, \beta, \gamma, \delta$ are integers with $\alpha\delta - \beta\gamma = 1$, [1] and so f and F represent the same integers. Therefore to determine what numbers are represented by a given binary quadratic form, we can study any binary quadratic form in the same equivalence class. If $f(x,y) = ax^2 + bxy + cy^2$ and $F(X,Y) = AX^2 + BXY + CY^2$ above, note that $A = f(\alpha, \gamma), C = f(\beta, \delta)$ and $B^2 - 4AC = b^2 - 4ac$ (in fact $B - b = 2(a\alpha\beta + b\beta\gamma + c\gamma\delta)$).

3 Algebraic Number Theory

3.1 Groups

A group is a pair $G = (G, \star)$ consisting of a set of elements G, and a binary operation $\star$ on G, such that:

1) G has an identity element, usually denoted 1_G or just 1 , with the property that

$$1_G \star g = g \star 1_G = g \text{ for all } g \in G.$$

2)The operation is associative, meaning $(a \star b) \star c = a \star (b \star c)$ for any $a, b, c \in G$. Consequently we generally don't write the parentheses.

3) Each element $g \in G$ has an inverse, that is, an element $h \in G$ such that

$$g \star h = h \star g = 1_G.$$

For example, the pair $(Z, +)$ is a group: $Z = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ is the set and the associative operation is addition. [Che16] Note that

1) The element $0 \in Z$ is an identity: $a + 0 = 0 + a = a$ for any a.

2) Every element $a \in Z$ has an additive inverse: $a + (-a) = (-a) + a = 0$. We call this group Z

3.2 Rings

A ring is a set R together with two operations $(+)$ and $(\cdot)$ satisfying the following properties (ring axioms):

(1) R is an abelian group under addition. That is, R is closed under addition, there is an additive identity (called 0), every element $a \in R$ has an additive

inverse $-a \in R$, and addition is associative and commutative.

(2) R is closed under multiplication, and multiplication is associative[MzK04]:

$$\begin{array}{rl} \forall a, b \in R & a \cdot b \in R \\ \forall a, b, c \in R & a \cdot (b \cdot c) = (a \cdot b) \cdot c \end{array}$$

(3) Multiplication distributes over addition:

$$\forall a, b, c \in R \quad a \cdot (b + c) = a \cdot b + a \cdot c \quad \text{and} \quad (b + c) \cdot a = b \cdot a + c \cdot a$$

A ring is usually denoted by $(R, +, \cdot)$ and often it is written only as R when the operations are understood.

The ring R is commutative if x is commutative.

Note that:
(a) The sets Z, Q, R and C are all rings with the usual addition and multiplication.

(b) The integers modulo n are also a ring with the usual addition and multiplication. We also denote it by Z/nZ.

(c) The zero ring is the ring R with a single element. We denote the zero ring by 0 . A ring is nontrivial if it is not the zero ring.[Cox11]

The study of rings has its roots in algebraic number theory, via rings that are generalizations and extensions of the integers, as well as algebraic geometry, via rings of polynomials. These kinds of rings can be used to solve a variety of problems in number theory and algebra; one of the earliest such applications was the use of the Gaussian integers by Fermat, [Row12] to prove his famous two-square theorem. There are many examples of rings in other areas of mathematics as well, including topology and mathematical analysis.

3.2.1 Examples of a ring

This section lists many of the common rings and classes of rings that arise in various mathematical contexts.

(1) The ring Z of integers is the canonical example of a ring. It is an easy exercise to see that Z is an integral domain but not a field.

(2) There are many other similar rings studied in algebraic number theory, of the form $Z[\alpha]$, where α is an algebraic integer. For example, $Z[\sqrt{2}] = \{a+b\sqrt{2} : a, b \in Z\}$ is a ring, an integral domain, to be precise. Also we have the ring of Gaussian integers $Z[i] = \{a+bi : a, b \in Z\}$, where i is the imaginary unit.[Che16]

(3) If R is a ring, then so is the ring $R[x]$ of polynomials with coefficients in R. In particular, when $R = Z/pZ$ is the finite field with p elements, $R[x]$ has many similarities with Z. For example, there is a Euclidean algorithm and hence unique factorization into irreducibles. See the introduction to algebraic number theory for details.

More generally, if X is a set and R is a ring, the set of functions from X to R is a ring, with the natural operations of pointwise addition and multiplication of functions. For many sets X, this ring has many interesting subrings constructed by restricting to functions with properties that are preserved under addition and multiplication. If $X = R = R$, for instance, there are subrings of continuous functions, differentiable functions, polynomial functions, and so on.

(4) The set of $n \times n$ matrices with entries in a commutative ring R is a ring, which is non-commutative for $n \geq 2$. This ring has a unity, the identity matrix. But it may have divisors of zero. E.g. $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$. This shows that $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ and $\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ are divisors of zero in the ring $M_2(R)$.

3.2.2 Properties of a ring

If $ab = 0$ in R and a and b are nonzero, then a and b are called zero-divisors. A ring with no zero-divisors is called a domain, and a commutative domain is called an integral domain.[Jar14]

If $n = ab$ is composite (where $1 < a, b < n$), then $ab \equiv 0 \bmod n$ but a and b are nonzero mod n because they are strictly smaller than n. So $Z/(n)$ is not an integral domain when n is composite.

On the other hand, if n is prime and $ab \equiv 0 \bmod n$, then $n \mid ab$, so $n \mid a$ or $n \mid b$ because n is prime. So then either a or b is 0 mod n. So $Z/(n)$ is an integral domain when n is prime.[Ser12]

The integral domain condition is weaker than the field condition:

Every field is an integral domain, but not every integral domain is a field.

Here is the proof:

Proof. First there is a Lemma: For all elements a of a ring $R, a \cdot 0 = 0 \cdot a = 0$.

Proof of lemma: Since 0 is the additive identity, $0+0 = 0$. Then $a \cdot 0 + a \cdot 0 = a \cdot 0$ by the distributive law. But we can add the additive inverse of $a \cdot 0$ to both sides, to get $a \cdot 0 = 0$. The proof of $0 \cdot a$ is similar.[Ser12]

Now for the proof of the result. If every nonzero element has a multiplicative inverse, suppose $ab = 0$ but a and b are nonzero. Then multiply both sides by a^{-1} to get $a^{-1}ab = a^{-1}0 = 0$, so $b = 0$, contradiction. So there are no zero-divisors.[Jar14]

To see that not every integral domain is a field, simply note that Z is an example of an integral domain that is not a field (since e.g. 2 does not have a multiplicative inverse in Z) □

3.3 Quotient

Given a ring R and an ideal I, there is an object called the quotient ring R/I. The example to keep in mind is $R = Z$ and $I =$ the ideal generated by an integer n. Then $R/I = Z/(n)$ is the familiar ring of integers mod$n$.

The ring R/I is the set of elements $\bar{a}$, where $a \in R$. Two expressions $\bar{a}$ and $\bar{b}$ are equal in R/I if and only if $a - b \in I$. Elements are added and multiplied just as they are in $R : \bar{a} + \bar{b} = \overline{a+b}$ and $\bar{a} \cdot \bar{b} = \overline{ab}$.[Coh94]

The subtle part of this definition is that it is well-defined: that is, the arithmetic in R/I gives the same results no matter which representative a of an element $\bar{a}$ is picked. (Again, the example to keep in mind is $Z/(n)$.)[Coh94]

3.4 Ideals

An ideal I in a commutative ring R is a nonempty set that

(1) is closed under addition.

(2) "swallows up" under multiplication: if $r \in R$ and $a \in I$, then $ra \in I$.[Che16]

If $a_1, a_2, \ldots, a_n \in R$, the set

$$(a_1, a_2, \ldots, a_n) = \{r_1a_1 + r_2a_2 + \cdots + r_na_n : r_i \in R\}$$

is an ideal, and is called the ideal generated by the a_i.

The ideal generated by one element, (a), the set of multiples of a, is called a principal ideal. A ring in which every ideal is principal is called a principal

ideal ring.

3.4.1 Properties of ideal

An ideal I of a ring R is prime if $I \neq R$ and $ab \in I \Rightarrow a \in I$ or $b \in I$.

An ideal I of a ring R is maximal if $I \neq R$ but any ideal that strictly contains I is the entire ring R. (That is, for an ideal $J, I \subseteq J \subseteq R$ implies $I = J$ or $J = R$.)[MzK04]

For example, The ideal (3) of Z is prime, because if $ab \in (3)$, then $3 \mid ab$, so $3 \mid a$ or $3 \mid b$ (because 3 is a prime number), so $a \in (3)$ or $b \in (3)$.

It is also maximal, because if J is an ideal strictly containing I, then there is an element $j \in J$ that is not a multiple of 3 . Now, since gcd $(3, j) = 1$, there are $x, y \in Z$ such that $3x + jy = 1$ by Bezout's identity, but $3x$ and jy are both in J, so their sum is, so $1 \in J$.

But then for any $r \in R, r = 1 \cdot r$ is in J, so $J = R$.[Cox11]

On the other hand, (4) is neither prime nor maximal, because $2 \cdot 2 \in (4)$ but $2 \notin (4)$; and the ideal (2) is strictly larger than (4) but is not the entire ring.

Theorem 1. *Let R be a commutative ring, and let I be an ideal not equal to R. Then:*

(1) R/I is an integral domain if and only if I is prime.

(2) R/I is a field if and only if I is maximal.

Here is the proof:

Proof. (1) comes directly from the definitions: if R/I is an integral domain and $ab \in I$, then $\bar{a}\bar{b} = 0$ in R/I, so $\bar{a} = 0$ or $\bar{b} = 0$, so $a \in I$ or $b \in I$, so I is prime. The converse is similar.

For (2), suppose I is maximal; then take a nonzero element $\bar{a} \in R/I$. Then

$$(a, I) = \{ax + i : x \in R, i \in I\}$$

is an ideal, and it's strictly bigger than I since it contains $a \notin I$. So it must equal the whole ring R, and in particular it contains 1. So there exist $x_0 \in R, i_0 \in I$ such that $ax_0 + i_0 = 1$, and in R/I this becomes

$$\overline{ax}_0 = \overline{1}$$

so a has a multiplicative inverse in R/I. This shows that R/I is a field. The converse is similar. □

3.4.2 Principal Ideals and Principal Ideal Domains

Recall from the Ideals of Rings that if $(R, +, *)$ is a ring then an ideal if a subring $(I, +, *)$ such that for all $r \in R$ and for all $i \in I$ we have that $r*i \in I$ and $i*r \in I$.

We now define a special type of ideal called a principal ideal.

Definition: Let $(R, +, *)$ be a commutative ring. An ideal of the form $aR = \{a * r : r \in R\}$ is called a Principal Ideal generated by a.

It is easy to verify that if R is a commutative ring then for every $a \in R, aR$ is indeed an ideal of R. To show this, let $q \in R$ and let $ar \in aR$. Then $qar = a(qr) \in aR$. Similarly, $(ar)q = a(qr) \in aR$.

For example, consider the ring of integers Z. Then $2Z = \{0, \pm 2, \pm 4, \ldots\}$ is a principal ideal and is generated by 2 .

In fact, the principal ideal generated by $k \in Z$ is:

$$kZ = \{0, \pm k, \pm 2k, \ldots\}$$

Definition: Let $(R, +, *)$ be an integral domain. Then R is said to be a Principal Ideal Domain (PID) if every ideal in ($R, +, *$) is a principal ideal.

For example, consider the set of integers Z. We will prove that Z is a principal ideal domain. Let I be an ideal of R.

First suppose that $I = \{0\}$. Then $I = 0R$, so I is a principal ideal.

Now instead suppose that $I \neq \{0\}$. Then there exists a smallest positive integer $a \in I$ such that $a > 0$. Now let $b \in I$ and suppose that $b > a$. By the division algorithm there exists $q, r \in R$ such that $b = aq + r$ with $0 \leq r < a$. So $r = b - aq$. Since $a \in I$ and $q \in R$ we have that $aq \in I$. So $b - aq \in I$. This shows that $r \in I$. Since a is the smallest positive integer in I, we must have that $r = 0$. So $b = aq$. So every element in I is of the form $b = aq$, so $I = aR$. Hence I is a principal ideal.

So every ideal of Z is a principal ideal, so Z is a principal ideal domain.

3.4.3 Fractional Ideals

Definition: Let R be a commutative domain and K its field of fractions. A fractional ideal of R is an R module I contained in K, such that for a certain non zero $a \in \bar{R}$ we have $aI \subset R$.

For example, the set

$$\frac{5}{2}Z = \left\{ \frac{5}{2}n \mid n \in Z \right\} = \frac{1}{2}(5)$$

is a fractional ideal of Z.

In other word, a fractional ideal is a generalization of an ideal in a ring R. Instead, a fractional ideal is contained in the number field F, but has the property that there is an element $b \in R$ such that

$$a = bf = \{bx \text{ such that } x \in f\}$$

is an ideal in R. In particular, every element in f can be written as a fraction, with a fixed denominator.

$$f = \{a/b \text{ such that } a \in a\}$$

Note that the multiplication of two fractional ideals is another fractional ideal. For example, in the field $Q(\sqrt{-5})$, the set

$$f = \left\{ \frac{2a_1 + a_2 - 5a_4 + (a_2 + 2a_3 + a_4)\sqrt{-5}}{3 + \sqrt{-5}} \right.$$

such that $a_i \in Z\}$ is a fractional ideal because

$$(3 + \sqrt{-5})f = \langle 2, 1 + \sqrt{-5} \rangle.$$

3.5 Number Fields and Its properties

Definition: A number field K is a field containing Q as a subfield which is a finite-dimensional Q-vector space. The degree of K is its dimension.

If r is an algebraic number of degree n, then the totality of all expressions that can be constructed from r by repeated additions, subtractions, multiplications, and divisions is called a number field (or an algebraic number field) generated by r, and is denoted $F[r]$. Formally, a number field is a finite extension $Q(\alpha)$ of the field Q of rational numbers.

The elements of a number field which are roots of a polynomial

$$z^n + a_{n-1}z^{n-1} + \ldots + a_0 = 0$$

with integer coefficients and leading coefficient 1 are called the algebraic integers of that field.

The coefficients of an algebraic equations such as the quintic equation can be characterized by the groups of their associated number fields. A database of the groups of number field polynomials is maintained by Klüners and Malle. For example, the polynomial $x^5 - x^4 + 2x^3 - 4x^2 + x - 1$ is associated with the group F (5) of order 20.

An order of an algebraic number field K is a subring $\mathcal{O} \subseteq \mathcal{O}_K$ which is also a Z-module of rank $n = [K : Q]$.

Let's say I have $K = Q(\sqrt{2})$. As we've seen before, this means $\mathcal{O}_K = Z[\sqrt{2}]$, meaning

$$\mathcal{O}_K = \{a + b\sqrt{2} \mid a, b \in Z\}$$

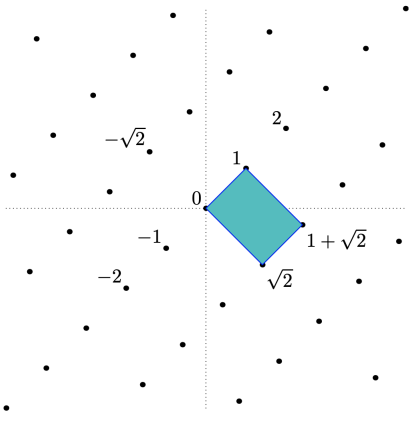
We can then think of this as a lattice, which connects to the geometrically of algebraic number. Thus, we want to think about this the same way we think about Z^2. We could embed this into Q^2 by sending $a + b\sqrt{2}$ to (a, b), but a better way is to think about the fact that there are two embeddings $\sigma_1 : K \to C$ and $\sigma_2 : K \to C$, namely the identity, and conjugation:

$$\sigma_1(a + b\sqrt{2}) = a + b\sqrt{2}$$
$$\sigma_2(a + b\sqrt{2}) = a - b\sqrt{2}$$

We can see that these embeddings both have real image. This leads us to consider the set of points

$$(\sigma_1(\alpha), \sigma_2(\alpha)) \in R^2 \quad \text{as} \quad \alpha \in K.$$

This lets us visualize what $\mathcal{O}_K$ looks like in R^2. The points of K are dense in R^2, but the points of $\mathcal{O}_K$ cut out a lattice.[Che16]



To see how big the lattice is, we look at how $\{1, \sqrt{2}\}$, the generators of $\mathcal{O}_K$, behave.

The point corresponding to $a + b\sqrt{2}$ in the lattice is

$$a \cdot (1, 1) + b \cdot (\sqrt{2}, -\sqrt{2})$$

The mesh of the lattice [1] is defined as the hypervolume of the "fundamental parallelepiped" which is colored blue above. For this particular case, it ought to be equal to the area of that parallelogram, which is

$$\det \begin{bmatrix} 1 & -\sqrt{2} \\ 1 & \sqrt{2} \end{bmatrix} = 2\sqrt{2}$$

Suppose $\alpha_1, \ldots, \alpha_n$ is a Z-basis of $\mathcal{O}_K$. The discriminant of the number field K is defined by

$$\Delta_K := \det \begin{bmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_n(\alpha_1) \\ \vdots & \ddots & \vdots \\ \sigma_1(\alpha_n) & \cdots & \sigma_n(\alpha_n) \end{bmatrix}^2$$

Note that this does not depend on the choice of the $\{\alpha_i\}$.

4 Bijection Among Class Groups and Quadratic Form

Let $F = ax^2 + bxy + cy^2$ be a binary quadratic form over Z. We say $D = b^2 - 4ac$ is the discriminant of F. If D is not a square integer and $\gcd(a, b, c) = 1$, we say $ax^2 + bxy + cy^2$ is primitive. If $D < 0$ and $a > 0$, we say $ax^2 + bxy + cy^2$ is positive definite.

Let K be a quadratic number field. Let R be an order of K. Let D be its discriminant. Let I be a fractional ideal of R. If there exists a fractional ideal J of R such that $IJ = R, I$ is called an invertible fractional ideal of R. The set of invertible fractional ideals of R forms a group $J(R)$ with the multiplications. We call $J(R)$ the group of invertible fractional ideals of R. We denote by $P(R)$ the group of principal fractional ideals of R.$P(R)$ is a subgroup of $J(R)$. We denote $J(R)/P(R)$ by $Cl(R)$.$Cl(R)$ is called the ideal class group of R. Let $P^+(R) = \{\alpha R; \alpha \in K, N_{K/Q}(\alpha) > 0\}$. $P^+(R)$ is a subgroup of $P(R)$. We denote $F(R)/P^+(R)$ by $Cl^+(R)$. If K is a imaginary quadratic field, $Cl(R) = Cl^+(R)$. We would like to establish a bijection between $Cl^+(R)$ and the set of classes of primitive binary quadratic forms of discriminant D.

Let $\alpha, \beta \in K$. We denote $\alpha\beta' - \alpha'\beta$ by $\Delta(\alpha, \beta)$, where α' (resp. β') is the conjugate of α (resp. β). $\Delta(\alpha, \beta) \neq 0$ if and only if α, β are linearly independent over Q.

If $D < 0$, we define $\sqrt{D}$ as $i\sqrt{|D|}$

Let $I \neq 0$ be a fractional ideal of R. Let $\{\alpha, \beta\}$ be Z-basis of I. If $\Delta(-\alpha, \beta)/\sqrt{D} > 0$, we say the basis $\{\alpha, \beta\}$ is positively oriented. If $\Delta(-\alpha, \beta)/\sqrt{D} < 0$, we say the basis $\{\alpha, \beta\}$ is negatively oriented. Suppose $\{\alpha, \beta\}$ and $\{\gamma, \delta\}$ are two positively oriented bases of I. There exist integers p, q, r, s such that

$$\alpha = p\gamma + q\delta$$

$$\beta = r\delta + s\delta$$

It is easy to see that $ps - qr = 1$.

I can be written as $I = J/\lambda$, where J is an ideal of R and $\lambda \in R$. We define the norm of I as $N(I) = N(J)/N(\lambda R)$. It is easy to see that this is well defined.

Let x, y be indeterminates. Let $\{\alpha, \beta\}$ be a positively oriented basis of I. We write $f(\alpha, \beta; x, y) = N_{K/Q}(x\alpha - y\beta)/N(I)$. Namely $f(\alpha, \beta; x, y) = (x\alpha - y\beta)(x\alpha' - y\beta')/N(I)$. It is easy to see that $f(\alpha, \beta; x, y)$ is a binary quadratic form of discriminant D. It is also easy to see that $f(\alpha, \beta; x, y)$ is positive definite if $D < 0$.

Suppose $\{\alpha, \beta\}$ and $\{\gamma, \delta\}$ are two positively oriented bases of I. It is a routine to check that $f(\alpha, \beta; x, y)$ and $f(\gamma, \delta; x, y)$ are equivalent under the action of $SL_2(Z)$. By the corollary of proposition 2 of this question, if I is invertible, $f(\alpha, \beta; x, y)$ is primitive.

Let $\{\alpha, \beta\}$ be a positively oriented basis of I. Let δ be an element of K such that $N_{K/Q}(\delta) > 0$. Then $\{\delta\alpha, \delta\beta\}$ is a positively oriented basis of the farctional ideal δI.

$$f(\delta\alpha, \delta\beta; x, y) = N_{K/Q}(x\delta\alpha - y\delta\beta)/N(\delta I) = \left(N_{K/Q}(\delta)/\left|N_{K/Q}(\delta)\right|\right) f(\alpha, \beta; x, y)$$

Hence $f(\delta\alpha, \delta\beta; x, y) = f(\alpha, \beta; x, y)$

Hence we get a map $\psi : Cl^+(R) \to F_0^+(D)/SL_2(Z)$ if $D < 0$ and $\psi : Cl^+(R) \to F_0(D)/SL_2(Z)$ if $D > 0$, where $F_0(D)$ is the set of primitive binary quadratic forms of discriminant D and $F_0^+(D)$ is the set of positive definate primitive binary quadratic forms of discriminant D.

5 Geometry of Algebraic Number

5.1 Class Fields

Let K be a number field, and let J_K denote the multiplicative group of fractional ideals of $\mathcal{O}_K$. Let P_K denote the multiplicative group of principal fractional ideals: those of the form $(x) = x\mathcal{O}_K$ for some $x \in K$.

As J_K is abelian, we can now define the class group to be the quotient

$$\mathrm{Cl}_K := J_K / P_K$$

The elements of Cl_K are called classes. Equivalently, The class group Cl_K is the set of nonzero fractional ideals modulo scaling by a constant in K.

In particular, Cl_K is trivial if all ideals are principal, since the nonzero principal ideals are the same up to scaling.

The size of the class group is called the class number.

5.2 Minkowski's Theorem

Theorem 1. Let $K \subset R^n$ be a bounded, convex, centrally symmetric set (meaning that $x \in S \iff -x \in S$). If in addition the volume of K satisfies vol $K > 2^n$, then K contains at least one non-trivial lattice point of Z^n.

Theorem 2. Let $K \subset R^n$ be a bounded, convex, centrally symmetric set, which in addition is also compact (thus contains its boundary). If the volume of K satisfies vol $K \geq 2^n$, then K contains at least one non-trivial lattice point of Z^n.

Note that Theorem 2 is a simple consequence of Theorem 1 and an elementary compactness argument. Let's suppose that the volume of K satisfies vol $K = 2^n$. For each $\epsilon > 0$, let K_ϵ be the dilate $K(1+\epsilon)$. Notice that the sets K_ϵ satisfy the assumption that vol $K_\epsilon > 2^n$, thus by Theorem 1, K_ϵ contains a nonzero lattice point of Z^n. But K_1 is bounded, so there are only finitely many possibilities for this nonzero lattice point for each $\epsilon \leq 1$. Thus, we can find a sequence of ϵ 's tending to 0 for which this lattice point is the same. The convexity of the sets K_ϵ, in combination with the fact that the sets contain 0, implies that the sets are nested, and therefore this lattice point lies in K_ϵ for all $\epsilon > 0$. Since K is compact, we have that

$$K = \bigcap_{\epsilon > 0} K_\epsilon,$$

and therefore this lattice point lies in K.

Thus, we will focus on the proof for Theorem 1.

Proof. The idea is to look again at the cube $\mathbf{Q} = [-1, 1]^n$ (this time its closed version). Note that this cube is centered at the origin and that all its translates by even coordinate vectors partition R^n. More formally, we can thus say that

$$R^n = \bigcup_{u \in 2Z^n} (\mathbf{Q} + u).$$

For conveniece, let us denote $\mathbf{Q} + u$ by $\mathbf{Q}_u$. Note that K is bounded, thus K intersects only a finite set of these $\mathbf{Q}_u$'s, call it $\mathcal{Q}$. Now, let us look at the sets $\mathbf{Q}_u$ from $\mathcal{Q}$ and their translations back to $\mathbf{Q}$. These translations will create an agglomeration of parts of K inside $\mathbf{Q}$. However, we know that $\operatorname{vol} K > 2^n$, whereas $\operatorname{vol} \mathbf{Q} = 2^n$. Therefore, there will be at least an overlap of two translated $\mathbf{Q}_u$'s; pick some point x lying in this overlap. This point x can be thus written as $x = v + y = w + z$ for some distinct points y, z in K and some distinct vectors v, w in $2Z^n$. In particular, we get that the point $\frac{y-z}{2} = \frac{w-v}{2}$ is in Z^n. But $y \in K$ and $-z \in K$ (as z is in K and K is centrally symmetric); thus the convexity of K yields that $\frac{y-z}{2}$ is also K, which means that $\frac{y-z}{2}$ is a non-zero lattice point that lies in K. This proves Minkowski's theorem. □

5.3 The Minkowski Bound

Let $a \subseteq \mathcal{O}_K$ be any nonzero ideal. Then there exists $0 \neq \alpha \in a$ such that

$$\mathrm{N}_{K/Q}(\alpha) \leq \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} \sqrt{|\Delta_K|} \cdot \mathrm{N}(a).$$

6 Finding Class Number of Quadratic Number Field

In the general case, one has a quadratic number field F, which is always of the form $Q(\sqrt{d})$ for some square-free integer d.

Minkowski Bound Theorem states that every equivalence class in the ideal class group C_F of an algebraic number field F of degree n over Q, with r_2 complex embeddings, contains a non-zero ideal I with norm

$$N(I) \leq \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} \sqrt{|d_F|}$$

where d_F is the discriminant of F.

So in order to find the elements of the class group, we need to find ideals of small norm in O_F.

There is a very important fact about ideals in rings of integers: $N(I) \in I$, so $I \mid (N(I))$. Now $N(I)$ is a natural number and can be factorised in the product of rational primes. So if we can factorise into primes all ideals (p) with $p \leq c$, we will be able to find all ideals of small norm as their factors.

For example, let $K = \mathbf{Q}(\sqrt{-14})$. We will show the class group is cyclic of order 4 .

Here $n = 2, r_2 = 1$, and $\text{disc}(K) = -56$. The Minkowski bound is ≈ 4.764, so the class group is generated by primes dividing (2) and (3). The following table shows how (2) and (3) factor in $\mathcal{O}_K$ based on how $T^2 + 14$ factors modulo 2 and modulo 3 .

p	$T^2 + 14 \bmod p$	(p)
2	T^2	p_2^2
3	$(T-1)(T+1)$	$p_3 p_3'$

Since $p_2^2 \sim 1, p_2 \sim p_2^{-1}$. Since $p_3 p_3' \sim 1, p_3' \sim p_3^{-1}$. Therefore the class group of K is generated by $[p_2]$ and $[p_3]$.

Both p_2 and p_3 are nonprincipal, since they have norm 2 and 3 but the equations $a^2 + 14b^2 = 2$ and $a^2 + 14b^2 = 3$ have no integral solutions.

To find relations between p_2 and p_3, we use $\mathrm{N}_{K/\mathbf{Q}}(2 + \sqrt{-14}) = 18 = 2 \cdot 3^2$. The ideal $(2 + \sqrt{-14})$ is divisible by only one of p_3 and p_3', since $2 + \sqrt{-14}$ is not a multiple of 3 . Without loss of generality, we may let p_3 be the prime of norm 3 dividing $(2 + \sqrt{-14})$. Then $p_2 p_3^2 \sim 1$, so

$$p_3^2 \sim p_2^{-1} \sim p_2,$$

so the class group of K is generated by [p_3]. Since p_2 is nonprincipal and $p_2^2 \sim 1$, [p_3] has order 4 . Thus, the class group of K is cyclic of order 4 .

For $Q(\sqrt{(}-17))$, the same procedure Cl(K) is trivial. The discriminates for which trivial class group happens are very important and are called Heegner numbers. And here is the definition:

Definition: A positive integer n is a Heegner number if the ring of integers of $Q(\sqrt{-n})$ has unique prime factorization. In fact, $n = 163$ is the largest number for which $Q(\sqrt{-n})$ has trivial class group. The complete list is $1, 2, 3, 7, 11, 19, 43, 67, 163$.

7 Acknowledgement

We thank Simon Rubinstein-Salzedo (Euler Circle), Kishan Jani (University of California Berkeley) and various classmates for providing useful resources, comments, and discussions.

References

[Che16] Evan Chen. An infinitely large napkin, 2016.

[Coh94] Harvey Cohn. *Introduction to the construction of class fields*. Courier Corporation, 1994.

[Cox11] David A Cox. *Primes of the form x2+ ny2: Fermat, class field theory, and complex multiplication*, volume 34. John Wiley & Sons, 2011.

[Jar14] Frazer Jarvis. *Algebraic number theory*, volume 1303. Springer, 2014.

[MzK04] Marios Magioladitis and Arbeitsgemeinschaft zur Klassenkörpertheorie. Primes of the form x2+ ny2. *Arbeitsgemeinschaft zur Klassenkorpertheorie, University of Duisburg-Essen*, 2004.

[Row12] Louis H Rowen. *Ring Theory, 83*. Academic Press, 2012.

[Ser12] Jean-Pierre Serre. *Algebraic groups and class fields*, volume 117. Springer Science & Business Media, 2012.