Ideals and class groups of number fields

A thesis submitted
To Kent State University in partial
Fulfillment of the requirements for the
Degree of Master of Science

by

Minjiao Yang

August, 2018
© Copyright
All rights reserved
Except for previously published materials
Thesis written by

Minjiao Yang

B.S., Kent State University, 2015
M.S., Kent State University, 2018

Approved by

______________________, Advisor
Gang Yu

______________________, Chair, Department of Mathematics Science
Andrew Tonge

______________________, Dean, College of Arts and Science
James L. Blank
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACKNOWLEDGEMENTS</td>
<td>iv</td>
</tr>
<tr>
<td>CHAPTER</td>
<td></td>
</tr>
<tr>
<td>I. Introduction</td>
<td>1</td>
</tr>
<tr>
<td>II. Algebraic Numbers and Integers</td>
<td>3</td>
</tr>
<tr>
<td>III. Rings of Integers</td>
<td>9</td>
</tr>
<tr>
<td>IV. Ideals</td>
<td>21</td>
</tr>
<tr>
<td>A review of ideals of commutative</td>
<td>21</td>
</tr>
<tr>
<td>Ideal theory of integer ring $O_k$</td>
<td>22</td>
</tr>
<tr>
<td>V. Ideal class group and class number</td>
<td>28</td>
</tr>
<tr>
<td>Finiteness of $Cl_k$</td>
<td>29</td>
</tr>
<tr>
<td>The Minkowski bound</td>
<td>32</td>
</tr>
<tr>
<td>Further remarks</td>
<td>34</td>
</tr>
<tr>
<td>BIBLIOGRAPHY</td>
<td>36</td>
</tr>
</tbody>
</table>
ACKNOWLEDGEMENTS

I want to thank my advisor Dr. Gang Yu who has been very supportive, patient and encouraging throughout this tremendous and enchanting experience. Also, I want to thank my thesis committee members Dr. Ulrike Vorhauer and Dr. Stephen Gagola who help me correct mistakes I made in my thesis and provided many helpful advices.
Chapter 1. Introduction

Algebraic number theory is a branch of number theory which leads the way in the world of mathematics. It uses the techniques of abstract algebra to study the integers, rational numbers, and their generalizations. Concepts and results in algebraic number theory are very important in learning mathematics.

Algebraic number theory started with Diophantine, Fermat, Gauss and Dirichlet. The beginnings of algebraic number theory can be traced to Diophantine equations, was conjectured by the 3rd-century famous mathematician, Diophantus, who studied them and developed methods for the solution of some of Diophantine equations. Diophantine equations have been studied for thousands of years and only a portion of his major work *Arithmetica* survived. Fermat’s last theorem, named after 17th century mathematician, Pierre de Fermat, was first discovered in the margin in his copy of an edition of Diophantus, and included the statement that the margin was too small to include the proof. No successful proof was published until 1995 and the unsolved problem stimulated the development of algebraic number theory in the 19th century. One of the founding works of algebraic number theory, *Disquisitiones Arithmeticae* was written by Carl Friedrich Gauss in 1798, in which Gauss brings together the work of number theory from his predecessors with his own important new result into a systematic framework, filled in gaps and extended the subject in numerous ways.

Algebraic number theory reached its first peak in the work of Kummer about cyclotomic
fields. However, Kummer was not at all interested in a general theory of algebraic numbers. He restricted his investigations to algebraic numbers connected with the nth roots of unity and the nth roots of such numbers. On the other hand, Dirichlet considered the group of units of the ring generated over \(\mathbb{Z}\) by an arbitrary integral algebraic number and determined the structure of this group. It was Dedekind who understood the basic notion of the theory of algebraic number field, which was absent in the investigation of his predecessor. Dedekind formulated the theory by means of ideals, an approach which is now generally accepted. During this same period, the basic notions and theorems were done in equivalent ways by Kronecker with adjunction of variables and Zolotarev with the notion of exponential valuation theory.

In the 19th century, David Hilbert unified the field of algebraic number theory and resolved a significant number-theory problem. In later time, Emil Artin established his Artin reciprocity law, which is a general theorem in number theory that forms a central part of global class field theory.

When writing this thesis, I was motivated by the desire to learn more about the principles of number theory. It is a compilation of various topics in number theory which were encountered during my course of study, particularly in the area of number theory and I aim to analyze the ideal class group in this thesis.
Chapter 2. Algebraic Numbers and integers

In this chapter, we will briefly introduce algebraic numbers and algebraic integers.

**Definition 2.1.** An algebraic number is any complex number that is a root of a non-zero polynomial equation with integer (or, equivalently, rational) coefficient, i.e., \( \alpha \) is an algebraic number if and only if it satisfies \( f(\alpha) = 0 \), where

\[
f(x) = a_n x^n + a_{n-1} x^{n-1} + a_{n-2} x^{n-2} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x] \quad (2.1)
\]

with \( a_n > 0 \). The minimal such \( n \) is called the degree of \( \alpha \). An algebraic integer is a complex number that is a root of some monic polynomial equation with integer coefficients, i.e., \( \alpha \) is an algebraic integer if and only if it satisfies \( f(\alpha) = 0 \) with

\[
f(x) = x^m + b_{m-1} x^{m-1} + b_{m-2} x^{m-2} + \cdots + b_1 x + b_0 \in \mathbb{Z}[x]
\]

for some positive integer \( m \). Clearly, algebraic integers are included in algebraic numbers.

**Remark 2.2.** If \( f(\alpha) = 0 \) for some \( f(x) \in \mathbb{Z}[x] \), then from the unique factorization of \( \mathbb{Z}[x] \), there is a unique irreducible factor \( g(x) \in \mathbb{Z}[x] \) (with positive leading coefficient) of \( f(x) \) such that \( g(\alpha) = 0 \). This \( g(x) \) is called the minimal polynomial of \( \alpha \), and the degree of \( g(x) \) is the degree of \( \alpha \). Apparently, the minimal polynomial of an algebraic integer is a monic irreducible polynomial with integer coefficients.

We think of algebraic integers and algebraic numbers as generalizations of ordinary
integers and rational numbers. All (ordinary or “rational”) integers belong to algebraic integers, and all rational numbers belong to algebraic numbers. Some other examples of algebraic integers are $i, \sqrt{2}, 4 + \sqrt{7}$ and $2 \cos \frac{2\pi}{9}$. The algebraic numbers include $\frac{1+i}{2}, \sqrt[5]{15}, \frac{4+\sqrt{7}}{2}$ and $\sin \frac{2\pi}{7}$. The numbers $e$ and $\pi$ are not algebraic—they are transcendental, meaning they are not solutions of any non-constant polynomial equation with rational coefficients.

Next we prove several simple properties of algebraic numbers. The first result is a relatively trivial fact about ordinary rational numbers.

**Proposition 2.3.** A rational number which is an algebraic integer is an integer.

**Proof.** Write $x = \frac{a}{b}$ in lowest terms, assume that $x$ is not an integer. Then $b$ is an integer greater than 1. We prove the result by contradiction.

Since $x$ is an algebraic integer, then there exists $c_0, c_1, \ldots, c_{n-1} \in \mathbb{Z}$ such that

$$f(x) = x^n + c_{n-1}x^{n-1} + c_{n-2}x^{n-2} + \cdots + c_1x + c_0 = 0.$$ 

We plug in $\frac{a}{b}$ for all $x$ and then we have

$$f \left( \frac{a}{b} \right) = \left( \frac{a}{b} \right)^n + c_{n-1} \left( \frac{a}{b} \right)^{n-1} + c_{n-2} \left( \frac{a}{b} \right)^{n-2} + \cdots + c_1 \left( \frac{a}{b} \right) + c_0 = 0.$$ 

Multiply $b^n$ for both sides and we get

$$a^n + c_{n-1}a^{n-1}b + c_{n-2}a^{n-2}b^2 + \cdots + c_1ab^{n-1} + c_0b^n = 0.$$ 

Which implies that $a^n \equiv 0 \ (mod \ b)$. Since $x$ is not an integer, $b \neq 1$ and thus there is a prime number $p$ such that $p|b$. So we have $p|a^n$, and hence $p|a$. Now we have $p$ dividing both $a$
and \( b \), which contradicts the assumption that \( \frac{a}{b} \) is in lowest terms. Therefore, the rational number \( x \) is an integer. ■

**Proposition 2.4.** For any algebraic number \( u \), there is an algebraic integer \( v \) such that \( uv \) is an algebraic integer.

**Proof.** It suffices to show that there is a rational integer \( v \), such that \( vu \) is an algebraic integer. Suppose

\[
f(x) = a_n x^n + a_{n-1} x^{n-1} + a_{n-2} x^{n-2} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]
\]

is the minimal polynomial of \( \alpha \) (so \( a_n \) is a positive integer). Let

\[
g(x) = x^n + a_{n-1} x^{n-1} + a_{n-2} a_n x^{n-2} + a_{n-3} a_n^2 x^{n-3} \cdots + a_1 a_n^{n-2} x + a_0 a_n^{n-1},
\]

then we see that \( g(x) \in \mathbb{Z}[x] \), and

\[
g(a_n \alpha) = a_n^{n-1} f(\alpha) = 0.
\]

Note that \( g(x) \) is monic, we thus have proved the theorem with \( v = a_n \). ■

Next, we show that algebraic numbers (integers) are closed under addition and multiplication.

**Theorem 2.5.** The sum and product of two algebraic integers are algebraic integers.

**Proof.** Say \( \alpha \) and \( \beta \) are two algebraic integers, we need to prove \( \alpha + \beta \) and \( \alpha \beta \) are also algebraic integers. Let \( \mathbb{Z}[\alpha, \beta] := \{ f(\alpha, \beta) | f(x, y) \in \mathbb{Z}[x, y] \} \). It suffices to show \( \gamma \) is an algebraic integer for all \( \gamma \in \mathbb{Z}[\alpha, \beta] \).

Since \( \alpha, \beta \) are algebraic integers, then there exist \( a_0, a_1, \ldots, a_{n-1} \in \mathbb{Z} \) and \( b_0, b_1, \ldots, b_{m-1} \in \mathbb{Z} \) such that
\[
\alpha^n + a_{n-1}\alpha^{n-1} + a_{n-2}\alpha^{n-2} + \cdots + a_1\alpha + a_0 = 0.
\]

and

\[
\beta^m + b_{m-1}\beta^{m-1} + b_{m-2}\beta^{m-2} + \cdots + b_1\beta + b_0 = 0.
\]

Thus

\[
\alpha^n = -a_{n-1}\alpha^{n-1} - a_{n-2}\alpha^{n-2} - \cdots - a_1\alpha - a_0,
\]

and

\[
\beta^m = -b_{m-1}\beta^{m-1} - b_{m-2}\beta^{m-2} - \cdots - b_1\beta - b_0.
\]

Hence

\[
\mathbb{Z}[\alpha, \beta] = \{ \sum_{i<n,j<m} c_{ij} \alpha^i \beta^j \mid c_{ij} \in \mathbb{Z} \}.
\]

Suppose \( \gamma \in \mathbb{Z}[\alpha, \beta] \). Note that for any non-negative integers \( k, l \), we have \( \gamma \alpha^k \beta^l \in \mathbb{Z}[\alpha, \beta] \). Thus \( \gamma \alpha^k \beta^l = \sum_{i<n,j<m} c_{ij}^{kl} \alpha^i \beta^j \), i.e.,

\[
\gamma \alpha^k \beta^l - \sum_{i<n,j<m} c_{ij}^{kl} \alpha^i \beta^j = 0 \quad (2.2)
\]

for some integers \( c_{ij}^{kl} \). Ordering \( \alpha^i \beta^j \) by \( \alpha^0 \beta^0, \alpha^1 \beta^0, \ldots, \alpha^{n-1} \beta^0, \alpha^0 \beta^1, \ldots, \alpha^{n-1} \beta^{m-1} \), then from (2.2), with \( k, l \) respectively running from 0 to \( n-1 \) and \( m-1 \), we get

\[
\begin{bmatrix}
\gamma - c_{00}^{10} & -c_{10}^{00} & \cdots \\
-c_{10}^{00} & \gamma - c_{10}^{10} & \cdots \\
\vdots & \vdots & \ddots
\end{bmatrix}
\begin{bmatrix}
\alpha^0 \beta^0 \\
\alpha^1 \beta^0 \\
\vdots
\end{bmatrix} = 0.
\]

Then the matrix is singular, and thus it has determinant 0. On the other hand, the determinant of the matrix is a degree \( mn \) monic polynomial of \( \gamma \) with integer coefficients, hence \( \gamma \) is an algebraic integer. \( \blacksquare \)
**Example 2.6.** Let \( \alpha = 1 + \sqrt{2} \) and \( \beta = 1 + \sqrt{3} \), They are both algebraic integers, and we have
\[
\alpha^2 - 2\alpha - 1 = 0, \quad \text{and} \quad \beta^2 - 2\beta - 2 = 0.
\]

Let \( \gamma = \alpha\beta = 1 + \sqrt{2} + \sqrt{3} + \sqrt{6} \). Rewrite this as \( \gamma - 1 - \sqrt{6} = \sqrt{2} + \sqrt{3} \) and square both sides to obtain
\[
(\gamma - 1)^2 - 2\sqrt{6}(\gamma - 1) + 6 = 5 + 2\sqrt{6},
\]

Which simplifies to \( \gamma^2 - 2\gamma + 2 = 2\sqrt{6}\gamma \). Squaring both sides, we obtain \( \gamma^4 - 4\gamma^3 - 16\gamma^2 - 8\gamma + 4 = 0 \).

From Theorem 2.5 and the proof of Proposition 2.4, or directly with a proof nearly identical to that for Theorem 2.5, we have

**Theorem 2.7.** The sum and product of two algebraic numbers are algebraic numbers.

We end this chapter by showing that, for a given algebraic number \( \alpha \), \( \mathbb{Q}[\alpha] \) is a field.

**Theorem 2.8.** Given any algebraic number \( \alpha \), \( \mathbb{Q}[\alpha] \) is a field.

**Proof:** Without loss of generality, we suppose that \( \alpha \) is an algebraic number of degree \( n \geq 2 \), with minimal polynomial \( f(x) \). From the proof of Theorem 2.5, we clearly have
\[
\mathbb{Q}[\alpha] = \{c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1} | c_0, c_1, \ldots, c_{n-1} \in \mathbb{Q}\} \quad (2.3)
\]

To show that this is a field, it suffices to show that, for any \( A, B \in \mathbb{Q}[\alpha] \), we have \( A \pm B, AB \) and \( 1/B \) (if \( B \neq 0 \)) are in \( \mathbb{Q}[\alpha] \).

Suppose
\[
A = h(\alpha) = a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}, \quad B = g(\alpha) = b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1}
\]
for some rational numbers \(a_0, \ a_1, \ ... \ a_{n-1}, \ b_0, \ b_1, \ ... \ b_{n-1}\). It is clear that \(A \pm B\) is also in the form of (2.3), and thus is in \(\mathbb{Q}[\alpha]\). From the Euclidean algorithm for polynomials over \(\mathbb{Q}\), there are \(q(x), r(x) \in \mathbb{Q}[x]\), with \(\deg(r) \leq n - 1\) such that

\[
g(x)h(x) = q(x)f(x) + r(x).
\]

Thus

\[
AB = g(\alpha)h(\alpha) = q(\alpha)f(\alpha) + r(\alpha) = r(\alpha) \in \mathbb{Q}[\alpha].
\]

Now suppose \(B \neq 0\), then \(g(x)\) and \(f(x)\) must be coprime, thus there are \(s(x), t(x) \in \mathbb{Q}[x]\), with \(\deg(t) \leq n - 1\), such that

\[
s(x)f(x) + t(x)g(x) = 1.
\]

We hence have

\[
1 = s(\alpha)f(\alpha) + t(\alpha)g(\alpha) = t(\alpha)g(\alpha) = t(\alpha)B.
\]

Thus \(\frac{1}{B} \in \mathbb{Q}[\alpha]\). ■

**Remark 2.9.** From Theorem 2.8 (and its proof), we see that \(\mathbb{Q}[\alpha] = \mathbb{Q}(\alpha)\), the field generated by \(\alpha\) over \(\mathbb{Q}\). From now on, we will use the notation \(\mathbb{Q}(\alpha)\) for this field. It can be shown that, for a finite number of algebraic numbers \(\alpha_1, \ldots, \alpha_k\), the field obtained by completing the set \(\mathbb{Q} \cup \{\alpha_1, \ldots, \alpha_k\}\) via \(+, - , \times, /\) is also in the form \(\mathbb{Q}(\alpha)\) for a single algebraic number \(\alpha\). We shall not prove this, but will assume this fact when it is needed. For an algebraic number \(\alpha\), \(\mathbb{Q}(\alpha)\) is called an *algebraic number field*, or simply a *number field*. 
Chapter 3. Rings of Integers

In this chapter, we study the algebraic integers in a number field \( \mathbb{Q}(\alpha) \) where \( \alpha \) is a given algebraic number which, without loss of generality, is supposed to have degree \( n \geq 2 \).

Let \( \alpha_1, \ldots, \alpha_n \) be the conjugates of \( \alpha \). The fields \( \mathbb{Q}(\alpha_j) \) are very similar to \( \mathbb{Q}(\alpha) \), each being generated by an element (over \( \mathbb{Q} \)) with the same minimum polynomial. In fact, they are all isomorphic. Note that if \( g_1, g_2 \in \mathbb{Q}[X] \) and \( g_1(\alpha) = g_2(\alpha) \), then for any if \( j \leq n \), we have \( g_1(\alpha_j) = g_2(\alpha_j) \) which follows from the fact that \( \alpha \) and \( \alpha_j \) have the same minimum polynomial. Therefore, it is fairly easy to verify that the map \( \sigma_j : \mathbb{Q}(\alpha) \to \mathbb{Q}(\alpha_j) \), defined by \( \sigma_j(g(\alpha)) = g(\alpha_j) \) for \( g \in \mathbb{Q}[X] \), is an isomorphism. We often let \( \alpha_1 = \alpha \), and then \( \sigma_1 \) is the identity map on \( \mathbb{Q}(\alpha) \).

3.1. Some basic properties

Let \( \alpha_1, \ldots, \alpha_n \) be the conjugates of a given degree \( n \) algebraic number \( \alpha \), and \( \sigma_1, \ldots, \sigma_n \) be the isomorphisms defined above.

**Definition 3.1.1.** Let \( \beta \in \mathbb{Q}(\alpha) \). Then norm of \( \beta \), denoted by \( N(\beta) \), is defined by

\[
N(\beta) = \prod_{j=1}^{n} \sigma_j(\beta)
\]
and $T(\beta)$, the *trace* of $\beta$, is defined by

$$T(\beta) = \sum_{j=1}^{n} \sigma_j(\beta).$$

**Proposition 3.1.2.** We have the following properties for the trace and norm of algebraic numbers

1. $N(\beta \gamma) = N(\beta)N(\gamma)$ for all $\beta, \gamma \in \mathbb{Q}(\alpha)$,
2. $N(c\beta) = c^nN(\beta)$ for all $c \in \mathbb{Q}$ and $\beta \in \mathbb{Q}(\alpha)$,
3. $T(\beta + \gamma) = T(\beta) + T(\gamma)$ for all $\beta, \gamma \in \mathbb{Q}(\alpha)$, and
4. $T(c\beta) = cT(\beta)$ for all $c \in \mathbb{Q}$ and $\beta \in \mathbb{Q}(\alpha)$.

**Proof:** These all easily follow from the definitions and the facts that the $\sigma_j$ preserve summation and multiplication. $\blacksquare$

Clearly, $N(0) = 0$ and $N(1) = 1$. If $\beta \neq 0$ then $1 = N(1) = N(\beta)N(\frac{1}{\beta})$ so that $N(\beta) \neq 0$. Next, we state without proof a very important fact about the trace and norm of an algebraic number.

**Proposition 3.1.3.** Suppose $\alpha$ is an algebraic number. For $\beta \in \mathbb{Q}(\alpha)$, we have $N(\beta) \in \mathbb{Q}$ and $T(\beta) \in \mathbb{Q}$. Moreover, if $\beta$ is an algebraic integer, then $N(\beta) \in \mathbb{Z}$ and $T(\beta) \in \mathbb{Z}$.

**Remark 3.1.4.** In fact, if $\alpha$ is a degree $n$ algebraic integer, with minimal polynomial

$$f(x) = x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1x + a_0,$$

then we have

$$-a_{n-1} = \alpha_1 + \cdots + \alpha_n = T(\alpha) \in \mathbb{Z}.$$
And

\((-1)^n a_0 = \alpha_1 \alpha_2 \cdots \alpha_n = N(\alpha) \in \mathbb{Z}.\)

Before we bring out the topic of the ring of integers of a number field, let us recall a little about the theory of commutative rings.

**Definition 3.1.5.** A commutative ring \( R \) is a set with two operations, addition and multiplication, such that:

1. \( R \) is an abelian group under addition,
2. \( ab = ba \) for all \( a, b \in R \),
3. \( a(bc) = (ab)c \) for any \( a, b, c \in R \),
4. There is an element \( 1 \in R \) with \( 1 \neq 0 \) and with \( 1 \cdot a = a \cdot 1 = a \) for any \( a \in R \),
5. \( a(b + c) = ab + ac \) for any \( a, b, c \in R \).

For a given a number field \( K \), consider the collection of all algebraic integers contained in \( K \). From Theorem 2.5, we can check that all conditions for a commutative ring is satisfied by the set under the ordinary summation and multiplication of complex numbers. We thus have the following

**Definition 3.1.6.** Given a number field \( K \), the ring of integers \( \mathcal{O}_K \) of \( K \) is the commutative ring consisting of the algebraic integers in \( K \), under the ordinary summation and multiplication.

In the special case that \( K = \mathbb{Q} \), we have \( \mathcal{O}_k = \mathbb{Z} \). While many arithmetic/algebraic properties of \( \mathbb{Z} \) are well known to us, we will see that general rings of integers have many important properties in common with \( \mathbb{Z} \).
Proposition 3.1.7. The ring of integers $\mathcal{O}_k$ is a finitely-generated $\mathbb{Z}$-module. Indeed, it is a free $\mathbb{Z}$-module, and thus has an integral basis $\omega_1, \ldots, \omega_n \in \mathcal{O}_k$ of the $\mathbb{Q}$-vector space $K$ such that each element $x$ in $\mathcal{O}_k$ can be uniquely represented as

$$x = \sum_{i=1}^{n} a_i \omega_i,$$

with $a_i \in \mathbb{Z}$. The rank $n$ of $\mathcal{O}_k$ as a free $\mathbb{Z}$-module is equal to the degree of $K$ over $\mathbb{Q}$, in which $[K : \mathbb{Q}] = n$.

Proposition 3.1.8. The ring of integers in a number field is a Dedekind domain.

Suppose $\omega_1, \ldots, \omega_n \in \mathcal{O}_k$ are a basis for $\mathcal{O}_k$ as a $\mathbb{Z}$-module. Consider the embedding $\sigma: K \to \mathbb{C}^n$ defined by $\sigma(a) = (\sigma_1(a), \sigma_2(a), \ldots, \sigma_n(a))$, where $\sigma_1, \sigma_2, \ldots, \sigma_n$ are the distinct embeddings of $K$ into $\mathbb{C}$. Let $A$ be the $n \times n$ matrix consisting of rows $\sigma(\omega_1), \ldots, \sigma(\omega_n)$, then

$$\det(AA^T) = \det(\sum_{k=1}^{n} \sigma_k(\omega_i) \sigma_k(\omega_j)) = \det\left(\sum_{k=1}^{n} \sigma_k(\omega_i \omega_j)\right) = \det(\text{Tr}(\omega_i \omega_j)_{1 \leq i, j \leq n})$$

which shows that $\det(AA^T)$ can be defined in terms of the trace, and we also conclude that $\det(AA^T)$ is a rational integer. Moreover, because changing the integral basis is equivalent to multiplying to $A$ (either to its left or right) an integer matrix $U$ of determinant $\pm 1$, thus $\det(AA^T)$ is independent of the choice of the integral basis.

Definition 3.1.9. The discriminant of a number field $K$, denoted by $d_K$ or $\Delta_K$, is the integer given by the $\det(AA^T)$.

$\Delta_K$ is one of the most important invariants of a number field $K$. In our Chapter 5 examples, when we try to find the class group/number of a (quadratic) fields, the size of $\Delta_K$ is a key factor that more or less determines the complexity of the computation.
3.2. Factorization of algebraic integers and the unit group

In this section, we will discuss divisibility and factorization of algebraic integers. For rational integers, we have the Fundamental Theorem of Arithmetic -- each positive integer can be uniquely expressed as the product of prime numbers. A rational prime number $p$ is a positive integer satisfying any one of the following two conditions.

(1) If $p = ab$ with $a, b \in \mathbb{Z}$ then $a = \pm 1$ or $b = \pm 1$. ----- (3.2.1)

(2) If $p \mid cd$ with $c, d \in \mathbb{Z}$ then $p \mid c$ or $p \mid d$. ----- (3.2.2)

These two conditions are equivalent, but their analogs in the ring of integers $\mathcal{O}_k$ are not necessarily equivalent.

**Definition 3.2.3.** For $\beta, \gamma \in \mathcal{O}_k$ with $\beta \neq 0$, we say that $\beta$ divides $\gamma$, or $\gamma$ is divisible by $\beta$ (with notation $\beta \mid \gamma$), if $\frac{\gamma}{\beta} \in \mathcal{O}_k$. $\beta \in \mathcal{O}_k$ is a unit in $\mathcal{O}_k$ if $\beta \mid 1$ or, equivalently, $\frac{1}{\beta} \in \mathcal{O}_k$.

**Lemma 3.2.4.** Let $\beta, \gamma \in \mathcal{O}_k$. If $\beta \mid \gamma$, then $N(\beta) \mid N(\gamma)$ as integers.

**Proof:** This is obvious from the definition of divisibility and Proposition 3.1.3 and 3.1.2(1). ■

It is fairly easy to show that the set of units of $\mathcal{O}_k$, denoted by $U(\mathcal{O}_k)$, forms an Abelian group under multiplication. We call $U(\mathcal{O}_k)$ the unit group of $\mathcal{O}_k$, or the unit group of $K$.

**Lemma 3.2.5.** Suppose that $K$ is a number field. Then $\beta \in U(\mathcal{O}_k)$ if and only if $N(\beta) = \pm 1$.

**Proof:** If $\beta \in U(\mathcal{O}_k)$, then there is a $\gamma \in \mathcal{O}_k$ such that $\beta \gamma = 1$. The lemma then follows directly from Proposition 3.1.3, and the fact that $N(1) = 1$. ■
**Definition 3.2.6.** An element \( \beta \in \mathcal{O}_k \) is **irreducible** if

1. \( \beta \neq 0 \),
2. \( \beta \) is not a unit,
3. If \( \beta = \gamma \delta \) with \( \gamma, \delta \in \mathcal{O}_k \) then either \( \gamma \) or \( \delta \) is a unit.

In \( \mathbb{Z} \), the irreducible elements have the form \( \pm p \), where \( p \) is a prime number. From Lemma 3.2.5, we obtain that if \( N(\beta) \) is a prime number then \( \beta \) is irreducible. The converse, however, is not true in general. For example, for \( K = \mathbb{Q}(i) \) we have \( \mathcal{O}_k = \mathbb{Z}[i] \) (we will see this later in section 3.3). One can check that 3 is irreducible in \( \mathcal{O}_k \), but \( N(3) = 9 \) is not prime.

Similar to the Fundamental Theorem of Arithmetic, every element in \( \mathcal{O}_k \) can be factored into a product of irreducibles.

**Theorem 3.2.7.** Let \( K \) be a number field. Suppose \( \beta \in \mathcal{O}_k \) with \( \beta \neq 0 \) and \( \beta \notin U(\mathcal{O}_k) \). Then there exist irreducible elements \( \gamma_1, \ldots, \gamma_k \in \mathcal{O}_k \) such that \( \beta = \gamma_1 \cdots \gamma_k \).

**Proof:** We prove by induction on \( |N(\beta)| \). Since \( \beta \neq 0 \) and \( \beta \notin U(\mathcal{O}_k) \), \( |N(\beta)| \geq 2 \). Now we have two cases, if \( \beta \) is irreducible then take \( k = 1 \) and \( \gamma_1 = \beta \). If \( \beta \) is reducible then \( \beta = \beta_1 \beta_2 \) where \( \beta_1, \beta_2 \in \mathcal{O}_k \) and \( \beta_1, \beta_2 \notin U(\mathcal{O}_k) \). Then \( |N(\beta_1)|, |N(\beta_2)| > 1 \) and \( |N(\beta)| = |N(\beta_1)||N(\beta_2)| \) implies \( |N(\beta_1)| < |N(\beta)| \) and \( |N(\beta_2)| < |N(\beta)| \). By induction hypothesis, \( \beta_1 \) and \( \beta_2 \) are products of irreducible elements. Combine these factorizations we see that \( \beta \) is also a product of irreducible elements. \( \blacksquare \)

A natural question about the factorization (into a product of irreducible integers) is whether it is unique. Before we go any further, let us define the **uniqueness** here. It is obvious that if \( \beta \) is irreducible and \( \xi \in U(\mathcal{O}_k) \) then \( \xi \beta \) is irreducible as well. We can adjust factorizations
by multiplying factors by units. For example, let $\beta = \gamma_1 \gamma_2 \gamma_3$ where $\gamma_1, \gamma_2, \gamma_3$ are irreducible, and $\in U(\mathcal{O}_K)$. Then

$$\beta = \gamma_1 \gamma_2 \gamma_3 \xi^{-1} = (\xi \gamma_1) \gamma_2 (\xi^{-1} \gamma_3) \quad (3.2.3)$$

gives two formally different factorizations of $\beta$ into irreducibles. These two factorizations are essentially the same if we consider factorizations modulo the unit group. We call two algebraic integers associated (or one is an associate of the other) if they differ by a unit factor. In the factorization of algebraic integers, we treat two associated integers as the same, and thus the two factorizations in (3.2.5) are regarded as the same. So, when it comes to the uniqueness of factorization, two factorizations are different only if one is not a re-ordering of associates of the integers in the other factorization.

**Example 3.2.8.** Let $K = \mathbb{Q}(\sqrt{-5})$. 2, 3, $1 + \sqrt{-5}$, and $1 - \sqrt{-5}$ are irreducible integers in $\mathcal{O}_K$, and they are not associated. Observing that $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$, $\mathcal{O}_K$ does not have unique factorization into irreducibles.

**Example 3.2.9.** Let $K = \mathbb{Q}(\sqrt{-6})$, from section 3.3 we will see that $\mathcal{O}_k = \mathbb{Z}[\sqrt{-6}]$. Now $6 = 2 \times 3 = \sqrt{-6}(-\sqrt{-6})$. These two factorizations of 6 into irreducible elements are inequivalent.

**Remark 3.2.10.** Examples 3.2.8 and 3.2.9 show that, in number fields, while every integer can be expressed as a product of irreducible integers, such factorization is not necessarily unique. Thus, if we pursue an analog of the Fundamental Theorem of Arithmetic in number fields, irreducible integers in number fields, as an extension of rational prime numbers following the definition (3.2.3), do not serve the same role as rational prime numbers in $\mathbb{Z}$. Next, let us consider the algebraic integers satisfying a condition similar to (3.2.4). We call such integers primes in the number field.
Definition 3.2.11. Let $\beta \in \mathcal{O}_k$, $\beta$ is prime if

1. $\beta \neq 0$,
2. $\beta$ is not a unit,
3. If $\beta | \gamma \delta$ with $\gamma, \delta \in \mathcal{O}_k$ then $\beta | \gamma$ or $\beta | \delta$.

Primes are always irreducible.

Lemma 3.2.12. Let $K$ be number field. If $\beta$ is a prime element of $\mathcal{O}_k$ then $\beta$ is irreducible in $\mathcal{O}_k$.

Proof: Let $\beta$ be prime and suppose that $\beta = \gamma \delta$ with $\gamma, \delta \in \mathcal{O}_k$. Then since $\beta | \gamma \delta$, we have $\beta | \gamma$ or $\beta | \delta$. Without loss of generality, we suppose $\beta | \gamma$. Also $\gamma | \beta$ implies $\delta = \beta / \gamma$ is a unit.

Therefore $\beta$ is irreducible. $\blacksquare$

Clearly, each $\mathcal{O}_k$ is an integral domain. While we see from Examples 3.2.8 and 3.2.9 that the unique factorization (into a product of irreducibles) does not hold in $\mathcal{O}_k$ in general, if some condition is satisfied, however, $\mathcal{O}_k$ becomes a UFD. (Recall that a UFD, namely a unique factorization domain, is a domain in which every non-zero element can be uniquely expressed as a product of irreducible elements.)

Theorem 3.2.13. Let $K$ be number field and suppose that every irreducible element of $\mathcal{O}_k$ is prime. Then $\mathcal{O}_k$ has unique factorization.

Proof: We prove by contradiction. Let

$$\beta = \gamma_1 \gamma_2 \cdots \gamma_s = \delta_1 \delta_2 \cdots \delta_k,$$

where $\gamma_j$ and $\delta_r$ are irreducible elements in $\mathcal{O}_k$ for $j = 1, \ldots, s$ and $k = 1, \ldots, k$. 


be two factorizations of $\beta$. We need to show these are equivalent by induction on $|N(\beta)|$. Since $\gamma_1$ is prime and $\gamma_1 \mid \delta_1 \cdots \delta_k$ then $\gamma_1 \mid \delta_r$ for some $r$. By shuffling the $\delta_r$ we may assume that $\gamma_1 \mid \delta_1$ and since $\delta_1$ is irreducible, we obtain $\delta_1 = \mu \gamma_1$ where $\mu$ is a unit. Thus

$$\frac{\beta}{\gamma_1} = \gamma_2 \cdots \gamma_s = \mu \delta_2 \cdots \delta_k$$

is a factorization into irreducibles and $|N(\beta/\gamma_1)| < |N(\beta)|$. By the inductive hypothesis, these factorizations of $\beta/\gamma_1$ are equivalent, and hence the given factorizations of $\beta$ are equivalent. □

We end this section by stating Dirichlet’s unit theorem. We mentioned before that $U(\mathcal{O}_K)$, the unit group of a number field $K$, is a finitely generated Abelian group. In fact, the following theorem of Dirichlet gives a precise description to the structure of $U(\mathcal{O}_K)$.

**Theorem 3.2.14.** (Dirichlet) For any number field $K$, the unit group $U(\mathcal{O}_k)$ is the product of a finite cyclic group of roots of unity with a free Abelian group of rank $r + s - 1$, where $r$ is the number of real embeddings of $K$, and $s$ is the number of complex conjugate pairs of embeddings.

**Remark 3.2.15.** Suppose $\alpha$ is algebraic of degree $n$. Among the conjugates $\alpha_1, \ldots, \alpha_n$ of $\alpha$, suppose there are $r$ real roots and $2s$ imaginary roots. Then $n = r + 2s$, and Dirichlet’s unit theorem says that, for $K = \mathbb{Q}(\alpha)$, we have

$$U(\mathcal{O}_k) \cong W \oplus \mathbb{Z}^{r+s-1},$$

where $W$ is a finite cyclic group.

### 3.3. Quadratic integers
In this section we particularly focus on the fields $K = \mathbb{Q}(\alpha)$ that have degree 2 over $\mathbb{Q}$.

Such a field $K$ is called a \textit{quadratic field}. In this case, $\alpha$ can be chosen as $\sqrt{d}$ for a unique square-free integer (either positive or negative) $d$. Namely, every quadratic field is in the form

$$\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} : a, b \in \mathbb{Q}\}.$$

Depending on the sign of $d$, there are two types of quadratic fields. If $d > 0$, then all element of $\mathbb{Q}(\sqrt{d})$ are real numbers, and we call $\mathbb{Q}(\sqrt{d})$ a real quadratic field; If $d < 0$, then $\mathbb{Q}(\sqrt{d})$ contains non-real numbers (imaginary numbers)—it is an imaginary quadratic field.

For the integer ring of a quadratic field $K = \mathbb{Q}(\sqrt{d})$, rather than $\mathcal{O}_K$, we would like to use a notation $R_d$ (to indicate the associated square-free number $d$).

Formally, for a number $\beta = c + f\sqrt{d} \in \mathbb{Q}(\sqrt{d})$, we call $\beta^* = c - f\sqrt{d}$ the conjugate of $\beta$.

\textbf{Theorem 3.3.1.} Suppose $d$ is a square-free integer (possibly with a negative sign). If $d \equiv \not\equiv 1 \pmod{4}$, then

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

And If $d \equiv 1 \pmod{4}$ then

\[ R_d = \left\{a + b\left(\frac{1+\sqrt{d}}{2}\right) : a, b \in \mathbb{Z}\right\}. \]

\textbf{Proof:} A direct calculation shows that both sets consist of algebraic integers. We need to show, conversely, that every element in $R_d$ has the indicated form.

Let $\alpha = x + y\sqrt{d} \in R_d$, so $\alpha + \alpha^* = 2x \in \mathbb{Z}$ and $\alpha\alpha^* = x^2 - dy^2 \in \mathbb{Z}$. The first condition means $x$ is half an ordinary integer, so either $x \in \mathbb{Z}$ or $x$ is half an odd number.
The importance of \(d\) being squarefree is that if \(dr^2 \in \mathbb{Z}\) for some \(r \in \mathbb{Q}\) then \(r \in \mathbb{Z}\). Indeed, if \(r\) has a prime factor \(p\) in its (reduced form) denominator then \(dr^2 \not\in \mathbb{Z}\) since \(p^2\) is not canceled by \(d\) in \(dr^2\). So \(dr^2 \in \mathbb{Z}\) implies \(r\) has no prime in its denominator, i.e., \(r \in \mathbb{Z}\).

If \(x\) is half an odd number, namely \(x = \frac{a}{2}\) with \(a\) odd, then from the fact that

\[N(\alpha) = x^2 - dy^2 = \frac{a^2}{4} - dy^2 \in \mathbb{Z},\]

we have

\[a^2 - d(2y)^2 \in 4\mathbb{Z} \]

Thus \(d(2y)^2\) is an integer congruent to 1 modulo 4. Since \(d\) is square-free, \(2y \in \mathbb{Z}\) and, moreover, \(y\) is half an odd number and \(d \equiv 1 \pmod{4}\) (because all odd squares are 1 mod 4).

Returning to \(\alpha\),

\[\alpha = x + y\sqrt{d} = \frac{a}{2} + \frac{b}{2}\sqrt{d} = \frac{a-b}{2} + b\left(1 + \frac{\sqrt{d}}{2}\right),\]

which has the necessary form because \(a - b\) is even.

We are done when \(d \equiv 1 \pmod{4}\). When \(d \not\equiv 1 \pmod{4}\) we can’t have \(x\) be half an odd number, so \(x \in \mathbb{Z}\). From \(N(\alpha) = x^2 - dy^2 \in \mathbb{Z}\), it follows that \(dy^2 \in \mathbb{Z}\), so from \(d\) being square-free we get \(y \in \mathbb{Z}\). Therefore \(\alpha\) has the necessary form, with \(a = x\) and \(b = y\). \(\blacksquare\)

To unify the notation, set

\[\omega = \begin{cases} \sqrt{d}, & \text{if } d \not\equiv 1 \pmod{4}, \\ \frac{1+\sqrt{d}}{2}, & \text{if } d \equiv 1 \pmod{4}. \end{cases}\]

Then, \(R_d = \{a + b\omega : a, b \in \mathbb{Z}\} = \mathbb{Z}[\omega]\).
A quick consequence of this is the following

**Theorem 3.3.2.** Suppose $d$ is a square-free integer (either positive or negative). Then for the quadratic field $K = \mathbb{Q}(\sqrt{d})$, we have $\Delta_K = d$ if $d \equiv 1 \mod 4$; and $\Delta_K = 4d$ if $d \equiv 2, 3 \mod 4$.

Let us turn to the unit group next. By $U_d$, we denote the unit group of $\mathbb{Q}(\sqrt{d})$. Dirichlet’s unit theorem shows that, if $d < 0$, then $U_d$ has rank 0 and thus is finite; if $d > 0$, then $U_d$ has rank 1. In fact, we have some much more precise results in this case.

**Theorem 3.3.3.** Suppose $-d > 0$ is a square-free integer. Then we have

$$U_d = \begin{cases} \{\pm 1, \pm \sqrt{-1}\}, & \text{if } d = -1, \\ \{\pm 1, \pm \alpha, \pm \alpha^2\}, & \text{if } d = -3, \\ \{\pm 1\}, & \text{if } d \neq -1, -3, \end{cases}$$

where $\alpha = (-1 + \sqrt{-3})/2$.

**Theorem 3.3.4.** Suppose $d > 1$ is a square-free integer. Then

$$U_d = \{\pm \zeta^r : r \in \mathbb{Z}\},$$

where $\zeta$ is the smallest possible unit of $U_d$ satisfying $\zeta > 1$, called the fundamental unit of $U_d$. 
Chapter 4. Ideals

We have seen from examples in Chapter 3 that the factorization of an algebraic integer into a product of irreducibles is not necessarily unique. In this chapter, I will introduce ideals in number fields (rings), and study some of their properties. In particular, we will see that the Fundamental Theorem of Arithmetic finds a good analog in the factorizations of ideals in number rings.

4.1. A review of ideals of commutative rings

First, we recall that an ideal of a commutative ring $R$ is a subset $I$ of $R$ such that

(1) $I$ is a subgroup of $R$,

(2) if $a, b \in I$, then $a + b \in I$,

(3) if $a \in I$ and $x \in R$ then $xa \in I$.

Norm of an ideal is the cardinality of the quotient ring $R/I$, i.e. $N(I) = [R : I]$. And $N(IJ) = N(I)N(J)$.

A principal ideal of a commutative ring $R$ is an ideal generated by a single element

$$\langle a \rangle = \{xa : x \in R\}$$

for some $a \in R$. 
By trivial ideals we mean the zero ideal \((0) = \{0\}\) and \(R\) itself. All other ideals of \(R\) are regarded nontrivial.

Ideals of commutative rings satisfy some basic (yet important) rules, such as
(1). If $I, J$ are ideals of $R$, then $I + J = \{a + b : a \in I, b \in J\}$ is also an ideal of $R$.

(2). If $I, J$ be ideals of $R$, then $I \cap J$ is also an ideal of $R$.

Moreover, if we define the product of two ideals as

$$IJ = \{a_1b_1 + a_2b_2 + \cdots + a_nb_n : a_1, \ldots, a_n \in I, b_1, \ldots, b_n \in J\},$$

then $IJ$ is the smallest ideal containing all $ab$.

The sum and product satisfy some formal properties:

(1) $I + I = I$, where $I$ is an ideal of $R$,

(2) $I + J = J + I$, where $I$ and $J$ are ideals of $R$,

(3) $I_1 + (I_2 + I_3) = (I_1 + I_2) + I_3$, where $I_1, I_2, I_3$ are ideals of $R$,

(4) $IJ \subseteq I \cap J$, where $I$ and $J$ are ideals of $R$,

(5) $IJ = JI$, where $I$ and $J$ are ideals of $R$,

(6) $I_1(I_2I_3) = (I_1I_2)I_3$, where $I_1, I_2, I_3$ are ideals of $R$,

(7) $I_1(I_1 + J_2) = IJ_1 + IJ_2$, where $I, J_1, J_2$ are ideals of $R$.

### 4.2. Ideal theory of integer ring $\mathcal{O}_K$

In this section, we will prove the fundamental theorem of ideal theory in number fields: every non-zero proper ideal in the integer ring of a number field can be uniquely factored into a product of prime ideals.

**Definition 4.2.1.** For ideals $a$ and $b$ in a commutative ring, write $a \mid b$ if $b = ac$ for an ideal $c$. 
Thus, divisibility and primality in $\mathcal{O}_K$ can be expressed in terms of ideals. For two integers $\beta, \gamma$, $\beta \mid \gamma$ if and only if $\gamma \in \langle \beta \rangle$ which occurs if and only if $\langle \beta \rangle \mid \langle \gamma \rangle$. Similarly, $\langle \beta \rangle = \langle \gamma \rangle$ if and only if $\gamma / \beta$ is a unit in $\mathcal{O}_K$.

**Definition 4.2.2.** We say that an ideal $P$ of $\mathcal{O}_K$ is *prime* if

1. $P \neq \langle 0 \rangle$,
2. $P \neq \langle 1 \rangle$,
3. If $\gamma, \delta \in \mathcal{O}_K$ and $\gamma \delta \in P$, then $\gamma \in P$ or $\delta \in P$.

Before we prove the unique factorization of ideals in a general number ring, we remark that, if $\mathcal{O}_K$ is a PID, then it is fairly easy to show that every irreducible element of $\mathcal{O}_K$ is prime, and then each nontrivial ideal of $\mathcal{O}_K$ is a product of prime ideals.

To prove for a general number field the fundamental theorem of ideals. We need some preparations.

**Lemma 4.2.3.** Let $K$ be a number field and $P$ be a prime ideal of $\mathcal{O}_K$. If $I$ and $J$ are ideals of $\mathcal{O}_K$ with $IJ \subseteq P$, then $I \subseteq P$ or $J \subseteq P$. In general, if $I_1 I_2 \cdots I_m \subseteq P$, then $I_k \subseteq P$ for some $k$.

**Proof:** Suppose $IJ \subseteq P$ but $I \nsubseteq P$ and $J \nsubseteq P$. There exist $\beta \in I, \gamma \in J$ with $\beta \not\in P$ and $\gamma \not\in P$, then $\beta \gamma \in IJ$. But $\beta \gamma \not\in P$ contradict $IJ \subseteq P$. The case of an $m$-term product $I_1 I_2 \cdots I_m$ now follows by induction. $\blacksquare$

**Definition 4.2.4.** An ideal $I$ of $\mathcal{O}_K$ is said to be an *maximal* ideal if, for all ideals $J$ of $\mathcal{O}_K$ such that $I \subseteq J \subseteq \mathcal{O}_K$, either $J = I$ or $J = \mathcal{O}_K$.

**Lemma 4.2.5.** Let $K$ be a number field. An ideal $I$ of $\mathcal{O}_K$ is prime if and only if it is maximal.
Proof: First suppose that \( I \) is maximal. Let \( \beta, \gamma \in \mathcal{O}_K \) with \( \beta \gamma \in I \) and \( \beta \notin I \). To show that \( I \) is prime it suffices to show that \( \gamma \notin I \). Let \( J = I + \langle \beta \rangle \). Then \( J \) is an ideal and \( I \subseteq J \), but \( I \neq J \) since \( \beta \in J \). By maximality of \( I, J = \mathcal{O}_K \). Hence \( 1 \in J \) so \( 1 = \mu + \delta \beta \) where \( \mu \in I \) and \( \delta \in \mathcal{O}_K \). Then \( 1 \equiv \delta \beta \ (mod \ I) \). Consequently, \( \gamma = 1 \gamma \equiv \delta \beta \gamma \equiv 0 \ (mod \ I) \), as \( \beta \gamma \notin I \). We conclude that \( \gamma \in I \) and that \( I \) is prime.

Conversely, suppose that \( I \) is prime, \( J \) is an ideal of \( \mathcal{O}_K \) with \( I \subseteq J \) and \( I \neq J \). We need to show that \( J = \mathcal{O}_K \), or equivalently, that \( 1 \in J \). Let \( \beta \in J \) and \( \beta \notin I \). Then \( J \subseteq I + \langle \beta \rangle \). The ideal \( I \) has finite index, \( m \), in \( \mathcal{O}_K \). Let \( \gamma_1, \gamma_2, \ldots, \gamma_m \) be coset representative for \( I \) in \( \mathcal{O}_K \). That is each element of \( \mathcal{O}_K \) is congruent modulo \( I \) to exactly one \( \gamma_j \). In particular, \( \gamma_j \equiv \gamma_k \ (mod \ I) \) if and only if \( j = k \). If \( \beta \gamma_j \equiv \gamma_k \ (mod \ I) \) then \( \beta (\gamma_j - \gamma_k) \in I \) and as \( I \) is prime and \( \beta \notin I \) then \( \gamma_j - \gamma_k \in I \) and so \( j = k \). The numbers \( \beta \gamma_1, \beta \gamma_2, \ldots, \beta \gamma_m \) lie in distinct cosets of \( I \), and so they represent all cosets. In particular \( 1 \equiv \beta \gamma_j \ (mod \ I) \) for some \( j \), and so \( 1 = \mu + \gamma_j \beta \) for some \( \mu \in I \). Thus \( 1 \in I + \langle \beta \rangle \) and \( I \) is maximal. ■

Lemma 4.2.6. Let \( K \) be a number field and \( I \) be a nontrivial ideal of \( \mathcal{O}_K \). Then there is a prime ideal \( P \) of \( \mathcal{O}_K \) such that \( I \subseteq P \).

Proof: Consider the nontrivial ideals \( J \) of \( \mathcal{O}_K \) with \( I \subseteq J \). There is at least one since \( J = I \) suffices. Take one, \( P \), with least possible norm. Then \( P \) is maximal, for if \( P \subseteq J_1 \) with \( J_1 \neq P \) an ideal of \( \mathcal{O}_K \), then \( N(J_1) < N(P) \) and so \( J_1 = \mathcal{O}_K \). ■

Lemma 4.2.7. Let \( K \) be a number field and \( I \) be a nontrivial ideal of \( \mathcal{O}_K \). Then \( I \supseteq P_1 P_2 \ldots P_m \) where \( P_j \) for \( j = 1, 2, \ldots \) are prime ideals of \( \mathcal{O}_K \).
Proof: Let’s use induction on \( N(I) \). If \( I \) is prime, then we can take \( m = 1 \) and \( P_1 = I \). If \( I \) is not prime, then there exist \( \beta, \gamma \in \mathcal{O}_K \) with \( \beta \notin I \), \( \gamma \notin I \) but \( \beta \gamma \in I \). Let \( J_1 = \langle \beta \rangle + I \) and \( J_2 = \langle \gamma \rangle + I \). Then \( I \leq J_1 \) and \( I \leq J_2 \), but \( I \neq J_1 \) and \( I \neq J_2 \). Hence \( N(J_1) < N(I) \) and \( N(J_2) < N(I) \). But \( J_1 J_2 = \langle \beta \gamma \rangle + \beta I + \gamma I + I^2 \leq I \) as \( \beta \gamma \in I \). By inductive hypothesis, \( J_1 \supseteq P_1 P_2 \cdots P_r \) and \( J_2 \supseteq Q_1 Q_2 \cdots Q_s \) where the \( P_j \) and \( Q_k \) are prime. Therefore, \( I \supseteq J_1 J_2 \supseteq P_1 P_2 \cdots P_r Q_1 Q_2 \cdots Q_s \). 

To prove that a non-zero proper ideal in \( \mathcal{O}_K \) has a unique factorization into a product of prime ideals, we need to show how to invert a prime ideal. The “inverse” of a prime ideal will be an \( \mathcal{O}_K \)-module in \( K \) (but not in \( \mathcal{O}_K \)). To this end, we need to introduce the \( \mathcal{O}_K \)-modules which are essentially ideals with denominators.

Definition 4.2.8. A fractional ideal of \( K \) is a set of the form \( \beta I \) where \( \beta \) is a nonzero element of \( K \) and \( I \) is a nonzero ideal of \( \mathcal{O}_K \).

Lemma 4.2.9. Let \( K \) be a number field, then \( I \) is a fractional ideal of \( K \) if and only if

1. \( I \) is a nonzero subgroup of \( K \) closed under addition,
2. If \( \beta \in I \) and \( \gamma \in \mathcal{O}_K \), then \( \gamma \beta \in I \),
3. There exists a nonzero \( \mu \in K \) such that \( \beta / \mu \in \mathcal{O}_K \) for each \( \beta \in I \).

Proof: If \( I = \mu J \) is a fractional ideal of \( K \), with \( \mu \in K \) and \( J \) an ideal of \( \mathcal{O}_K \), then the three properties follow with the same value of \( \mu \). Conversely, suppose the three properties hold. Then \( J = \mu^{-1} I = \{ \beta / \mu : \beta \in I \} \) is a nonzero ideal of \( \mathcal{O}_K \) and so \( I = \mu J \) is a fractional ideal. 

Theorem 4.2.10. Every fractional ideal is invertible. That is, for a given fractional ideal \( I \), there is a fractional ideal \( J \) with \( IJ = \langle 1 \rangle \).
Lemma 4.2.11. Let $K$ be a number field and $I$ be a nonzero ideal of $\mathcal{O}_K$. If $\gamma I \subseteq I$ for some $\gamma \in K$, then $\gamma \in \mathcal{O}_K$.

Proof: We know each nonzero ideal of $\mathcal{O}_K$ is a free abelian group of rank $n$ under the operation of addition. $I \subseteq \mathcal{O}_K$ is a free abelian group, let $\beta_1, \ldots, \beta_n$ be an integral basis of $I$. Then $\gamma \beta_j \in I$ for all $j$, so $\gamma \beta_j = \sum_{k=1}^n a_{jk} \beta_k$ where the $a_{jk} \in \mathbb{Z}$. Hence $\gamma \mathbf{v} = A \mathbf{v}$ where $\mathbf{v}$ is the column vector with entries the $\beta_j$ and $A$ is the matrix with entries the $a_{jk}$. Thus $\gamma$ is an eigenvalue of $A$ which is a matrix with integer entries. Thus $\gamma$ is an algebraic integer and so $\gamma \in K \cap \mathbf{B} = \mathcal{O}_K$, where $\mathbf{B}$ is basis of $A$. $
$
Lemma 4.2.12. Let $K$ be a number field and $P$ be a prime ideal of $\mathcal{O}_K$. Then there is a fractional ideal $J$ of $K$ with $PJ = (1)$.

Proof: Let $P^* = \{ \beta \in K : \beta P \subseteq \mathcal{O}_K \}$. Then $P^*$ is a fractional ideal of $K$, $\mathcal{O}_K \subseteq P^*$ and $P \subseteq PP^* \subseteq \mathcal{O}_K$. By the maximality of the prime ideal $P$, either $PP^* = P$ or $PP^* = \mathcal{O}_K$. We show that the latter is true, so to obtain a contradiction, suppose that $PP^* = P$.

Then if $\gamma \in P^*$ we have $\gamma P \subseteq P$ and so $\gamma \in \mathcal{O}_K$ by Lemma 4.2.11 hence $P^* \subseteq \mathcal{O}_K$ and we conclude that $P^* = \mathcal{O}_K$. To obtain the desired contradiction, it suffices to find an element in $P^*$ but not in $\mathcal{O}_K$.

Let $\beta$ be a nonzero element of $P$. Then by Lemma 4.2.7 $\langle \beta \rangle$ contains a product $P_1 P_2 \cdots P_r$ of prime ideals. Choose such a product with fewest possible factors. Then $P \supseteq \langle \beta \rangle \supseteq P_1 P_2 \cdots P_r$ and so $P \supseteq P_j$ for some $j$ by Lemma 4.2.3. We assume, without loss of generality, that $P \supseteq P_1$. Then by maximality of the prime ideal $P_1$, $P = P_1$. Thus $\langle \beta \rangle \supseteq PI$ where $I = P_2 \cdots P_r$. As $r$
was chosen to be minimal then $\langle \beta \rangle \not\subseteq I$. Thus, there exists $\gamma \in I$ but $\gamma \notin \langle \beta \rangle$. Hence $\delta = \gamma / \beta \notin O_K$. But $\gamma P \subseteq PL \subseteq \langle \beta \rangle$ and so $\delta P = \beta^{-1}\gamma P \subseteq O_K$. So $\delta \in P^*$, but as $\gamma \notin \langle \beta \rangle$ then $\delta \notin O_K$.

The assumption that $P^* = O_K$ has led to a contradiction. We cannot then have $PP^* = P$ and we conclude that $PP^* = O_K = \langle 1 \rangle$. ■

**Theorem 4.2.13. (The Fundamental Theorem of Ideals in Number Fields)** Let $K$ be a number field and $I$ be a nonzero ideal of $O_K$. Then $I = P_1P_2 \cdots P_m$, where $P_j$ for $j = 1, 2 \ldots$ are prime ideals and, if the order of the prime ideals is unimportant, this factorization is unique.

**Proof:** We use induction on $N(I)$. When $I$ is prime, we are done. Assume not, by Lemma 4.2.6 $I \subseteq P$ for some prime ideal $P$. Let $P^{-1}$ be the inverse of $P$ as a fractional ideal. Since $P \subseteq O_K$ then $O_K = PP^{-1} \subseteq O_KP^{-1}$. Let $J = IP^{-1}$, since $I \subseteq P$ then $J \subseteq PP^{-1} = O_K$ and $J$ is an ideal of $O_K$. Also $I = PJ$, thus $J$ is a proper ideal of $O_K$.

We know $P^{-1} \supseteq O_K$ but $P^{-1} \not\subseteq O_K$ for otherwise $P^{-1}$ would be $O_K$ which is not an inverse of $P$. Hence $J = IP^{-1} \supseteq IO_K = I$. If we had $J = I$ then $\gamma I \subseteq I$ for all $\gamma \in P^{-1}$ and so $P^{-1} \subseteq O_K$ by Lemma 4.2.11, this contradicts $P^{-1} \not\subseteq O_K$. Therefore, $I \subseteq J$ but $I \neq J$ and so $N(J) < N(I)$. By the inductive hypothesis $J$ is a product of primes, and hence so is $I = PJ$. ■

The unique factorization theorem has some quick consequences.

**Corollary 4.2.14.** Let $K$ be a number field and $I_1, I_2$ be nonzero ideals of $O_K$. Then $I_1 \supseteq I_2$ if and only if there is an ideal $J$ of $O_K$ with $I_2 = I_1 J$.

**Proof:** If $I_2 = I_1 J$ for an ideal $J$ then $I_1 | I_2$, we obtain $I_1 \supseteq I_2$. Conversely, suppose $I_1 \supseteq I_2$, then $O_K = I_1I_1^{-1} \supseteq I_2I_1^{-1}$. Say $J = I_2I_1^{-1}$ is an ideal of $O_K$ and $I_1J = I_1I_2I_1^{-1} = I_2$. ■
**Theorem 4.2.15.** Let $K$ be a number field and $m$ be a positive integer. There are only finitely many ideals $I$ in $\mathcal{O}_K$ with $N(I) = m$.

**Proof:** Let $(m) = p_1^{e_1} p_2^{e_2} \cdots p_g^{e_g}$ be a product of primes. $(m) \subseteq I$ implies $I | (m)$, then we obtain

$I = p_1^{f_1} p_2^{f_2} \cdots p_g^{f_g}$

where $0 \leq f_i \leq g_i$. So there are only finitely many possibilities for $I$. ■
Chapter 5. Ideal class group and class number

In this chapter, we will introduce ideal class group and some of its important properties.

For a number field $K$, we denote by $I_k$ the abelian group formed by the set of fractional ideals of $K$ under multiplication; by $P_k$ we define the subgroup of $I_k$ consisting of the principal fractional ideals.

**Definition 5.0.1.** The class group of $K$, denoted by $Cl_K$, is the quotient group $I_k/P_k$; the elements of $Cl_K$, namely the cosets of $P_k$ in $I_k$, are called ideal classes; the number of ideal classes (i.e., the cardinality of $Cl_K$), denoted by $h_K$, is called the class number of $K$.

An ideal class is an equivalence class of fractional ideals under the equivalence relation $I \sim J$ if $I = \alpha J$ for some nonzero element $\alpha$ in $K$. The set of principal fractional ideals forms an ideal class, the principal ideal class. We denote the ideal class containing the fractional ideal $I$ by $[I]$. We can see $Cl_K$ as the set of such symbols $[I]$ follow the rules:

1. $[I] = [J]$ whenever $J = \alpha I$, and the operation $[I][J] = [IJ]$ is well defined,
2. the identity element of $Cl_K$ is $[\langle 1 \rangle] = [\mathcal{O}_K]$,
3. if $I = \alpha J$ for some ideal $J$, then $[I] = [J]$ and so each ideal class contains ideals.

**Example 5.0.2.** $\mathbb{Z}$, $\mathbb{Z}[\omega]$, and $\mathbb{Z}[\sqrt{-1}]$ have trivial ideal class groups, where $\omega$ is a primitive cubic root of 1.
5.2. Finiteness of $Cl_K$

**Proposition 5.1.1.** Let $K$ be a number field. There is a positive number $m \in K$ such that, in each nonzero ideal $I$ of $O_K$, there is a nonzero element $\beta$ with $|N(\beta)| \leq mN(I)$.

**Proof:** Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ form an integral basis of $O_K$. Let $q = N(I)$ and let $r$ be the integer part of $q^n$, i.e., $r \leq q^n < r + 1$. Consider set

$$S = \{b_1\alpha_1 + b_2\alpha_2 + \cdots + b_n\alpha_n : b_j \in \mathbb{Z}, 0 \leq b_j \leq r\}.$$ 

We can see that $S$ has $(r + 1)^n$ elements and so $|S| > q$. The elements of $S$ cannot lie in distinct cosets of $I$ in $O_K$. Hence there are $\beta_1, \beta_2 \in S$ with $\beta_1 \neq \beta_2$ but $\beta_1 \equiv \beta_2 (\text{mod } I)$. Set $\beta = \beta_1 - \beta_2$. Then $\beta \neq 0$ but $\beta \in I$. Also $\beta = \sum_{j=1}^{n} c_j \alpha_j$ where $c_j \in \mathbb{Z}$ and $|c_j| \leq r$.

Now $N(\beta) = \prod_{k=1}^{n} \sigma_k(\beta)$ and $\sigma_k(\beta) = \sum_{j=1}^{n} c_j \sigma_k(\alpha_j)$. Thus

$$|\sigma_k(\beta)| \leq \sum_{j=1}^{n} |c_j||\sigma_k(\alpha_j)| \leq r \sum_{j=1}^{n} |\sigma_k(\alpha_j)|.$$ 

Multiplying all together, we obtain

$$|N(\beta)| \leq r^n \prod_{k=1}^{n} \sum_{j=1}^{n} |\sigma_k(\alpha_j)| \leq mq = mN(I)$$

With $m = \prod_{k=1}^{n} \sum_{j=1}^{n} |\sigma_k(\alpha_j)|$. ■

**Proposition 5.1.2.** If $m$ is as in the above proposition, then every ideal class in $Cl_K$ contains an ideal of norm $\leq m$.

**Proof:** Let $I$ be an ideal of $O_K$ and consider its ideal class $[I]$. By Proposition 5.1.1. there exists $\beta \in I$, $\beta \neq 0$ with $|N(\beta)| \leq mN(I)$. Since $I \supseteq \langle \beta \rangle$, by Lemma 5.2.12 there is an ideal
\( J \subseteq \mathcal{O}_K \) with \( \langle \beta \rangle = IJ \). Then as \([I][J] = [\langle \beta \rangle] = [\mathcal{O}_K]\) it follows that the class \([J]\) is the inverse of \([I]\), \([J] = [I]^{-1}\). Now \( N(J) = \frac{N(\langle \beta \rangle)}{N(I)} = \frac{|N(<\beta>)|}{N(I)} \leq m \). Therefore, the ideal class \([I]^{-1}\) has an ideal of norm at most \( m \). ■

**Theorem 5.1.3.** Let \( K \) be a number field, then \( Cl_K \) is a finite abelian group.

**Proof:** By Propositions 5.1.1 and 5.1.2, there is a positive number \( m \) with each class of \( K \) containing an ideal of \( \mathcal{O}_K \) with norm at most \( m \). By Lemma 5.2.1, there are only finitely many ideals \( I \) of \( \mathcal{O}_K \) of each given norm, and so there are only finitely many ideals of norm at most \( m \). Hence \( K \) has only finitely many ideal classes, that is \( Cl_K \) is a finite abelian group. ■

**Remark 5.1.4.** The above results (and their proofs) suggest a method to determine \( Cl_K \). Given \( K \), we calculate the bound \( m \) (defined as in the proof of Proposition 5.1.1), and then find all integral ideals of norm at most \( m \). Since every ideal class has a representative among these ideals, we can find \( Cl_K \) by determining how many classes these ideals belong to.

**Remark 5.1.5.** In the quadratic case that \( K = \mathbb{Q}(\sqrt{d}) \), where \(|d|\) is a square-free integer, the bound \( m \) is equal to

\[
m = (|\sigma_1(1)| + |\sigma_1(\sqrt{d})|)(|\sigma_2(1)| + |\sigma_2(\sqrt{d})|) = (1 + \sqrt{|d|})^2 \quad (5.1.1)
\]

if \( d \equiv 2, 3 \mod 4 \), and

\[
m = (|\sigma_1(1)| + |\sigma_1((1 + \sqrt{d})/2)|)(|\sigma_2(1)| + |\sigma_2((1 + \sqrt{d})/2)|) = \frac{(3 + \sqrt{|d|})^2}{4} \quad (5.1.2)
\]

if \( d \equiv 1 \mod 4 \).

**Example 5.1.6.** Let \( K = \mathbb{Q}(\sqrt{-6}) \). Then \( \mathcal{O}_K \) has integral basis \( 1, \sqrt{-6} \). Using the proof of Proposition 5.1.3 we can take
\[
m = (|\sigma_1(1)| + |\sigma_1(\sqrt{-6})|)(|\sigma_2(1)| + |\sigma_2(\sqrt{-6})|) = (1 + \sqrt{6})^2 \approx 11.9.
\]

We shall find all prime ideals of norm at most 11. We find that 2 and 3 split, 5 and 7 and 11 split. In detail \(\langle 2 \rangle = P_2^2\) where \(P_2 = \langle 2, \sqrt{-6} \rangle\), \(\langle 3 \rangle = P_3^2\) where \(P_3 = \langle 3, \sqrt{-6} \rangle\), \(\langle 5 \rangle = P_5Q_5\) where \(P_5 = \langle 5, \sqrt{-6} + 2 \rangle\) and \(Q_5 = \langle 5, \sqrt{-6} - 2 \rangle\), \(\langle 7 \rangle = P_7Q_7\) where \(P_7 = \langle 7, \sqrt{-6} + 1 \rangle\) and \(Q_7 = \langle 7, \sqrt{-6} - 1 \rangle\), and \(\langle 11 \rangle = P_{11}Q_{11}\) where \(P_{11} = \langle 11, \sqrt{-6} + 4 \rangle\) and \(Q_{11} = \langle 11, \sqrt{-6} - 4 \rangle\).

Thus \(P_2, P_3, P_5, Q_5, P_7, Q_7, P_{11}\) and \(Q_{11}\) are prime ideals of norm at most 11, and each ideal class of \(K\) is equal to one of \([P_2], [P_3] \ldots [Q_{11}]\) as a product of some of those, e.g. \(P_2P_3\) if the norm is \(\leq 11\).

Now we look at the factorization of principal ideals of small norm to find the relations between these ideal classes. We’ve already know that \([P_2]^2 = \langle 2 \rangle = \langle 1 \rangle\), \([P_3]^2 = \langle 3 \rangle = \langle 1 \rangle\), \([P_5][Q_5] = \langle 5 \rangle = \langle 1 \rangle\), \([P_7][Q_7] = \langle 7 \rangle\) and \([P_{11}][Q_{11}] = \langle 11 \rangle = \langle 1 \rangle\). Consider \(\langle \sqrt{-6} \rangle\), it has norm 6 = 2 · 3, that is the product of prime ideals of norms 2 and 3. Hence \(\sqrt{-6} = P_2P_3\) and \([P_2][P_3] = \langle 1 \rangle\). As \([P_2]^2 = \langle 1 \rangle\) then \([P_2] = [P_3]\). Next \(\langle 1 + \sqrt{-6} \rangle\) has norm 7, so this is a prime ideal of norm 7. As \(1 + \sqrt{-6} \in P_7\) then \(P_7 = \langle 1 + \sqrt{-6} \rangle\) is principal, and so \([P_7] = \langle 1 \rangle\) and \([Q_7] = \langle 1 \rangle\)[\(P_7\)]\(^{-1}\) = \([1\rangle\). Next \(\langle 2 + \sqrt{-6} \rangle\) has norm 10 and so is the product of prime ideals of norms 2 and 5. Hence it is either \(P_2P_5\) or \(P_2Q_5\). But \(2 + \sqrt{-6} \in P_5\) and so \(\langle 2 + \sqrt{-6} \rangle \subseteq P_5\). Hence \(\langle 2 + \sqrt{-6} \rangle = P_2P_5\) and \([P_5] = [P_2]^{-1} = [P_2]\). Also \([Q_5] = [P_5]^{-1} = [P_2]^{-1} = [P_2]\). Then \(\langle 4 + \sqrt{-6} \rangle\) has norm 22 and so is the product of prime ideals of norms 2 and 11. It is either \(P_2P_{11}\) or \(P_2Q_{11}\). But \(4 + \sqrt{-6} \in P_{11}\) and so \(\langle 4 + \sqrt{-6} \rangle \subseteq P_{11}\). Hence \(\langle 4 + \sqrt{-6} \rangle = P_2P_{11}\) and so \([P_{11}] = [P_2]^{-1} = [P_2]\). Also \([Q_{11}] = [P_{11}]^{-1} = [P_2]^{-1} = [P_2]\). In conclusion, we have \([P_2] = [P_3] = [P_5] = [Q_5] = [P_{11}] = [Q_{11}]\) and \([P_7] = [Q_7] = \langle 1 \rangle\). We
also have \([P_2]^2 = [(1)]\). Therefore, \(Cl_k = \{[(1)], [P_2]\}\). We have seen that \(P_2\) is non-principal so that \([P_2] \neq [(1)]\). So the class group has two element and \(h_k = 2\).

### 5.2. The Minkowski bound

In the previous section, we have seen that there is a positive number \(m\) with each class of \(K\) containing an ideal of \(\mathcal{O}_K\) with norm at most \(m\). This yields a method for us to find \(Cl_K\). This whole process, however, is often very complicated. In this section, we introduce a bound that improves the \(m\) used in section 5.1 a little bit. In applications, this new bound largely reduces the complexity of computation.

Let number field \(K = \mathbb{Q}(\alpha)\), where \(\alpha\) has degree \(n\). Consider the conjugates \(\alpha_1, \alpha_2, \ldots, \alpha_n\) of \(\alpha\). Denote \(s\) as the number of \(\alpha_j\) which are real. Since the nonreal conjugates come in pairs, there are \(2t\) nonreal conjugates of \(\alpha\) and \(s + 2t = n\). The Minkowski bound of \(K\) is

\[
M_K = \left(\frac{4}{\pi}\right)^{\frac{1}{2}} \frac{n!}{n^n} \sqrt{|\Delta_k|},
\]

where \(\Delta_k\) is the discriminant of \(K\).

In particular, when \(K\) is real quadratic then \(M_K = \frac{1}{2} \sqrt{|\Delta_k|}\), and when \(K\) is imaginary quadratic, we have \(M_K = \frac{2}{\pi} \sqrt{|\Delta_k|}\). Comparing these with the \(m\) given by (5.1.1) and (5.1.2), one sees that \(M_K\) is significantly smaller in general.

**Theorem 5.2.1.** Each ideal class of \(K\) contains an ideal \(I\) of \(\mathcal{O}_K\) with \(N(I) \leq M_K\).

**Example 5.2.2.** Let \(K = \mathbb{Q}{}(\sqrt{82})\). We will show the class group is cyclic of order 4.

Note that \(n = 2, t = 0, \Delta_K = 4 \cdot 82\), we have the Minkowski bound approximately 9.055. Now
we look at the primes lying over 2, 3, 5, and 7. The following table describes how \((p)\) factors from the way \(T^2 - 82\) factor modulo \(p\).

<table>
<thead>
<tr>
<th>(p)</th>
<th>(T^2 - 82 \mod p)</th>
<th>((p))</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>(T^2)</td>
<td>(p_2^2)</td>
</tr>
<tr>
<td>3</td>
<td>((T - 1)(T + 1))</td>
<td>(p_3p_3')</td>
</tr>
<tr>
<td>5</td>
<td>Irreducible</td>
<td>Prime</td>
</tr>
<tr>
<td>7</td>
<td>Irreducible</td>
<td>Prime</td>
</tr>
</tbody>
</table>

Thus, the class group of \(\mathbb{Q}(\sqrt{82})\) is generated by \([p_2]\) and \([p_3]\), with \(p_2^2 = <2> \sim <1>\) and \(p_3' \sim p_3^{-1}\).

Since \(N_{K/\mathbb{Q}}(10 + \sqrt{82}) = 18 = 2 \cdot 3^2\), and \(10 + \sqrt{82}\) is not divisible by 3, \((10 + \sqrt{82})\) is divisible by just one of \(p_3\) and \(p_3'\). Let \(p_3\) be that prime, so \((10 + \sqrt{82}) = p_2p_3^2\). Thus \(p_2 \sim p_3^{-2}\), so the class group of \(K\) is generated by \([p_3]\) and we have the formulas

\[
[p_2]^2 = 1, \ [p_3]^2 = [p_2].
\]

Hence \([p_3]\) has order dividing 4.

We will show \(p_2\) is non-principal, so \([p_3]\) has order 4, and thus \(K\) has a class group \(\langle [p_3] \rangle \cong \mathbb{Z}/4\mathbb{Z}\). If \(p_2 = (a + b\sqrt{82})\), then \(a^2 - 82b^2 = \pm 2\), so \(2\) or \(-2\) is congruent to a square modulo 41. This is no contradiction, since \(2 \equiv 17^2 \mod 41\). We need a different idea.

The idea is to use the known fact that \(p_2^2\) is principal. If \(p_2 = (a + b\sqrt{82})\), then \((2) = p_2^2 = \left((a + b\sqrt{82})^2\right)\), so \(2 = (a + b\sqrt{82})^2 u\), where \(u\) is a unit.
Taking norms here $N(u)$ must be positive, so $N(u) = 1$. The unit group of $\mathbb{Z}[\sqrt{82}]$ is $\pm (9 + \sqrt{82})^2$, with $9 + \sqrt{82}$ having norm $-1$. Therefore, the positive units of norm $1$ are the integral powers of $(9 + \sqrt{82})^2$, which are all squares. A unit square can be absorbed into the $(a + b\sqrt{82})^2$ terms, so we have to be able to solve $2 = (a + b\sqrt{82})^2$ in integers $a$ and $b$. This implies $\sqrt{2}$ lies in $\mathbb{Z}[\sqrt{82}]$. Thus, $p_2$ is not principal.

**Example 5.2.3.** Let $K = \mathbb{Q}(\sqrt{-14})$. We will show the class group is cyclic of order $4$. $n = 2$, $t = 1$, $\Delta_k = 4 \cdot -14 = -56$, so the Minkowski bound is approximately $4.764$. So the class group is generated by primes dividing $(2)$ and $(3)$ . The following table describes how $(2)$ and $(3)$ factor in $\mathcal{O}_K$ from the way $T^2 - 82$ factor modulo $2$ and modulo $3$.

<table>
<thead>
<tr>
<th>$p$</th>
<th>$T^2 + 14 \mod p$</th>
<th>$(p)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>$T^2$</td>
<td>$p_2^2$</td>
</tr>
<tr>
<td>3</td>
<td>$(T - 1)(T + 1)$</td>
<td>$p_3 p_3'$</td>
</tr>
</tbody>
</table>

Since $p_2^2 \sim 1$ and $p_2 \sim p_2^{-1}$. 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 non-principal, since 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 $N_{K/\mathbb{Q}}(2 + \sqrt{-14}) = 18 = 2 \cdot 3^2$. And the ideal $(10 + \sqrt{82})$ is divisible by just one of $p_3$ and $p_3'$. Since $10 + \sqrt{82}$ is not a multiple of $3$. We may let $p_3$ be the prime of norm $3$ dividing $(2 + \sqrt{-14})$. Then $p_2 p_3^2 \sim 1$, so $p_3^2 \sim p_2^{-1} \sim p_2$ and the class group of $K$ is generated by $[p_3]$. Since $p_2$ is non-principal and $p_2^2 \sim 1$, $[p_3]$ has order $4$. Hence, the class group of $K$ is cyclic of order $4$. 


5.3. Further remarks

Other than that the class number of a given number field is finite, more about the values of class numbers is known to us.

Take the quadratic case as an example. The classical class number problem of Gauss asks for a classification of all quadratic fields with a given class number \( k \). In particular, Gauss conjectured

1. \( h_d \to \infty \) as \( -d \to \infty \) (thus \( h_d \) can be arbitrarily large);

2. For each positive integer \( k \), there are finitely many imaginary quadratic fields with class number equal to \( k \). In particular, there are exactly 9 imaginary quadratic fields with class number one, namely: \( \mathbb{Q}(\sqrt{-1}) \), \( \mathbb{Q}(\sqrt{-2}) \), \( \mathbb{Q}(\sqrt{-3}) \), \( \mathbb{Q}(\sqrt{-7}) \), \( \mathbb{Q}(\sqrt{-11}) \), \( \mathbb{Q}(\sqrt{-19}) \), \( \mathbb{Q}(\sqrt{-43}) \), \( \mathbb{Q}(\sqrt{-67}) \), and \( \mathbb{Q}(\sqrt{-163}) \);

3. There are infinitely many real quadratic fields with class number one.

These conjectures have stimulated the development of number theory. We do not want to review the complete history here, but it is worth mentioning that conjecture (1) was proved by Heilbronn in 1934; The class number 1 problem of imaginary quadratic fields was solved from the work of Baker (1966), Stark (1967), and Heegner (1952); The class number 2 problem was solved from the work of Baker (1971), and Stark (1971); In 2004, Mark Watkins found the complete list of imaginary quadratic fields with class number up to 100.

In the real quadratic case, we have a completely different story. Lack of understanding of the fundamental units, people know very little about how the class numbers are distributed. In view of this, conjecture (3) is still big open.
Bibliography


