The Ideal Class Group of Quadratic Fields

by

Ravinder Sra

THESIS SUBMITTED IN PARTIAL FULFILMENT OF
THE REQUIREMENTS OF THE DEGREE OF
MASTER OF SCIENCE
IN
MATHEMATICS

UNIVERSITY OF NORTHERN BRITISH COLUMBIA

April 2023

Dedicated

to

My mother(Mohinder Kaur)

Acknowledgement

I would like to thank my supervisor Dr. Edward Dobrowolski who took over the task of helping me finish my thesis.

Prince George, BC
April 11, 2023 *(Ravinder Singh Sra)*

Abstract

The ideal class group problem is one of the very interesting problems in algebraic number theory. In this thesis we focused on quadratic fields. We studied the group of units of the rings of algebraic integers and calculated fundamental units in several quadratic fields. We also studied a detailed proof of the analytic Dirichlet class number formula with numerical examples and its relation to binary quadratic forms. In addition, we also presented a detailed proof of Carlitz's theorem with numerical examples.

Contents

Chapter 1

Introduction

We assume that reader is familiar with notions of field, ring, and group. For example $\mathbb{Q}, \mathbb{R}$, and $\mathbb{C}$ are fields. Let E be a field and $F \subseteq E$. Then F is a subfield of E if it is a field with respect to operations from E. For example, $\mathbb{Q}$ is a subfield of $\mathbb{R}$, and $\mathbb{R}$ is a subfield of $\mathbb{C}$.
If E is a subfield of F, $E \subseteq F$, then F is a vector space over E, where elements of F are considered as 'vectors' and elements of E as 'scalars'.

1.0.1 Preliminaries

Definition 1 (Degree of Extension)**.**
The dimension of F considered as a vector space over E is denoted by $[F : E]$ and is called the degree of F over E.

Such degree can be finite or infinite.
For example $[\mathbb{R} : \mathbb{Q}] = \infty$, but $[\mathbb{C} : \mathbb{R}] = 2$.
In this thesis, we will consider only subfields of $\mathbb{C}$ that are finite extensions of $\mathbb{Q}$.

Definition 2 (Algebraic element)**.**
An element α of field K is called algebraic if α is a root of a polynomial with rational

coefficients.

Definition 3 (Algebraic Extension)**.**

An extension K of $\mathbb{Q}$ *(finite or infinite) is called algebraic if every element* α *of K is algebraic over* $\mathbb{Q}$*, that is,* α *is root of a polynomial with rational coefficients.*

Definition 4 (Adjoining elements to $\mathbb{Q}$)**.**

Let $\alpha_1, \alpha_2, ...\alpha_n$ *be complex numbers. The smallest subfield of* $\mathbb{C}$ *containing* $\mathbb{Q}$ *and* $\alpha_1, \alpha_2, ...\alpha_n$ *is denoted by* $\mathbb{Q}(\alpha_1, \alpha_2, ...\alpha_n)$*. Such field always exists and it is the intersection of all subfields of* $\mathbb{C}$ *containing* $\mathbb{Q}$ *and* $\alpha_1, \alpha_2, ...\alpha_n$*. We say that K is obtained from* $\mathbb{Q}$ *by adjoining* $\alpha_1, \alpha_2, \ldots, \alpha_n$.

Definition 5 (Algebraic number field)**.**

An algebraic number field is a finite degree field extension of the field of rational numbers $\mathbb{Q}$.

Note: It is known that

1. Every field extension of $\mathbb{Q}$ of finite degree is algebraic, and

2. Every algebraic number field is generated by a single element.

For example, it is easy to show that $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$.
We have $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, the basis of $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$ is $[1, \sqrt{2}]$, and every element of $\mathbb{Q}(\sqrt{2})$ is algebraic.
Another example: $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. This field is generated by a single element $\theta = \sqrt{2} + \sqrt{3}$.
The minimal polynomial of θ is $x^4 - 10x^2 + 1$, and its conjugates are
$\theta = \sqrt{2} + \sqrt{3}, \sqrt{2} - \sqrt{3}, -\sqrt{2} + \sqrt{3}$, and $-\sqrt{2} - \sqrt{3}$. Thus, $K = \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\theta)$.
We have $[K : \mathbb{Q}] = 4$, the basis of K over $\mathbb{Q}$ is $[1, \theta, \theta^2, \theta^3]$, another basis is $[1, \sqrt{2}, \sqrt{3}, \sqrt{6}]$.

Definition 6 (Cyclotomic field)**.**

A cyclotomic field is a number field obtained by adjoining a complex root of unity to $\mathbb{Q}$.

Definition 7 (Algebraic integer)**.**

An algebraic integer is any complex number that is a root of ***monic*** *polynomial with coefficient in* $\mathbb{Z}$.

For example, the rational integers are algebraic integers, the numbers $a+b\sqrt{2}$ where $a,b \in \mathbb{Z}$ are algebraic integers, but perhaps surprisingly, unlike the rational integers, algebraic integers may have nontrivial denominators. For example, $\alpha = \frac{1+\sqrt{5}}{2}$ is an algebraic integer because it is a root of $x^2 - x - 1$.

Definition 8 (Ring of algebraic integers in a field)**.**

The set of all algebraic integers in an algebraic field K forms a ring denoted by O_K.

Definition 9 (Quadratic fields)**.**

A quadratic field is an algebraic number field of degree two over $\mathbb{Q}$. *Every quadratic field is of the form* $\mathbb{Q}(\sqrt{d})$, *where d is a square free integer other than* 0 *and* 1. *If* $d > 0$, *the corresponding quadratic field is called a* real quadratic field, *and for* $d < 0$ *an* imaginary quadratic field *or* complex quadratic field.

We are interested in the arithmetics in the rings of algebraic integers.

1.0.2 Ideals

Note: In this thesis we consider only commutative rings. In what follows we assume that every ring under consideration is commutative.

Definition 10 (Ideal)**.**

Let $(R,+,.)$ be a commutative ring. A subset I of R is called an ideal of R if $(I,+)$ is subgroup of $(R,+)$ and for every $r \in R$ and $x \in I$, $rx \in I$.

Notation: $I \triangleleft R$ means that I is an ideal of R.

An ideal I of R other than R is called a proper ideal.

Multiplication of Ideals

Let I and J be two ideals of a ring R, the product IJ is the smallest ideal containing all the products of elements of I with elements of J, that is

$$IJ = \{\sum_{k=1}^{n} r_k i_k j_k | i_k \in I, j_k \in J, n \in \mathbb{N}, r_k \in R\}.$$

Notation: Let $a_1, \ldots, a_n$ be elements of a commutative ring R. The smallest ideal that contains these elements is denoted by $(a_1, \ldots, a_n)$. Clearly we have

$$(a_1, \ldots, a_n) = \{r_1 a_1 + \cdots + r_n a_n | r_i \in R, i = 1 \ldots n\}$$

Consequently, if $I = (a_1, b_1), J = (a_2, b_2)$ are two ideals in R

then $IJ = (a_1a_2, a_1b_2, b_1a_2, b_1b_2)$.

An application of this formula is shown in the next example.

Example. Consider the ideal $I = (2, 1+\sqrt{-5})$ in $\mathbb{Z}[\sqrt{-5}]$. We shall prove that $I^2 = (2)$. We have

$$I^2 = (2, 1+\sqrt{-5})(2, 1+\sqrt{-5}) = (4, 2(1+\sqrt{-5}), 2(1+\sqrt{-5}), -2(2-\sqrt{-5})).$$

Since every generator of I^2 is a multiple of 2, we conclude that

$$(2, 1+\sqrt{-5})^2 \subseteq (2).$$

On the other hand $2\sqrt{-5} = 4 - 2(2-\sqrt{-5}) \in (2, 1+\sqrt{-5})^2$, and also
$2 = 2(1+\sqrt{-5}) - 2\sqrt{-5}$. By combining these two equalities, we conclude that $2 \in I^2$ as a linear combination of generators of I^2 with coefficients from $\mathbb{Z}[\sqrt{-5}]$.
Thus $(2) \subseteq I^2$. Since we have showed above that $I^2 \subseteq (2)$, we conclude that $(2) = I^2$.

The situation in the ring of rational integers $\mathbb{Z}$ is rather trivial. It is easy to show that every ideal of $\mathbb{Z}$ is generated by a single element. For example,let $I = (2) = 2\mathbb{Z}$, and $J = (3) = 3\mathbb{Z}$. Then $IJ = (2)(3) = (2 \times 3) = 6\mathbb{Z}$. We see that in this case the ideals behave just like numbers. This was an initial idea to use ideals, especially in a number fields. As we will see later, algebraic integers may not have unique factorization property, but ideals do.

Propostion 1. *The ideals of the ring of integers of an algebraic number field form an Abelian semigroup with unity.*
It means that the multiplication is commutative and associative. The ring itself is the unity.

Definition 11 (Prime ideal)**.**
A proper ideal P of an integral domain $D^\star$ is called prime ideal if for all $a, b \in D$, $ab \in P$ implies $a \in P$ or $b \in P$.

* The definition of integral domain and its forms are discussed in the next section. Here we note that O_K is an integral domain.

Definition 12 (Maximal ideal)**.**
In a ring R, a proper ideal I is called maximal ideal, if there exist no other proper ideal J of

R such that $I \subseteq J \subseteq R$. That is if $I \subseteq J \subseteq R$, then either $I = J$ or $J = R$.

Propostion 2. *If $\mathfrak{p}$ is a prime ideal in O_K then $\mathfrak{p} \bigcap \mathbb{Q} = p\mathbb{Z}$. Hence $\mathfrak{p}$ contains a unique prime number p.*

Proof. It suffices to notice that $\mathfrak{p} \bigcap \mathbb{Q}$ is a prime ideal in $\mathbb{Z}$ which is easy to prove. □

Propostion 3. *Every prime ideal of O_K is a maximal ideal of O_K.*

Proof. Let $\mathfrak{p}$ be a prime ideal in O_K. We know then that the quotient ring $A = O_K/\mathfrak{p}$ is an integral domain, that is, has no zero divisors. The ideal $\mathfrak{p}$ is maximal if and only if A is a field. Hence, it remains to show that every nonzero element of A is invertible, that is, if $\alpha \in O_K \setminus \mathfrak{p}$ then there exists $\beta \in O_K$, such that

$$(\alpha + \mathfrak{p})(\beta + \mathfrak{p}) = 1 + \mathfrak{p}.$$

Let $f(x) = x^m + c_{m-1}x^{m-1} + \cdots + c_m$ be the smallest degree monic polynomial in $\mathbb{Z}[x]$, such that $f(\alpha) \in \mathfrak{p}$. Such polynomials certainly exist, since α is an algebraic integer so, $g(\alpha) = 0 \in \mathfrak{p}$ for some monic polynomial $g(x)$ in $\mathbb{Z}[x]$. We have $\alpha^m + c_1\alpha^{m-1} + \cdots + c_m \in \mathfrak{p}$. Thus

$$\alpha(\alpha^{m-1} + \cdots + c_{m-1}) + \mathfrak{p} = -c_m + \mathfrak{p}.$$

Let p be the unique prime number in $\mathfrak{p}$. Then p cannot divide c_m, since otherwise we would have $\alpha^{m-1} + \cdots + c_{m-1} \in \mathfrak{p}$ because $\mathfrak{p}$ is a prime ideal not containing α, but this contradicts the fact that m was minimal. Hence, there are integers a and $b <$ such that $ac_m + bp \equiv 1 \mod p$. Let $\beta = a(\alpha^{m-1} + \cdots + c_{m-1})$. Then

$$(\alpha + \mathfrak{p})(\beta + \mathfrak{p}) = (\alpha\beta + \mathfrak{p}) = 1 + \mathfrak{p}$$

which finishes the proof. □

Note: Every maximal ideal in any domain is a prime ideal but the converse is in general false. However as we have proved above, the converse is true in the ring of algebraic integers O_K.

Propostion 4. *If* $\mathfrak{p}$ *is a prime ideal of* O_K*, and* $\mathfrak{a}$ $\mathfrak{b}$ *are ideals in* O_K*, then*

$$\mathfrak{p} \supset \mathfrak{ab} \Rightarrow \mathfrak{p} \supset \mathfrak{a} \text{ or } \mathfrak{p} \supset \mathfrak{b}.$$

Further, if $\mathfrak{p} \supset \mathfrak{p}_1 \dots \mathfrak{p}_r$*, where all ideals* $\mathfrak{p}_i$ *are prime then*

$$\mathfrak{p} = \mathfrak{p}_i \text{ for some } i.$$

Proof. The first part follows directly from the definition of prime ideal. The second uses the fact that prime ideals are maximal. □

Theorem 1. *Let K be an algebraic number field. Then every proper ideal of* O_K *can be expressed uniquely up to order as a product of prime ideals.*

Note: This s a very important theorem. In general,as we mentioned above, algebraic integers do not factor uniquely into a product of irreducible (or prime) elements, but the ideal do. This is the reason we are using ideals in studying algebraic number fields. The proof of this theorem can be found in most textbooks on algebraic number theory, for example in ([1], Theorem 8.3.1).

Definition 13 (Fractional ideal)**.**

Let D be an integral domain, and K be quotient field of D. A nonempty subset A of K with following three properties:

1. $\alpha, \beta, \in A \Rightarrow \alpha + \beta \in A$.

2. $\alpha \in A, r \in D \Rightarrow ra \in A$.

3. There exists a nonzero $\gamma \in D$ *such that* $\gamma A \subseteq D$,

is called fractional ideal *of D.*

Note: For clarity, we will refer to ordinary ideals of D as integral ideals, so every integral ideal of D is also a fractional ideal but not vice versa.

If A is a fractional ideal of D then

$A = \frac{1}{\gamma} I$, where γ is nonzero and $\gamma \in D$ and I is integral ideal of D.

For example, let

$$A = \left\{ \frac{n}{25} : n \in \mathbb{Z} \right\}$$

so A is a nonempty subset of $\mathbb{Q}$. Clearly A has properties (1) and (2). Also,

$25A = \mathbb{Z}$ so that (3) holds. Hence A is a fractional ideal of $\mathbb{Z}$.

One more example, $\frac{5}{4}\mathbb{Z}$ is a fractional ideal of $\mathbb{Z}$

The multiplication of fractional ideals is defined in exactly the same way as multiplication of integral ideals. However, while integral ideals form a semigroup, the fractional ideals form a group. We have

Theorem 2. *The set of fractional ideals of an algebraic number field K form an Abelian group under multiplication.*

Proof. The identity element is O_K as in the case of semigroup of integral ideals. It is easily seen that the product of fractional ideals is a fractional ideal, their multiplication is commutative and associative. However, the existence of an inverse ideal requires proof. We need to prove that if I is a fractional ideal of K then there exists a fractional ideal J of K, such that $IJ = O_K$.

We will somewhat modify an expository paper by Keith Conrad ([5]).

Suppose that I is a fractional ideal of K. Then for some $\gamma \in K$, γI is a proper ideal of O_K. Consequently, $\gamma I = \mathfrak{p}_1 \dots \mathfrak{p}_m$, where $\mathfrak{p}_i, i = 1 \dots m$ are prime ideals. The next step is to show that each prime ideal of O_K is invertible.

Let $\mathfrak{p}$ be prime ideal of O_K. Define $\tilde{\mathfrak{p}}$ by

$$\tilde{\mathfrak{p}} = \{\gamma \in K : \gamma\mathfrak{p} \subseteq O_K\}.$$

Then this definition directly implies that $\tilde{\mathfrak{p}}$ is a fractional ideal. Indeed, the closure under addition or subtraction is clear, as is the closure under multiplication by elements form O_K. Further, for any δ from $\mathfrak{p}$, $\delta\tilde{\mathfrak{p}} \subseteq O_K$.

We show first that $\mathfrak{p} \supsetneq O_K$.

The inclusion $\mathfrak{p} \supset O_K$ follows directly from definition of $\tilde{\mathfrak{p}}$. It remains to show the existence of $x \in \tilde{\mathfrak{p}} \setminus O_K$. For this, let x be any nonzero element of $\mathfrak{p}$. Then

$$(x) \subseteq \mathfrak{p}.$$

Suppose that the ideal (x) factors as

$$(x) = \mathfrak{q}_1 \dots \mathfrak{q}_r$$

into a product of prime ideals.

If $r = 1$ we get

$$\mathfrak{p} \supseteq (x) = \mathfrak{q}_1.$$

But $\mathfrak{p}$ and $\mathfrak{q}_1$ are maximal as prime ideals. Hence $\mathfrak{p} = (x)$. Consequently, $\frac{1}{x} \in \tilde{\mathfrak{p}}$, and $\frac{1}{x} \notin O_K$.

Suppose then that $r \geq 2$. Then $(x) = \mathfrak{q}_1 \dots \mathfrak{q}_r \subset \mathfrak{q}_2 \dots \mathfrak{q}_r$ and by unique factorization of ideals the inclusion is sharp. Therefore there exists $y \in \mathfrak{q}_2 \dots \mathfrak{q}_r \setminus (x)$.

Now, we will use the fact that $\tilde{\mathfrak{p}} \supsetneq O_K$ to show that $\tilde{\mathfrak{p}}$ is the inverse of $\mathfrak{p}$.

Pick $x \in \tilde{\mathfrak{p}}$ that is not in O_K. Then $(x)\mathfrak{p} \subseteq O_K$, so

$$\mathfrak{p} \subseteq \mathfrak{p} + (x)\mathfrak{p} \subseteq O_K.$$

Clearly, $\mathfrak{p} + (x)\mathfrak{p}$ is an ideal. Since $\mathfrak{p}$ is maximal, there are two possibilities:

1. $\mathfrak{p} + (x)\mathfrak{p} = O_K$, and

2. $\mathfrak{p} = \mathfrak{p} + (x)\mathfrak{p}$.

The first possibility gives

$$\mathfrak{p} + (x)\mathfrak{p} = \mathfrak{p}(O_K + (x)) = O_K.$$

This means that $\tilde{\mathfrak{p}} = O_K + (x)$ is the inverse of $\mathfrak{p}$.

It remains to rule out the second possibility. It implies that

$$x\mathfrak{p} \subseteq \mathfrak{p}.$$

We will see later that every ideal has integral basis, that is there are elements $\alpha_1, \ldots, \alpha_n$ of $\mathfrak{p}$, such that every element of $\mathfrak{p}$ can be uniquely expressed as a linear combination of these elements with coefficients in $\mathbb{Z}$. This gives

$$x \begin{bmatrix} \alpha_1 \\ \ldots \\ \alpha_n \end{bmatrix} = \begin{bmatrix} z_{11} & \ldots & z_{1n} \\ \ldots & \ldots & \ldots \\ z_{n1} & \ldots & z_{nn} \end{bmatrix} \begin{bmatrix} \alpha_1 \\ \ldots \\ \alpha_n \end{bmatrix}$$

This implies that x is an eigenvalue of the characteristic polynomial of the matrix $[z_{ij}]$. This polynomial is monic and so x is an algebraic integer in O_K, which is not the case.

We conclude that prime ideals are invertible fractional ideals.

Returning now to any nonzero fractional ideal I we know that γI is an integral ideal for some nonzero $\gamma \in O_K$. Hence $\gamma I = \mathfrak{p}_1 \ldots \mathfrak{p}_r$ is a product of prime ideals which are invertible. Therefore

$$I^{-1} = \frac{1}{\gamma}\mathfrak{p}_1^{-1} \ldots \mathfrak{p}_r^{-1}$$

is a fractional ideal that is the inverse of I. □

Definition 14 (Norm of ideal)**.**

Let I be a nonzero (proper) ideal, then norm of I is defined by

$$N(I) = |O_K/I| = [O_K : I].$$

Thus, the norm of a non zero ideal I of a ring O_K is the size of finite quotient ring O_K/I. The norm of the zero ideal is taken to be zero.

Propostion 5. *If J is an ideal in O_K then $N(J) = |O_K/J|$ is finite.*

Proof. In Section 1.0.4 we prove [Theorem 4] that O_K has an integral basis. Let $[K:\mathbb{Q}] = n$ and $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ be such a basis. It is easy to show that $J \cap \mathbb{Z}$ is an integral ideal in $\mathbb{Z}$. Since $\mathbb{Z}$ is PID, there exists a positive integer a, such that $J \cap \mathbb{Z} = (a)$ and obviously $(a) \subseteq J$. There exist natural homomorphism $\phi : O_K/(a) \longrightarrow O_K/J$ defined by $\phi(x+(a)) = x+J$. Clearly, ϕ is onto. It is suffices to show that $O_K/(a)$ is finite.

$O_K = \{m_1\alpha_1 + m_2\alpha_2 + \cdots + m_n\alpha_n | m_i \in \mathbb{Z}, i = 1, \ldots, n\}$.

Every element of (a) is multiple of a, so

$(a) = \{m_1\alpha_1 + m_2\alpha_2 \cdots + m_n\alpha_n | m_i \in \mathbb{Z} \text{ and } a | m_i\}$

because if $m_1\alpha_1 + m_2\alpha_2 \cdots + m_n\alpha_n$ is multiple of a then

$m_1\alpha_1 + m_2\alpha_2 \cdots + m_n\alpha_n = a(m'_1\alpha_1 + m'_2\alpha_2 + \cdots + m'_n\alpha_n)$

$= am'_1\alpha_1 + am'_2\alpha_2 + \cdots + am'_n\alpha_n$,

by linear independence of basis, we conclude that $m_i = am'_i$ for each $i = 1, 2, \ldots, n$,

we conclude that (a) has a^n cosets in O_K, because there are a residues for each m_i modulo a.

□

Later we will state an equivalent definition of the norm of an ideal in another form.

Note: It is not difficult to prove that the norm is multiplicative, that is $N(IJ) = N(I)N(J)$. Also $N(J) = 1$ if and only if $J = O_K$. This implies the following

Propostion 6. *If norm of an ideal is a prime number, that is, $N(J) = p$, then J is a prime ideal.*

Proof. If $J = LM$, where L and M are ideals, then $N(J) = N(LM) = N(L)N(M) = p$. Hence $N(L)$ or $N(M) = 1$. This implies that $L = O_K$ or $M = O_K$. Therefore J is irreducible, hence a prime ideal. □

In order to define a *norm of an element* we need some preliminary notions.

Let K be an algebraic number field. An *embedding* of K into the field of complex number $\mathbb{C}$ is a homomorphism of K into $\mathbb{C}$. We know that K is generated by a single algebraic element θ. Suppose that $\deg\theta = n$, so θ has n algebraic conjugates including itself. Let $\theta = \theta_1, \theta_2, \ldots, \theta_n$ be these conjugates.

If $\sigma : K \to \mathbb{C}$ is an embedding then σ is an isomorphism of K onto $\sigma(K)$. Each such isomorphism is completely defined by the value of $\sigma(\theta)$ which must be one of the conjugates θ_i. There are exactly n such embedding, so we have n embedding $\sigma_1, \sigma_2, \ldots, \sigma_n$ with $\sigma_i = \theta_i$ for all $i = 1, 2, \ldots, n$.

Definition 15 (Norm of an element)**.**

Let K be an algebraic number field and let $\sigma_1, \sigma_2, \ldots, \sigma_n$ be a complete set of embeddings of K into $\mathbb{C}$. If $\alpha \in K$ then $N_{K/\mathbb{Q}}\alpha$ is defined by

$$N_{K/\mathbb{Q}}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha).$$

Note : If $[K : \mathbb{Q}] = n$, $\alpha \in K$ and $\deg\alpha = m$, then $[\mathbb{Q}(\alpha) : \mathbb{Q}] = m$, and $m|n$ because

$$[K : \mathbb{Q}] = [K : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}].$$

If $\alpha_1 = \alpha, \alpha_2 \ldots, \alpha_m$ are conjugate of α then

$$N_{K/\mathbb{Q}}(\alpha) = \left(\prod_{j=1}^{m} \alpha_j \right)^{\frac{n}{m}}$$

because, it can be shown that each conjugate α_j will occur the same number of times among $\sigma_1(\alpha), \sigma_2(\alpha), \ldots, \sigma_n(\alpha)$, that is $\frac{n}{m}$ times.

Corollary 1. *In the case when* $\alpha \in K$, $[K:\mathbb{Q}] = \deg\alpha = n$ *we get*

$$N(\alpha) = \alpha_1\alpha_2\ldots\alpha_n,$$

where $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_n$ *are the conjugates of* α.

The situation is easy when K is a quadratic field.

Corollary 2. *Let* α *be element of a quadratic number field* $K = \mathbb{Q}(\sqrt{d})$. *Then there are exactly two embeddings* σ_1, *and* σ_2 *of* K *into* $\mathbb{C}$, *given by* $\sigma_1(\sqrt{d}) = \sqrt{d}$, *and* $\sigma_2(\sqrt{d}) = -\sqrt{d}$. *If* $\alpha = a + b\sqrt{d}$ *then the norm of* α *equals*

$$N(\alpha) = \sigma_1(\alpha)\sigma_2(\alpha) = \alpha\bar{\alpha},$$

where we denoted $\sigma_2(\alpha)$ *by* $\bar{\alpha}$.

If $\alpha \notin \mathbb{Q}$ *then* $\bar{\alpha}$ *is its algebraic conjugate, if* $\alpha \in \mathbb{Q}$ *then* $\bar{\alpha} = \alpha$.

Thus we have $N(a + b\sqrt{d}) = a^2 - db^2$,

$N(2) = 4$ because $a = 2, b = d = 0$,

$N(\sqrt{10}) = -10$ because $a = 0, b = 1, d = 10$

Definition 16 (Principal ideal)**.**

A principal ideal is an ideal I in ring R that is generated by single element a of R,we write $I = (a)$.

We have $I = \{ra : r \in R\}$

For example, for positive integer 5 the set

$$5\mathbb{Z} = \{0, \pm 5, \pm 10, \ldots\}$$

is an ideal of $\mathbb{Z}$ and $5\mathbb{Z}$ is principal ideal generated by 5 (or-5) so that

$$5\mathbb{Z} = (5) = (-5)$$

.

Propostion 7. *Principal fractional ideals form a group under multiplication.*

It is a subgroup of the group of fractional ideals.

Proof. Let K be a field, I and J be principal ideals. Principal ideals are a subset of the fractional ideals, it is sufficient to show that I and J are closed under multiplication and inverse. Since I and J are principal ideals,

$aI = (b), cJ = (d)$ for $a,b,c,d \in O_K$ where $a,c \neq 0$.

I is multiple of $\frac{b}{a}$, and J is multiple of $\frac{d}{c}$ and their product IJ is multiple of $\frac{bd}{ac}$, which is again a fractional ideal thus closed under multiplication.

I^{-1} is multiple of $\frac{a}{b}$ which is again a fractional ideal thus closed under inverse. □

1.0.3 Domain

Definition 17 (Integral domain)**.**

An integral domain is a nonzero commutative ring in which the product of any two nonzero elements is nonzero.

Definition 18 (Unit in an integral domain)**.**

An element u of an integral domain D is said to be a unit if there exist some element u^{-1} such that $uu^{-1} = 1$.

Definition 19 (Irreducible element in an integral domain)**.**

An irreducible element of an integral domain is a nonzero element that is not invertible and is not the product of two non invertible elements.

Definition 20 (Prime element in an integral domain)**.**

An element p is said to be prime element of an integral domain D if $p \neq 0$, p is a nonunit and if $p|ab$ then either $p|a$ or $p|b$ for $a,b \in D$.

Unique factorization domain or UFD

Definition 21 (Associate element)**.**

Two elements a and b in an integral domain D are called associated if $b = au$*, where u is unit in D, then* $a = bu^{-1}$.

Example. In $\mathbb{Z}$, we have

$30 = (2)(3)(5) = (-2)(-3)(5) = (2)(-3)(-5) = (-2)(3)(-5)$.

The elements 2 and -2, 3 and -3, 5 and -5 are associated elements.

Definition 22 (Unique factorization domain)**.**

An integral domain D is called unique factorization domain, or UFD, if every nonzero, nonunit element a of D can be expressed as product of irreducible elements and a every two such factorization the number of factors is the same and corresponding elements are associated.

For example, $\mathbb{Z}$ is UFD. This is known as the fundamental theorem of arithmetic.

Note: If $a_1a_2\ldots a_n = b_1b_2\ldots b_n$ and a_i is associated with b_i for each $i = 1,2,\ldots,n$ then $b_1 = a_1u_1\ldots b_n = a_nu_n$ with units $u_1,u_2,\ldots,u_n$ then

$b_1b_2\ldots b_n = (u_1u_2\ldots u_n)a_1a_2\ldots a_n = va_1a_2\ldots a_n$,

so we say that D is UFD, if every nonzero, nonunit element of D can be written in a unique form $c = va_1a_2\ldots a_n$, where v is unit in D and $a_1,a_2,\ldots,a_n$ are irreducible elements of D.

Definition 23 (Principal ideal domain)**.**

A principal ideal domain, or PID, is an integral domain in which every ideal is principal i.e. can be generated by a single element.

Propostion 8. *Suppose that a principal ideal domain R is not a field. Then an ideal* $I = (p)$ *is maximal if and only if p is an irreducible element.*

Proof. $(\Rightarrow)$ Let $I = (p)$ be a maximal ideal.

If $p = 0$ then (0) would be the only proper ideal in R. This implies that for any $p \neq 0$ we

have $(p) = R$ which implies that for some $s \in R$, $sp = 1$, so every nonzero p is invertible and R is a field, against our assumption. Similarly, p cannot be a unit, because then $p^{-1} \in R$, and $1 = p^{-1}p \in I$, so $I = R$, which is not the case.

Now, suppose that $p = ab$. Then $a|p$. Hence $(p) = pR \subseteq aR = (a)$.

However I is a maximal ideal, hence either $I = aR$ or $aR = R$

Suppose $I = aR$ then $a \in P$, because $1 \in R$. Hence $a = pq$ with some $q \in R$.

We get$p = ab = pqb$. Since the cancellation law holds in a domain, we get $1 = qb$. Hence b is a unit.

Now suppose that $aR = R$. Since $1 \in R$, we get $1 = as$, with some $s \in R$. Hence, a is unit.

So in both cases, $p = ab$ either a is unit or b is unit,

Thus $p = ab$ implies that a or b is a unit. Therefore p is irreducible.

($\Leftarrow$) Let p be an irreducible element of R.

Then $(p) \neq R$, since $(p) = R$ would imply that p is a unit.

Suppose that $(p) \subseteq J \subsetneq R$. Now, J is an ideal in R, but R is a PID, so $J = (q)$ for some $q \in R$. This implies that $q|p$. However p is irreducible, so $p = qs$, where s is a unit of R. Then $(p) = (qs) = Rsq = (Rs)q = Rq = (q)$, which proves that (p) is maximal. □

We are going to prove now that every PID is a UFD ring. The next proposition is the first step in this direction.

Propostion 9. *In every PID the ascending chain of ideals*

$$(a_1) \subseteq (a_2) \subseteq (a_3) \dots$$

stabilizes, that is $(a_n) = (a_m)$ for all $n \geq m$, staring at some m. This is called the ascending chain condition on principal ideals.

Proof. If $(a_1) \subseteq (a_2) \subseteq \dots$ is an ascending chain of ideals in R, let $A = \bigcup_{i=1}^{\infty}(a_i)$. We claim that A is an ideal. Suppose $a, b \in A$, then $a \in (a_j)$ and $b \in (a_k)$, for some $j, k \geq 1$. Either

$j \geq k$ or $k \geq j$, suppose $k \geq j$. Then $(a_j) \subseteq (a_k)$, so that $a, b \in (a_k)$. Since (a_k) is an ideal we know that $a - b \in (a_k) \subseteq A$ and $ra \in (a_k) \subseteq A$ for some $r \in R$. Therefore, A is an ideal and R is PID, $A = (c)$ for some $c \in R$. Since $A = \bigcup(a_i)$, we know that $c \in (a_n)$ for some n. consequently, $(c) \subseteq (a_n)$ and for each $i \geq n$

$(a_n) \subseteq (a_i) \subseteq \bigcup(a_t) = A = (c) \subseteq (a_n)$

Therefore, $(a_i) = (a_n)$ for each $i \geq n$.

□

Corollary 3. *Let R be a PID ring. Then every nonzero nonunit element a is divisible by an irreducible element.*

Proof. Let a_1 be nonzero nonunit element of R, and let $I = (a_1)$.

If I is a maximal ideal then a_1 is irreducible, so $a_1|a_1$, and we are done.

If I is not maximal then there exist an ideal $I_2 \in R$ such that $I_1 \subsetneq I_2 \subsetneq R$.

If I_2 ia an ideal of R then $I_2 = (a_2)$ with some $a_2 \in R$.

If I_2 is maximal then a_2 is irreducible $(a_1) \subsetneq (a_2) \Rightarrow a_2|a_1$.

If I_2 is not maximal then there exist an ideal $I_3 \in R$ such that $I_2 \subsetneq I_3 \subsetneq R$, and $a_3 \mid a_1$.

By the previous proposition this process must stop at some maximal ideal (a_m). Then $a_m \mid a_1$, and a_m is irreducible. □

Corollary 4. *An element in PID is prime if and only if it is irreducible.*

Proof. Let R be a PID, and p a prime element in R.

Suppose that $p = ab$ with $a, b \in R$. So $p|ab$. Since p is prime element, then $p|a$ or $p|b$.

If $p|a$ then $a = pm$, for $m \in R$. So $p = pmb$. Hence $p - pmb = 0$ and $p(1 - mb) = 0$, but p is nonzero, so $1 - mb = 0$, $mb = 1$ and b is a unit.

Similarly, we can show that a is unit if we start with $p|b$. Thus p is irreducible.

Conversely, suppose p is irreducible and $p|ab$.

Let (p) be the ideal R generated by p. By Proposition 7, (p) is maximal ideal because p is irreducible. Every maximal ideal is a prime ideal. Now, $p|ab$ implies that $ab \in (p)$. Since

(p) is prime, we conclude that $a \in (p)$ or $b \in (p)$. Thus $a|p$ or $p|b$. Therefore p is a prime element. □

Corollary 5. *Every nonzero, nonunit element in PID is product of irreducible elements.*

Proof. Suppose there exists a nonzero nonunit element $a \in D$, which is not a product of irreducible elements.

Then $a = b_1c_1$ where b_1, c_1 are nonunits.

Now either b_1 or c_1 cannot be written as a product of irreducibles, say $b_1 = d_1$ is one which cannot be. Then d_1 is reducible and $d_1 = b_2c_2$ where neither b_2 nor c_2 is a unit. Now either b_2 or c_2 cannot be written as a product of irreducibles, let us say that $b_2 = d_2$ is this element. Note that $(d_1) \subset (d_2)$.

Now the element d_2 is reducible $d_2 = b_3c_3$, where neither b_3 nor c_3 is a unit and either b_3 or c_3 (assume b_3) cannot be written as product of irreducibles. Set $d_3 = b_3$.

Now $(d_1) \subset (d_2) \subset (d_3)$, continuing in this way, we can construct a strictly ascending chain of ideals, this is not possible by Proposition 9 □

Theorem 3. *Every PID is a UFD.*

Proof. Let R be PID.

Let a be a nonzero, nonunit element of R.

By Corollary 5, a is a product of irreducible elements.

Suppose that $a = p_1p_2 \dots p_m = q_1q_2 \dots q_n$,where

each p_i and q_i are irreducible elements.

Now we show that p_i is associate of some q_i and $m = n$.

Suppose that $n > m$.

Now $p_1|a$, so p_1 divides one of the elements $q_1, q_2, \dots, q_n$

By Corollary 4, p_1 is a prime element, since it is irreducible.

Without loss of generality,

suppose that $p_1|q_1$. Hence $q_1 = p_1x_1$, with some $x_1 \in R$

But q_1 is irreducible, so x_1 must be unit.

Now $a = p_1p_2 \dots p_m = q_1q_2 \dots q_n$ implies that

$p_1p_2 \dots p_m = p_1x_1q_2 \dots q_m$. So

$p_2p_3 \dots p_m = x_1q_2 \dots q_n$.

By applying same argument to p_2 and q_2 we get

$p_3p_4 \dots p_m = x_1x_2q_3 \dots q_n, \dots$

By proceeding like this, at the end we get

$1 = x_1x_2 \dots x_mq_{m+1}q_{m+2} \dots q_n$.

$1 = (x_1x_2 \dots x_mq_{m+1} \dots q_{n-1})q_n$,

which implies q_n is a unit, a contradiction.

Thus $n \not> m$. Similarly we show that $m \not> n$, so $m = n$. Further p_i and q_i are associated.

□

Note : The converse is not true, i.e. every UFD is not a PID.

For example, consider the ring $\mathbb{Z}[x]$. The ideal $(2,x)$ is not principal: suppose $(2,x) = (a)$ for some a. Since this ideal contains the even integers, a must be some integer and in fact it must be 2. But (2) does not contain polynomials with odd coefficients, so $(2,x) \neq (2)$. However, $\mathbb{Z}[x]$ is UFD ring, which can be shown by Euclidean algorithm.

1.0.4 Integral basis

Definition 24 (An integral basis of O_K)**.**

A set of algebraic integers $\alpha_1, \alpha_2 ... \alpha_s \in K$ is called integral basis of O_K if every algebraic integer $\gamma \in K$ can be written uniquely in the form

$\gamma = b_1\alpha_1 + b_2\alpha_2 + \dots + b_s\alpha_s$,

where $b_1, b_2, ... b_s \in Z$.

We also refer to an integral basis of O_K as an integral basis of K. In a theorem below we prove that every algebraic number field has at least one integral basis.

Let K be an algebraic number field and $[K:\mathbb{Q}]=n$. Then $K=\mathbb{Q}(\theta)$ for some $\theta\in K$. Let $\sigma_1,\sigma_2,\ldots,\sigma_n$ be the embedding of K into $\mathbb{C}$, and $\sigma_i=\theta_i$ for $i=1,2\ldots,n$, $\theta=\theta_1,\theta_2,\ldots,\theta_n$ are the conjugates of θ.

Definition 25 (Discriminant of an element)**.**

Let $\alpha_1,\alpha_2,\ldots,\alpha_n$ be elements of K. Their discriminant is defined by

$$D(\alpha_1,\alpha_2,\ldots,\alpha_n)=\begin{vmatrix}\sigma_1(\alpha_1) & \sigma_1(\alpha_2) & \ldots & \sigma_1(\alpha_n)\\ \ldots & \ldots & \ldots & \ldots\\ \sigma_n(\alpha_1) & \sigma_n(\alpha_2) & \ldots & \sigma_n(\alpha_n)\end{vmatrix}^2.$$

It can be shown that $D(\alpha_1,\alpha_2,\ldots,\alpha_n)\neq 0$ if and only if $\alpha_1,\alpha_2\ldots,\alpha_n$ are linearly independent over $\mathbb{Q}$.

Theorem 4. *Every number field has an integral basis.*

Proof. We will follow the exposition from ([10] , Section 2.4). Let $[K:\mathbb{Q}]=n$ and suppose that $\alpha_1,\alpha_2\ldots,\alpha_n$ be a basis of K over $\mathbb{Q}$. By multiplying these elements by appropriate non zero integers, we can obtain another basis whose elements are algebraic integers.

Hence in what follows we assume that $\alpha_1\ldots,\alpha_n$ are algebraic integers. We shall prove that a basis with algebraic integers which has the smallest discriminant in fact an integral basis. Suppose that $\alpha_1,\ldots,\alpha_n$ has the smallest discriminant and for a contradiction, suppose it is not an integral basis of K. It means there exists an algebraic integer $\alpha\in K$ that is not linear combination of $\alpha_1\ldots,\alpha_n$ with integral coefficients, since $\alpha_1\ldots,\alpha_n$ is also basis over $\mathbb{Q}$, we have

$\alpha=c_1\alpha_1+\cdots+c_n\alpha_n$ with $c_1,\ldots,c_n\in\mathbb{Q}$ and at least one of c_i is not an integer. Without loss of generality, suppose that $c_1\notin\mathbb{Z}$. Then $c=a_1+r$ with some $a_1\in\mathbb{C}$ and $0<r<1$(r is the fractional part of c_1)

If we replace α_1 by $\alpha-a_1\alpha_1=r\alpha_1+\cdots+c_n\alpha_n$, we obtain another basis $\{\alpha-a_1\alpha_1,\alpha_2,\ldots,\alpha_n\}$ of K over $\mathbb{Q}$.

$$0 \neq D(\alpha - a_1\alpha_1, \alpha_2 \ldots, \alpha_n) = \begin{vmatrix} r\sigma_1(\alpha_1) & \sigma_1(\alpha_2) & \ldots & \sigma_1(\alpha_n) \\ \ldots & \ldots & \ldots & \ldots \\ r\sigma_n(\alpha_1) & \sigma_n(\alpha_2) & \ldots & \sigma_n(\alpha_n) \end{vmatrix}^2 .$$

The last matrix is obtained by subtracting c_i multiple of the i-th column for $i = 2 \ldots n$ from first column.

We obtain a contradiction because

$$D(\alpha - a\alpha_1, \ldots, \alpha_n) = r^2 D(\alpha_1, \ldots, \alpha_n) < D(\alpha_1, \ldots, \alpha_n).$$

Therefore, $\{\alpha_1, \ldots, \alpha_n\}$ is an integral basis of K.

□

Theorem 5. *Let K be a quadratic field $\mathbb{Q}(\sqrt{d})$. If $d \equiv 1 \mod 4$ then an integral basis of K is $\{1, \frac{1+\sqrt{d}}{2}\}$, otherwise it is $\{1, \sqrt{d}\}$.*

Proof. Let d be a squarefree integer. Let $\alpha \in \mathbb{Q}(\sqrt{d})$. Then α can be written as $\alpha = \frac{r+s\sqrt{d}}{t}$, where r, s, t are integers with $\gcd(r,s,t) = 1$ and $t \geq 1$, and if α is an algebraic integer then α satisfies

$$x^2 - \frac{2r}{t}x + \frac{r^2 - s^2 d}{t^2} = 0$$

with $\frac{-2r}{t}$, $\frac{r^2 - s^2 d}{t^2} \in \mathbb{Z}$

So $t|2r$ and $t^2|r^2 - s^2 d$ also $(r,s,t) = 1$.

We shall show that $(t,r) = 1$. Suppose $(t,r) = m$.

Then $m|r$ and $m^2|r^2 - s^2 d$, hence $m^2|s^2 d$.

Further, $m|r$ so $m^2|r^2$. Together with $m|r^2 - s^2 d$ this gives $m^2|s^2 d$.

But $(m,s) = 1$ because $(r,s,t) = 1$.

It follows that $m^2|d$, however d is a squarefree integer. Hence $m = 1$.

Now $t|2r$ implies $t|2$, thus either $t = 1$ or 2.

If $t = 1$ this will yield the element of $\mathbb{Z}(\sqrt{d})$.

The case $t = 2$ can only occur if $4|r^2 - ds^2$. Then d must be a quadratic residue modulo 4, and since d is squarefree we must have $d \equiv 1 \mod 4$, and also $r \equiv s \mod 2$. Thus $\alpha = \frac{r+s\sqrt{d}}{2}$ with $r \equiv s \mod 2$. This yield an integral basis

$$\left\{1, \frac{1+\sqrt{d}}{2}\right\}.$$

If $d \not\equiv 1 \mod 4$ we must have $t = 1$, so $\alpha = r + s\sqrt{d}$. Hence $\{1, \sqrt{d}\}$ is an integral basis in this case. □

Definition 26 (Free abelian group)**.**

An abelian group G is called free abelian group of rank n if there are n elements $\alpha_1, \alpha_2, \ldots, \alpha_n$ *in G such that* $G = \mathbb{Z}\alpha_1 + \mathbb{Z}\alpha_2 + \cdots + \mathbb{Z}\alpha_n$ *and every element p of G can be expressed by unique linear combination of the form* $p = m_1\alpha_1 + m_2\alpha_2 + \cdots + m_n\alpha_n$, $m_i \in \mathbb{Z}$ *for* $i = 1, 2, \ldots, n$.

Theorem 6. *Let* $[K : \mathbb{Q}] = n$ *and let J be a nonzero ideal of* O_K*. Then J has an integral basis of n elements.*

Proof. We have shown that O_K has integral basis. Let $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ be such a basis. Then $O_K = \mathbb{Z}\alpha_1 + \mathbb{Z}\alpha_2 + \cdots + \mathbb{Z}\alpha_n \equiv \mathbb{Z}^n$. We say that $\{O_K, +\}$ is free abelian group of rank n. It is known that every subgroup H of a free abelian group G is also free a abelian group. Further, if H has finite index in G than $\text{rank}(H) = \text{rank}(G)$. We have proved that $[O_K : K]$ is finite, therefore, J is free abelian group of n elements. So J has integral basis with n elements. □

Lemma 1. *Let J be a nonzero ideal of* O_K*. Suppose that* $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ *is an integral basis of* O_K*. Then for every* $i, 1 \leq i \leq n$*, there is a positive integer* m_i *such that* $m_i\alpha_i \in J$.

Proof. By Proposition [5], we know that $[O_K : J]$ is finite. Consider an infinite sequence of cosets

$$\alpha_i + J, 2\alpha_i + J, 3\alpha_i + J \ldots$$

Since $[O_K : J]$ is finite, there are positive integers r and s, $r < s$ such that $r\alpha_i + J = s\alpha_i + J$. Hence, $(s-r)\alpha_i \in J$ and proposition follows with $m_i = s - r$. □

Direct and constructive proof of the fact that every nonzero ideal J of O_K, for $[K : \mathbb{Q}] = n$ has an integral basis with n elements.

The following Lemma provide a constructive proof of the existence of the integral basis of a nonzero J of O_K.

Lemma 2. *Let J be a nonzero ideal of O_K. Then J has integral basis with n elements of the form*

$$\beta_1 = m_1\alpha_1 + c_{12}\alpha_2 + \cdots + c_{1n}\alpha_n,$$

$$\beta_2 = m_2\alpha_2 + c_{23}\alpha_3 + \cdots + c_{2n}\alpha_n,$$

$$\ldots\ldots\ldots\ldots$$

$$\beta_n = m_n\alpha_n,$$

where all c_{ij} are integers and $m_1, m_2, \ldots, m_n$ are positive integers.

Proof. We construct β_i successively, starting with β_1. Consider the set of elements of J of the form

$$S_1 = \{k_1\alpha_1 + k_2\alpha_2 + \cdots + k_n\alpha_n | k_1 > 0, k_i \in \mathbb{Z}, i = 1, 2, \ldots, n\}.$$

By Lemma [1], $S_1 \neq \phi$, because $m_1\alpha_1 \in S_1$.

Choose β_1 from S_1 to be any element whose coefficient k_1 of α_1 is the smallest. Let $\beta_1 = m_1\alpha_1 + c_{12}\alpha_2 + \cdots + c_{1n}\alpha_n$. Then m_1 divides all coefficients k_i of elements in S_1. This

is because J is closed to linear combinations with integer coefficients. Euclidean algorithm to find the greatest common divisor m_2. Then consider the set of element in J of the form

$$S_2 = \{k_2\alpha_2 + k_3\alpha_3 + \cdots + k_n\alpha_n | k_2 > 0, k_i \in \mathbb{Z}, i = 2,3,\ldots,n\}.$$

Again $S_2 \neq \phi$ because $m_2\alpha_2 \in S_2$. Let again m_2 be the smallest coefficient k_2 for all elements in S_2. We continue this process, until we determine all elements $\beta_1, \beta_2 \ldots, \beta_n$.

□

Claim : $\{\beta_1, \beta_2, \ldots, \beta_n\}$ is integral basis of J.

Proof. Let $\beta = b_1\alpha_1 + b_2\alpha_2 + \cdots + b_n\alpha_n \in J$ with $b_1, b_2, \ldots, b_n \in \mathbb{Z}$.

Then b_1 is multiple of m_1, say $b_1 = z_1 m$. Then $\beta - z_1\beta_1 \in S_1$, $\beta - z_1\beta_1 = b_2'\alpha_2 + \cdots + b_n'\alpha_n$.

Now, b_2' is multiple of m_2, say $b_2' = z_2 m_2$. Then $\beta - z_1\beta_1 - z_2\beta_2 \in S_2$, etc.

At the end we get,

$$\beta - z_1\beta_1 - z_2\beta_2 - \cdots - z_n\beta_n = 0.$$

Moreover, the set $\{\beta_1, \beta_2, \ldots, \beta_n\}$ is linearly independent over $\mathbb{Z}$. This is because $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ is linearly independent.

If $c_1\beta_1 + c_2\beta_2 + \cdots + c_n\beta_n = 0$ with $c_1, c_2, \ldots, c_n \in \mathbb{Z}$.

Then $c_1 = 0$ because α_1 occurs only in β_1,

then $c_2 = 0$ because α_2 occurs only in β_2, etc. □

Lemma 3. *We have $|O_K/J| = m_1 m_2 \ldots m_n$, where $m_1, m_2, \ldots, m_n$ are defined in the previous lemma.*

Proof. It suffices to show that the set of cosets of the form

$$r_1\alpha_1 + r_2\alpha_2 + \cdots + r_n\alpha_n + J, \tag{1.1}$$

where $0 \leq r_i \leq m_i$ for each $i = 1,2,\ldots,n$,

is a complete set or distinct cosets of J in O_K.

Completeness :

Let $z_1\alpha_1 + z_2\alpha_2 + \cdots + z_n\alpha_n + J$ be any coset of J in O_K

Elements, $\beta_1, \beta_2 \ldots, \beta_n$ are in J.

We have $z_i = k_i m_i + r_i$ with $0 \leq r_i < m$.

Then $z_1\alpha_1 + z_2\alpha_2 + \cdots + z_n\alpha_n + J = z_1\alpha_1 + z_2\alpha_2 + \cdots + z_n\alpha_n - k_1\beta_1 + J$

$r_1\alpha_1 + z_1'\alpha_1 + \cdots + z_n'\alpha_n + J$.

By successively interacting an appropriate multiple of β_i, $i = 1, 2, \ldots, n$, we get

$z_1\alpha_1 + z_2\alpha_2 + \cdots + z_n\alpha_n + J = r_1\alpha_1 + r_2\alpha_2 + \cdots + r_n\alpha_n + J$ with $0 \leq r_i < m_i$, $i = 1, 2, \ldots, n$

These show the completeness of the cosets in (1.1).

Now we show that all cosets in (1.1) are distinct.

Suppose that $r_1\alpha_1 + r_2\alpha_2 + \cdots + r_n\alpha_n + J = s_1\alpha_1 + s_2\alpha_2 + \cdots + s_n\alpha_n + J$ where all $0 \leq r_i <$ m_i, $0 \leq s_i < m_i$ for $i = 1, 2, \ldots, n$.

Then $(r_1 - s_1)\alpha_1 + (r_2 - s_2)\alpha_2 + \cdots + (r_n - s_n)\alpha_n \in J$.

This implies that $r_1 - s_1$ is multiple of m_1, but $|r_1 - s_1| < m_1$, hence $r_1 = s_1$.

The we show successively that $r_i = s_i$, by considering $i = 2$, then 3, etc. □

This leads us to the following

Theorem 7. *Let $J \neq \{0\}$ be an ideal of O_K.*
Then $N(J) = |O_K/J| = \sqrt{\frac{\triangle(\beta_1, \beta_2, \ldots, \beta_n)}{\triangle(\alpha_1, \alpha_2 \ldots, \alpha_n)}}$
where $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ is integral basis of O_K, and $\{\beta_1, \beta_2, \ldots, \beta_n\}$ is integral basis of J.

Proof. The particular form of $\beta_1, \beta_2, \ldots, \beta_n$ corresponds to

$$\begin{bmatrix} \beta_1 \\ \beta_2 \\ \ldots \\ \beta_n \end{bmatrix} = \begin{bmatrix} m_1 & c_{12} & c_{13} & \ldots & c_{1n} \\ 0 & m_2 & c_{23} & \ldots & c_{2n} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & \ldots & \ldots & 0 & m_n \end{bmatrix} \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \ldots \\ \alpha_n \end{bmatrix}. \tag{1.2}$$

We note that $|O_K/J| = m_1 \ldots m_k$ is the determinant of the matrix in (1.2). Let call this matrix B. □

Claim : If $\{\beta_1{}', \ldots, \beta_n{}'\}$ is any integral basis of J, and

$$\begin{bmatrix} \beta_1{}' \\ \beta_2{}' \\ \cdots \\ \beta' \end{bmatrix} = A \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \cdots \\ \alpha_n \end{bmatrix}$$

with integral matrix A, then $|detA| = |detB|$.

Proof. Since $\{\beta_1, \ldots, \beta_n\}$ and $\{\beta_1{}', \ldots, \beta_n{}'\}$ are both basis of J then there exist integer matrices M and M' such that

$$\begin{bmatrix} \beta_1{}' \\ \beta_2{}' \\ \cdots \\ \beta_n{}' \end{bmatrix} = M' \begin{bmatrix} \beta_1 \\ \beta_2 \\ \cdots \\ \beta_n \end{bmatrix} \text{ and } \begin{bmatrix} \beta_1 \\ \beta_2 \\ \cdots \\ \beta_n \end{bmatrix} = M \begin{bmatrix} \beta' \\ \beta' \\ \cdots \\ \beta' \end{bmatrix}$$

with integer matrices M and M' , we conclude that $MM' = I_n$, linear independent of $\{\beta_1, \ldots, \beta_n\}$.

Note that $det(MM') = det(I) = 1$. Since M and M' are integer matrices, this implies $detM = detM' = \pm 1$.

Now $\begin{bmatrix} \beta_1{}' \\ \beta_2{}' \\ \cdots \\ \beta_n{}' \end{bmatrix} = A \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \cdots \\ \alpha_n \end{bmatrix}$ implies that $M' \begin{bmatrix} \beta_1 \\ \beta_2 \\ \cdots \\ \beta_n \end{bmatrix} = A \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \cdots \\ \alpha_n \end{bmatrix} \Rightarrow M'B \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \cdots \\ \alpha_n \end{bmatrix} = A \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \cdots \\ \alpha_n \end{bmatrix}$

We have proved that if $\begin{bmatrix} \beta_1 \\ \beta_2 \\ \cdots \\ \beta_n \end{bmatrix} = C \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \cdots \\ \alpha_n \end{bmatrix}$, where C is an integer matrix then $|O_K/J| = |\det C|$

Now suppose that $\{\beta_1, \beta_2, \ldots, \beta_n\}$ is an integral basis of J and

$$\begin{bmatrix} \beta_1 \\ \beta_2 \\ \cdots \\ \beta_n \end{bmatrix} = \mathbb{C} \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \cdots \\ \alpha_n \end{bmatrix}, \text{ where } \mathbb{C} \text{ is an integer matrix.}$$

Then $\begin{bmatrix} \sigma_i(\beta_1) \\ \sigma_i(\beta_2) \\ \dots \\ \sigma_i(\beta_n) \end{bmatrix} = \mathbb{C} \begin{bmatrix} \sigma_i(\alpha_1) \\ \sigma_i(\alpha_2) \\ \dots \\ \sigma_i(\alpha_n) \end{bmatrix}$, for any embedding σ_i of K into $\mathbb{C}$.

We get $\begin{bmatrix} \sigma_1(\beta_1) & \sigma_2(\beta_1) & \dots & \sigma_n(\beta_1) \\ \sigma_1(\beta_2) & \sigma_2(\beta_2) & \dots & \sigma_n(\beta_2) \\ \dots & \dots & \dots & \dots \\ \sigma_1(\beta_n) & \sigma(\beta_n) & \dots & \sigma_n(\beta_n) \end{bmatrix} = \mathbb{C} \begin{bmatrix} \sigma_1(\alpha_1) & \sigma_2(\alpha_1) & \dots & \sigma_n(\alpha_1) \\ \sigma_1(\alpha_2) & \sigma_2(\alpha_2) & \dots & \sigma_n(\alpha_2) \\ \dots & \dots & \dots & \dots \\ \sigma_1(\alpha_n) & \sigma_2(\alpha_n) & \dots & \sigma_n(\alpha_n) \end{bmatrix}$

By taking determinant and squaring we get

$\triangle(\beta_1,\dots,\beta_n) = det(\mathbb{C})^2 \triangle(\alpha_1,\dots,\alpha_n)$

We proved above that $|det\mathbb{C}| = N(J)$. Hence

$N(J) = \sqrt{\frac{\triangle(\beta_1,\dots,\beta_n)}{\triangle(\alpha_1,\dots,\alpha_n)}}$. □

1.0.5 Examples of calculation of integral basis of ideals and their norms

Propostion 10. *If α is a generator of an ideal J then $N_{\frac{\mathbb{Q}(\alpha)}{\mathbb{Q}}}(\alpha)$ is in J.*

Proof. Suppose that α is an algebraic integer of degree m, and let

$x^m + a_{m-1}x^{m-1} + \dots + a_0 \in \mathbb{Z}[x]$ be its minimal polynomial. Then

$a_0 = (-1)^m N_{\frac{\mathbb{Q}(\alpha)}{\mathbb{Q}}}(\alpha) = -a_{m-1}\alpha^{m-1} - \dots - a_1\alpha \in J$. □

Corollary 6. *If $J = (\alpha_1, \alpha_2 \dots, \alpha_k)$ then $d = gcd(N_{\frac{\mathbb{Q}(\alpha_1)}{\mathbb{Q}}}, \dots, N_{\frac{\mathbb{Q}(\alpha_k)}{\mathbb{Q}}}) \in J$.*

Hence if $d = 1$ then $J = O_K$ and $N(J) = 1$. The integral basis of J in this case is just integral basis of O_K.

Example 1 Let O_K be ring of algebraic integers of $K = \mathbb{Q}(\sqrt{7})$ and let $J = (3+5\sqrt{7}, 5-9\sqrt{7})$.

We have $N_{\frac{K}{\mathbb{Q}}}(3+5\sqrt{7}) = 9 - 25 \times 7 = -166$,

and $N_{\frac{K}{\mathbb{Q}}}(5-9\sqrt{7}) = 25 - 81 \times 7 = -542$,

$\gcd(-166, -542) = 2(83, 271) = 2$,

hence $J = (3+5\sqrt{7}, 5-9\sqrt{7}) = (3+5\sqrt{7}, 5-9\sqrt{7}, 2)$

$= (1+\sqrt{7}, 1+\sqrt{7}, 2) = (1+\sqrt{7}, 2)$.

Since the integral basis of O_K is $(1, \sqrt{7})$, we can take $1+\sqrt{7}$ as the first element of an integral basis of J. Further

$J = \{(a+b\sqrt{7})(1+\sqrt{7}) + (c+d\sqrt{7})(2) | a,b,c,d \in \mathbb{Z}\}$

$= \{(a+7b+2c) + (a+b+2d)\sqrt{7}\}$.

We just need the second element, which is multiple of $\sqrt{7}$.

So $a+7b+2c = 0$ and $|a+b+2d|$ is minimum $\neq 0$.

Hence $a = -7b-2c$ and $a+b+2d = -7b-2c+b+2d = -6b-2c+2d = 2(-3b-c+d)$.

Since $\gcd(-3,-1,1) = 1$, we get $2\sqrt{7}$ as second element. Therefore the integral basis of J is $\{1+\sqrt{7}, 2\sqrt{7}\}$. Note also that $\{1+\sqrt{7}, 2\}$ is also such basis, because

$$\begin{bmatrix} 1+\sqrt{7} \\ 2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 2 & -1 \end{bmatrix} \begin{bmatrix} 1+\sqrt{7} \\ 2\sqrt{7} \end{bmatrix} \text{ and } \det \begin{bmatrix} 1 & 0 \\ 2 & -1 \end{bmatrix} = -1$$

$$\triangle(1+\sqrt{7}, 2) = \begin{bmatrix} 1+\sqrt{7} & 2 \\ 1-\sqrt{7} & 2 \end{bmatrix}^2 = 16 \times 7, \triangle(K) = 4 \times 7$$

So $N(J) = \sqrt{\frac{16\times 7}{4\times 7}} = 2$.

Example 2 Let $K = \mathbb{Q}(\sqrt{11})$ and $J = (3+7\sqrt{11}, 5+8\sqrt{11})$.

$N_{\frac{K}{\mathbb{Q}}}(3+7\sqrt{11}) = -530$, $N_{\frac{K}{\mathbb{Q}}}(5+8\sqrt{11}) = -679$

$(679, 530) = 1$. Hence $1 \in J$, so $J = O_K$.

The integral basis is $\{1, \sqrt{11}\}$ and $N(J) = 1$.

Example 3 Let $K = \mathbb{Q}(\sqrt{11})$ and $J = (3+\sqrt{11}, 6+9\sqrt{11})$

$N_{\frac{K}{\mathbb{Q}}}(3+7\sqrt{11}) = -530$ and $N_{\frac{K}{\mathbb{Q}}}(6+9\sqrt{11}) = -855$.

$J = \{(a+b\sqrt{11})(3+7\sqrt{11}) + (c+d\sqrt{11})(6+9\sqrt{11}) | a,b,c,d \in \mathbb{Z}\}$

$= \{(3a+77b+6c+99d) + (7a+3b+9c+6d)\sqrt{11} | a,b,c,d \in \mathbb{Z}\}$.

First element: $\gcd(3,77,6,99) = 1$. Take $b = 2, a = -51, c = d = 0$,

we get $1 + (7(-51)+3(2))\sqrt{11} = 1 - 351\sqrt{11}$.

Second element: $3a+77b+6c+99d = 0 \Rightarrow a = \frac{-77}{3}b - 2c - 33d$,

let $b = 3k, a = -77k - 2c - 33d$.

Now $7a+3b+9c+6d = 7(-77k-2c-33d)+9k+9c+6d$

$= 530k-5c-225d$, $\gcd(530,5,225) = 5$.

Hence the second element is $5\sqrt{11}$. The integral basis is $(1-351\sqrt{11}, 5\sqrt{11})$ or simpler one $(1-\sqrt{11}, 5\sqrt{11})$.

$$\triangle(1-\sqrt{11}, 5\sqrt{11}) = \begin{bmatrix} 1-\sqrt{11} & 5\sqrt{11} \\ 1+\sqrt{11} & -5\sqrt{11} \end{bmatrix}^2 = 100 \times 11.$$

$d(K) = 4 \times 11$, $N(J) = \sqrt{\frac{100\times 11}{4\times 11}} = 5$.

Example 4 Let $K = \mathbb{Q}(\sqrt{17})$, $J = (3-2\sqrt{17}, 3+9\sqrt{17})$.

The integral basis of O_K is $\{1, \frac{1+\sqrt{17}}{2}\}$ because $17 \equiv 1 \mod 4$.

We have $3-2\sqrt{17} = 5-4(\frac{1+\sqrt{17}}{2})$ and $3+9\sqrt{17} = -6+18(\frac{1+\sqrt{17}}{2})$.

Let $\zeta = \frac{1+\sqrt{17}}{2}$ then $\zeta^2 = \zeta+4$ and $J = (5-4\zeta, -6+18\zeta) = (5-4\zeta, -1+14\zeta)$

$= (1-14\zeta, 66\zeta)$.

So $J = \{(a+b\zeta)(1-14\zeta)+(c+d\zeta)(66\zeta) | a,b,c,d \in \mathbb{Z}\}$

$= \{(a-14b+264d)+(-14a-13b+66c++66d)\zeta | a,b,c,d \in \mathbb{Z}\}$,

then $a = 14b-264d$ and $-14a-13b+66c+66d = -14(14b-264d)-13b+66c+66d$

$= 209b+66c+3762d$.

Since $\gcd(209,66,3762) = 11$, we get 11ζ as the second element. we get basis of J as $\{1-14\zeta, 11\zeta\}$.

Another basis is $\{1-3\zeta, 11\zeta\}$ and $N(J) = 11$.

Chapter 2

Units

Definition 27 (Unit)**.**

If a is an element of the ring of integers O_F of an algebraic number field F, a is called a unit if there exist a nonzero element b in O_F such that $ab = 1$. O_F may contain an infinite number of units.

Theorem 8. *(Dirichlet's unit theorem) Let K be an algebraic number field of degree n. Let r be the number of real embedding of K into $\mathbb{C}$ and 2s the number of complex embedding of K. Then O_K contains $r+s-1$ units $\varepsilon_1, \varepsilon_2 ... \varepsilon_{r+s-1}$ such that each unit of O_K can be expressed uniquely in the form $\rho\varepsilon_1^{n_1} \dots \varepsilon_{r+s-1}^{n_{r+s-1}}$, where ρ is a root unity in O_K and $n_1, \dots n_{r+s-1}$ are integers.*

2.0.1 Units in quadratic number fields

Dirichlet's unit theorem allow us to describe all units in quadratic number fields $Q(\sqrt{d})$. All unis have the form $\varepsilon = \zeta^n \eta_1^{k_1} \eta_2^{k_2} \dots \eta_t^{k_t}$,
where ζ is a primitive root of unity in $Q(\sqrt{d})$.

When $d > 0$ i.e. $K = Q(\sqrt{d})$ is real quadratic field, $r = 2, s = 0, t = r+s-1 = 1$. We get

$\varepsilon = \zeta^n \eta^k = \pm\eta^k$,

because $\zeta = -1$ is only real primitive root of unity O_K. Thus, every real quadratic field has infinitely many units. The unit η is called the fundamental unit in O_K.

For example;

If $d = 3$,

$\Rightarrow r = 2, s = 0, t = r + s - 1 = 1$, then $\varepsilon = 2 + \sqrt{3}$.

If $d = -3$,

$\Rightarrow r = 0, s = 1, t = r + s - 1 = 0$, then $\varepsilon = \pm(\frac{-1+\sqrt{-3}}{2})^n$, where $n = 0, 1, 2$.

2.0.2 Fundamental unit

Theorem 9. *Let $d > 1$ be a squarefree integer, and $K = \mathbb{Q}(\sqrt{d})$.*

1. *Then in O_K exists the smallest unit η that is greater than 1, $\eta > 1$.*
2. *Every unit of O_K is the form $u = \pm\eta^n$ with $n \in \mathbb{Z}$.*

Proof. 1. If $d \not\equiv 1 \mod 4$ then $O_K = \{a + b\sqrt{d} | a, b \in \mathbb{Z}\}$.

If $d \equiv 1 \mod 4$ then $O_K = \{\frac{a+b\sqrt{d}}{2} : a \equiv b \mod 2, a, b \in \mathbb{Z}\}$.

We will restrict the proof to the case $d \not\equiv 1 \mod 4$. The proof for $d \equiv 1 \mod 4$ is almost the same and we will skip it.

Let U be the group of units of O_K, and define

$S = \{u \in U : u > 1\}$, $S_+ = \{u \in S : u = a + b\sqrt{d}, ab > 0, a, b \in \mathbb{Z}\}$, and

$S_- = \{u \in S : u = a + b\sqrt{d}, ab < 0, a, b \in \mathbb{Z}\}$.

Then $S = S_+ \cup S_-$.

We shall show that there are no units $\eta > 1$ in S_-.

For this suppose that $\eta > 1$ is in S_-. Then $\eta = a + b\sqrt{d}$ and $ab < 0$. Let $\widetilde{\eta} = a - b\sqrt{d}$.

Then $\eta\widetilde{\eta} = a^2 - b^2 d = \pm 1$, because it is a unit in $\mathbb{Z}$. Hence $\eta^{-1} = \pm\widetilde{\eta}$. Now, $a(-b) >$

0, so $\eta^{-1} = |a| + |b|\sqrt{d}$. However $\eta^{-1} < 1$. This leaves the only possibility that $\eta = |a|$, a contradiction.

We conclude that all units $\eta > 1$ are in S_+. Clearly S_+ has the smallest unit $\eta > 1$ because a and b are positive integers. Therefore, the smallest unit $\eta > 1$ exists in O_K.

2. Now we prove that unit in O_K is of the form $u = \pm\eta^n$ with $n \in \mathbb{Z}$.

   Consider first case $u > 1$. By the choice of η, we get $u \geq \eta > 1$. There exists a positive integer n, such that

$$\eta^{n+1} > u \geq \eta^n$$

   Hence, $\eta > \frac{u}{\eta^n} \geq 1$. By the choice of η, we conclude that $\frac{u}{\eta^n} = 1$, so $u = \eta^n$.

   Now consider the case $0 < u < 1$. Then $u^{-1} > 1$, and we get $u^{-1} = \eta^n$ with a positive integer n, so $u = \eta^{-n}$, $-n \in \mathbb{Z}$.

   Finally, the case $u < 0$, can be reduced to previous case by considering the unit $-u > 0$.

   Clearly, $-u = \eta^n$ with same $n \in \mathbb{Z}$.

   Therefore, every unit in O_K is of the form $\pm\eta^n$, $n \in \mathbb{Z}$.

   (Trivially, it is also true for $u = \pm 1$)

□

Definition 28 (Fundamental unit)**.**

Let $d > 1$ be a squrefree integer and $K = \mathbb{Q}(\sqrt{d})$. Then the unit $\eta > 1$ described in the Theorem 9 is called the fundamental unit of K.

The fundamental unit of $K = \mathbb{Q}(\sqrt{d})$ can be found by expansion of $\sqrt{d}$ into a continued fraction.

$$\sqrt{d} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \ldots}}}$$

a_i, $i = 1,2,3\ldots$ are defined by $a_0 = \lfloor\sqrt{d}\rfloor$, $x_0 = a_0 - \lfloor\sqrt{d}\rfloor = \{\sqrt{d}\}$ = fractional part of $\sqrt{d}$.

If a_n and x_n are already defined, then we define $a_{n+1} = [\frac{1}{x_n}]$ and $x_{n+1} = \{\frac{1}{x_n}\}$.

The continued fraction for any irrational number is infinite. For brevity we write

$\sqrt{d} = [a_0, a_1, a_2, a_3, \ldots]$, rather then writing compound fraction. In 1770, Lagrange proved that continued fractions for quadratic irrationalities are always periodic.

In case of $\sqrt{d}$ we get

$\sqrt{d} = [a_{0;}, a_1, a_2, \ldots, a_l, a_1, a_2, a_3, \ldots] = [a_{0;}, \overline{a_1, a_2, \ldots, a_l}]$

which means that $a_1, a_2, \ldots, a_l$ is the period of the expansion and l is its length.

The finite part $[a_0; a_1, a_2, \ldots, a_r]$ of infinite continued fraction can be simplified to a rational fraction

$\frac{n_r}{k_r} = [a_0; a_1, a_2, \ldots, a_r]$ where n_r, k_r are relatively prime integers called convergents of the fraction.

Example $\sqrt{8} = [2; \overline{1,1,4}]$

$\frac{h_1}{k_1} = 2 + \frac{1}{1} = 3$

$\frac{h_2}{k_2} = 2 + \frac{1}{1+\frac{1}{1}} = \frac{5}{2}$

$\frac{h_3}{k_3} = 2 + \frac{1}{1+\frac{1}{1+\frac{1}{4}}} = 2 + \frac{1}{1+\frac{4}{5}} = 2 + \frac{5}{9} = \frac{23}{9}$.

The formula for the fundamental unit η is determined by h_{l-1} and k_{l-1} where l is the length of the period of continued fraction for $\sqrt{d}$. The details are given in [1] as follows.

Propostion 11. *Let $d > 1$ be squarefree integer, $K = \mathbb{Q}(\sqrt{d})$, and suppose that $[a_0; \overline{a_1 a_2 \ldots a_l}]$ is the continued fraction expansion of $\sqrt{d}$. Denote the fundamental unit of K by η. Then*

1. *If $d \not\equiv 1 \mod 4$ or $d \equiv 1 \mod 8$ then $\eta = h_{l-1} + k_{l-1}\sqrt{d}$.*

2. *If $d \equiv 5 \mod 8$ and there are positive odd divisors A of h_{l-1} and B of k_{l-1}, such that $A < 2h_{l-1}^{\frac{1}{3}}$, and $B < 2(\frac{k_{l-1}}{d})^{\frac{1}{3}}$ and $A^3 + 3AB^2d = 8h_{l-1}$ and $3A^2B + B^3d = 8k_{l-1}$ then $\eta = \frac{A+B\sqrt{d}}{2}$ otherwise $\eta = h_{l-1} + k_{l-1}\sqrt{d}$.*

In either case $N(\eta) = (-1)^l$.

Determining the fundamental unit η of $O_{Q(\sqrt{d})}$ for positive squarefree integer d.

Step 1: $h_{-1}=1, k_{-1}=0,$

$P_0=0, Q_0=1, a_0=[\sqrt{d}], h_0=[\sqrt{d}], k_0=1.$

Step 2: Calculate P_n, Q_n, a_n, h_n, k_n for $n=1,23....$

$P_n=-P_{n-1}+a_{n-1}Q_{n-1}, n=1,2,3...,$

$Q_n=\frac{m-P_n^2}{Q_{n=1}}, n=1,2,3...,$

$a_n=[\frac{P_n+\sqrt{d}}{Q_n}], n=1,2,3...,$

$h_n=a_nh_{n-1}+h_{n-2}, n=1,2,3...,$

$k_n=a_nk_{n-1}+k_{n-2}, n=1,2,3...,$

Stop at N^{th} step when $P_N=P_1, Q_N=Q_1$.

Step 3: Put $l=N-1$

Step 4: If $d\equiv 2 \mod 4, d\equiv 3 \mod 4$, or $d\equiv 1 \mod 8$ then

$\eta=h_{l-1}+k_{l-1}\sqrt{d}, N(\eta)=(-1)^l$

Step 5: If $d\equiv 5 \mod 8$ find all positive odd divisor A of $h_{l=1}$ less than $2h_{l-1}^{1/3}$ and all positive odd divisor B of k_{l-1} less than $2(k_{l-1}/m)^{1/3}$. If for some pair (A,B) we have

$A^3+3AB^2d=8h_{l-1}, 3A^2B+B^3d=8k_{l-1}$

then

$\eta=\frac{A+B\sqrt{d}}{2}, N(\eta)=(-1)^l;$

otherwise we have

$\eta=h_{l-1}+k_{l-1}\sqrt{d}, N(\eta)=(-1)^l.$

For example,

Suppose $d=13$ so $13\equiv 5(mod 8)$ and $\sqrt{13}=3.6055$

$\alpha_0=\sqrt{13}.$

$\alpha_1=\frac{1}{\alpha_0-[\alpha_0]}=\frac{1}{\sqrt{13}-3}=\frac{1}{\sqrt{13}-3}\frac{\sqrt{13}+3}{\sqrt{13}+3}=\frac{3+\sqrt{13}}{4}$

$\alpha_2=\frac{1}{\alpha_1-[\alpha_1]}=\frac{1}{\frac{3+\sqrt{13}}{4}-1}=\frac{4}{\sqrt{13}-1}\frac{\sqrt{13}+1}{\sqrt{13}+1}=\frac{1+\sqrt{13}}{3}$

$\alpha_3=\frac{1}{\alpha_2-[\alpha_2]}=\frac{1}{\frac{1+\sqrt{13}}{3}-1}=\frac{3}{\sqrt{13}-2}\frac{\sqrt{13}+2}{\sqrt{13}+2}=\frac{2+\sqrt{13}}{3}$

$\alpha_4=\frac{1}{\alpha_3-[\alpha_3]}=\frac{1}{\frac{2+\sqrt{13}}{3}-1}=\frac{3}{\sqrt{13}-1}\frac{\sqrt{13}+1}{\sqrt{13}+1}=\frac{1+\sqrt{13}}{4}$

$\alpha_5 = \frac{1}{\alpha_4 - [\alpha_4]} = \frac{1}{\frac{1+\sqrt{13}}{4} - 1} = \frac{4}{\sqrt{13}-3}\frac{\sqrt{13}+3}{\sqrt{13}+3} = \frac{3+\sqrt{13}}{1}$

$\alpha_6 = \frac{1}{\alpha_5 - [\alpha_5]} = \frac{1}{3+\sqrt{13}-6} = \frac{1}{\sqrt{13}-3}\frac{\sqrt{13}+3}{\sqrt{13}+3} = \frac{3+\sqrt{13}}{4} = \alpha_1$

$a_0 = [\alpha_0] = 3, a_1 = [\alpha_1] = 1, a_2 = [\alpha_2] = 1, a_3 = [\alpha_3] = 1,$

$a_4 = [\alpha_4] = 1, a_5 = [\alpha_5] = 6, a_6 = [\alpha_6] = 1.$

$h_{-1} = 1, h_0 = 3, h_n = a_n h_{n-1} + h_{n-2}$

$h_1 = a_1 h_0 + h_{-1} = 4$

$h_2 = a_2 h_1 + h_0 = 7$

$h_3 = a_3 h_2 + h_1 = 11$

$h_4 = a_4 h_3 + h_2 = 18$

$h_5 = a_5 h_4 + h_3 = 119$

$h_6 = a_6 h_5 + h_4 = 137$

$k_{-1} = 1, k_0 = 1, k_n = a_n k_{n-1} + k_{n-2}$

$k_1 = a_1 k_0 + k_{-1} = 1$

$k_2 = a_2 k_1 + k_0 = 2$

$k_3 = a_3 k_2 + k_1 = 3$

$k_4 = a_4 k_3 + k_2 = 5$

$k_5 = a_5 k_4 + k_3 = 33$

$k_6 = a_6 k_5 + k_4 = 38$

$a_n = \frac{P_n + \sqrt{13}}{Q_n}$

$N = 6, l = N - 1 = 5, h_{l-1} = 18, k_{l-1} = 5,$

A is odd, $A | h_{l-1}, 1 \le A \le 2h_{l-1}^{1/3} \Rightarrow A | 18, 1 \le A \le 5.3, \Rightarrow A = 1$ or 3.

B is odd, $B | k_{l-1}, 1 \le B \le (\frac{k_{l-1}}{b})^{1/3}, \Rightarrow B | 5, 1 \le B \le 1.5, \Rightarrow B = 1.$

It means we have $(A,B) = (1,1)$ or $(3,1)$ and

only $(3,1)$ satisfies $A^3 + 39AB^2 = 144$ and $3A^2B + 13B^3 = 40$.

Hence the fundamental unit of $O_{Q(\sqrt{13})}$ is

$\eta = \frac{3+\sqrt{13}}{2}$ and $N(\eta) = (-1)^l = (-1)^5 = -1.$

Take one more example;

Suppose $d = 79, 79 \equiv 3(mod4)$

$\alpha_0 = \sqrt{79}$

$\alpha_1 = \frac{1}{\alpha_0 - [\alpha_0]} = \frac{1}{\sqrt{79}-8} = \frac{1}{\sqrt{79}-8}\frac{\sqrt{79}+8}{\sqrt{79}+8} = \frac{8+\sqrt{79}}{15}.$

$\alpha_2 = \frac{1}{\alpha_1 - [\alpha_1]} = \frac{1}{\frac{8+\sqrt{79}}{15}-1} = \frac{15}{\sqrt{79}-7}\frac{\sqrt{79}+7}{\sqrt{79}+7} = \frac{7+\sqrt{79}}{2}$

$\alpha_3 = \frac{1}{\alpha_2 - [\alpha_2]} = \frac{1}{\frac{7+\sqrt{79}}{2}-7} = \frac{2}{\sqrt{79}-7}\frac{\sqrt{79}+7}{\sqrt{79}+7} = \frac{7+\sqrt{79}}{15}$

$\alpha_4 = \frac{1}{\alpha_3 - [\alpha_3]} = \frac{1}{\frac{7+\sqrt{79}}{15}-1} = \frac{15}{\sqrt{79}-8}\frac{\sqrt{79}+8}{\sqrt{79}+8} = 8+\sqrt{79}$

$\alpha_5 = \frac{1}{\alpha_4 - [\alpha_4]} = \frac{1}{8+\sqrt{79}-16} = \frac{1}{\sqrt{79}-8}\frac{\sqrt{79}+8}{\sqrt{79}+8} = \frac{8+\sqrt{79}}{15} = \alpha_1.$

$a_0 = [\alpha_0] = 8, a_1 = [\alpha_1] = 8, a_2 = [\alpha_3] = 7$

$a_3 = [\alpha_3] = 1, a_4 = [\alpha_4] = 16, a_5 = [\alpha_5] = 1$

$h_{-1} = 1, h_0 = a_0 = [\alpha_0] = 8, h_n = a_n h_{n-1} + h_{n-2}, n = 1, 2, 3...$

$h_1 = a_1 h_0 + h_{-1} = 1 \times 8 + 1 = 9$

$h_2 = a_2 h_1 + h_0 = 7 \times 9 + 8 = 71$

$h_3 = a_3 h_2 + h_1 = 1 \times 71 + 9 = 80$

$h_4 = a_4 h_3 + h_2 = 16 \times 80 + 71 = 1351$

$h_5 = a_5 h_4 + h_3 = 1 \times 1351 + 80 = 1431$

$k_{-1} = 0, k_0 = 1, k_n = a_n k_{n-1} + k_{n-2}$

$k_1 = a_1 k_0 + k_{-1} = 1 \times 1 + 0 = 1$

$k_2 = a_2 k_1 + k_0 = 7 \times 1 + 1 = 8$

$k_3 = a_3 k_2 + k_1 = 1 \times 8 + 1 = 9$

$k_4 = a_4 k_3 + k_2 = 16 \times 9 + 8 = 152$

$k_5 = a_5 k_4 + k_3 = 1 \times 152 + 9 = 161$

n	P_n	Q_n	a_n	h_n	k_n
-1	–	–	–	1	0
0	0	1	8	8	1
1	8	15	1	9	1
2	7	2	7	71	8
3	7	15	1	80	9
4	8	1	16	1351	152
5	8	15	1	1431	161

$N = 5, l = N - 1 = 4$

$\eta = h_{l-1} + k_{l-1}\sqrt{79} = 80 + 9\sqrt{79}.$

$N(\eta) = (-1)^l = (-1)^4 = 1.$

2.0.3 Maple procedure

We were able to program this algorithm as a Maple procedure which we called *fundamentalunit*.

The procedure takes two parameters, d and *steps*. The parameter d correspond to the field $\mathbb{Q}(\sqrt{d})$, while *steps* is the maximum number of steps in the algorithm. It prevent the procedure to work indefinitely in a loop.

```
> fundamentalunit := proc(d, steps)
  local h, k, P, Q, a, n, l, T, A, B, SetA, SetB, m, H, K:
  h[-1] := 1 : k[-1] := 0 :
  P[0] := 0 : Q[0] := 1 : a[0] := floor(sqrt(d)) :
  h[0] := floor(sqrt(d)) : k[0] := 1 : T := 0 :
      printf("\n  Pn    Qn    an    hn    kn \n") :
      for n from 1 to steps do
      P[n] := -P[n-1] + a[n-1]*Q[n-1]:
      Q[n] := floor((d-P[n]^2)/Q[n-1]) :
      a[n] := floor((P[n]+sqrt(d))/Q[n]) :
      h[n] := a[n]*h[n-1] + h[n-2] :
      k[n] := a[n]*k[n-1] + k[n-2] :
      printf(" %5d   %5d   %8d   %8d    %8d   %8d \n", n, P[n], Q[n], a[n], h[n], k[n]) :
      if n > 1 and P[n] = P[1] and Q[n] = Q[1] then break end if: end do:
   l := n-1 :
  if d mod 4 = 2 or d mod 4 = 3 or d mod 8 = 1 then
  printf("\n    unit = a +b sqrt(d),  where  a and b are ") : printf("%8d %8d", h[l-1], k[l-1]) :
  print("N(unit)=", (-1)^l) :
   end if:
   if d mod 8 = 5 then
  SetA := { } : H := h[l-1] :
          for m from 1 by 2 to H do

          if H mod m = 0 and evalf(m) < evalf(2*H^(1/3)) then SetA := SetA∪{m} end if: end do:
  SetB := { } : K := k[l-1] :
          for m from 1 by 2 to K do

          if K mod m = 0 and evalf(m) < evalf(2*(K/d)^(1/3)) then SetB := SetB∪{m} end if:end do: :

             for A in SetA do
              for B in SetB do
                  if A^3 + 3*A*B^2*d = 8*H and 3*A^2*B + B^3*d = 8*K then
                  printf("\n  unit =(a+b sqrt(d))/2  where a and b are ") : printf("%8d  %8d", A, B) :
                  print("N(unit)=", (-1)^l) :
                   T := 1 :
                  end if: end do end do:
  if T = 0 then printf("\n  unit = a +b sqrt(d)   where a and b are ") : printf(" %8d %8d", H, K)
                                  print("N(unit)=", (-1)^l) : end if:
  end if
  end proc:
```

```
> fundamentalunit(10, 20)

   Pn      Qn      an      hn     kn
    1       3       1       6      19       6
    2       3       1       6     117      37

    unit = a +b sqrt(d),  where  a and b are     3      1
                                 "N(unit)=", -1

> fundamentalunit(142, 20)

   Pn      Qn      an      hn     kn
    1      11      21       1     12       1
    2      10       2      10    131      11
    3      10      21       1    143      12
    4      11       1      22   3277     275
    5      11      21       1   3420     287

    unit = a +b sqrt(d),  where  a and b are   143     12
                                 "N(unit)=", 1

> fundamentalunit(7, 20)

   Pn      Qn      an      hn     kn
    1       2       3       1      3       1
    2       1       2       1      5       2
    3       1       3       1      8       3
    4       2       1       4     37      14
    5       2       3       1     45      17

    unit = a +b sqrt(d),  where  a and b are     8      3
                                 "N(unit)=", 1

>

> fundamentalunit(82, 20)

   Pn      Qn      an      hn     kn
    1       9       1      18     163      18
    2       9       1      18    2943     325

    unit = a +b sqrt(d),  where  a and b are     9      1
                                 "N(unit)=", -1
```

```
> fundamentalunit(97, 20)

   Pn      Qn      an      hn     kn
    1       9      16       1     10          1
    2       7       3       5     59          6
    3       8      11       1     69          7
    4       3       8       1    128         13
    5       5       9       1    197         20
    6       4       9       1    325         33
    7       5       8       1    522         53
    8       3      11       1    847         86
    9       8       3       5   4757        483
   10       7      16       1   5604        569
   11       9       1      18 105629      10725
   12       9      16       1 111233      11294

    unit = a +b sqrt(d),  where  a and b are     5604      569
                                 "N(unit)=", -1
```

Chapter 3

Ideal Class Group

3.0.1 Legendre symbol

Legendre symbol is a multiplicative function with values $-1, 0, 1$.

Definition 29 (Legendre symbol)**.**
Let p be an odd prime. An integer a is a quadratic residue modulo p if it is congruent to a perfect square modulo p and a quadratic nonresidue modulo p otherwise. The Legendre symbol is a function of a and p defined as

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{if } a \text{ is a square modulo } p \text{ and } a \not\equiv 0 \mod p \\ 1, & \text{if } a \text{ is a nonquadratic modulo } p \\ 0, & \text{if } a \equiv 0 \mod p \end{cases}$$

Properties of the Legendre symbol; Suppose p and q are odd primes, and a and b are integers not divisible by p, the following properties for Legendre symbol hold;

1. If $a \equiv b \mod p$, then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$

2. $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$

3. $\left(\frac{a^2}{p}\right) = 1$

4. $\left(\frac{1}{p}\right) = 1$

5. $\left(\frac{-1}{p}\right) = \begin{cases} 1, & \text{if } p \equiv 1 \mod 4 \\ -1, & \text{if } p \equiv -1 \mod 4 \end{cases}$

6. $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

7. $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$

The last property is known as the famous quadratic reciprocity law.

For example, consider $\left(\frac{385}{97}\right) = \left(\frac{5\times7\times11}{97}\right) = \left(\frac{5}{97}\right)\left(\frac{7}{97}\right)\left(\frac{11}{97}\right)$

now consider $\left(\frac{5}{97}\right) = (-1)^{\frac{5-1}{2}\frac{97-1}{2}}\left(\frac{97}{5}\right)$

$= \left(\frac{2}{5}\right) = -1.$

consider $\left(\frac{7}{97}\right) = (-1)^{\frac{7-1}{2}\frac{97-1}{2}}\left(\frac{97}{7}\right)$

$= \left(\frac{97}{7}\right) = \left(\frac{6}{7}\right)$

$= \left(\frac{2}{7}\right)\left(\frac{3}{7}\right) = 1(-1) = -1$

consider $\left(\frac{11}{97}\right)$

$= (-1)^{\frac{11-1}{2}\frac{97-1}{2}}\left(\frac{97}{11}\right) = \left(\frac{97}{11}\right)$

$= \left(\frac{9}{11}\right) = \left(\frac{3^2}{11}\right) = 1.$

Thus, $\left(\frac{385}{97}\right) = \left(\frac{5}{97}\right)\left(\frac{7}{97}\right)\left(\frac{11}{97}\right)$

$= (-1)(-1)1 = 1.$

Take one more example,

consider $\left(\frac{105}{109}\right) = \left(\frac{3\times5\times7}{109}\right)$

$\left(\frac{3}{109}\right)\left(\frac{5}{109}\right)\left(\frac{7}{109}\right)$,

now consider $\left(\frac{3}{109}\right) = (-1)^{\frac{3-1}{2}\frac{109-1}{2}}\left(\frac{109}{3}\right)$

$\left(\frac{109}{3}\right) = \left(\frac{1}{3}\right) = 1.$

consider $\left(\frac{5}{109}\right) = (-1)^{\frac{5-1}{2}\frac{109-1}{2}} \left(\frac{109}{5}\right)$

$= \left(\frac{109}{5}\right) = \left(\frac{4}{5}\right) = \left(\frac{2^2}{5}\right) = 1.$

consider $\left(\frac{7}{109}\right) = (-1)^{\frac{7-1}{2}\frac{109-1}{2}} \left(\frac{109}{7}\right)$

$= \left(\frac{109}{7}\right) = \left(\frac{4}{7}\right) = \left(\frac{2^2}{7}\right) = 1$

Thus, $\left(\frac{105}{109}\right) = \left(\frac{3}{105}\right)\left(\frac{5}{109}\right)\left(\frac{7}{105}\right) = 1.1.1 = 1$

Kronecker symbol

Let n be a nonzero integer with prime factorization

$n = u.p_1^{e_1} \dots p_k^{e_k}$,

where u is unit, and p_i are primes. Let a be an integer. The Kronecker symbol $\left(\frac{a}{n}\right)$ is defined by

$$\left(\frac{a}{n}\right) = \left(\frac{a}{u}\right) \prod_{i=1}^{k} \left(\frac{a}{p_i}\right)^{e_i}$$

.

For odd p_i, the number $\left(\frac{a}{p_i}\right)$ is simply the usual Legendre symbol. The case when $p_i = 2$, we define $\left(\frac{a}{2}\right)$ by

$$\left(\frac{a}{2}\right) = \begin{cases} 0, & \text{if } a \text{ is even} \\ 1, & \text{if } a \equiv \pm 1 \mod 8 \\ -1, & \text{if } a \equiv \pm 3 \mod 8. \end{cases}$$

The quantity $\left(\frac{a}{u}\right) = 1$ when $u = 1$. When $u = -1$, we define it by

$$\left(\frac{a}{-1}\right) = \begin{cases} -1, & \text{if } a < 0 \\ 1, & \text{if } a \geq 0 \end{cases}$$

Finally, when $u = 0$,

$$\left(\frac{a}{0}\right) = \begin{cases} 1, & \text{if } a = \pm 1 \\ 0, & \text{otherwise.} \end{cases}$$

Basic properties of the Kronecker symbol:

1. $\left(\frac{a}{u}\right) = \pm 1$, if $\gcd(a,n) = 1$, otherwise $\left(\frac{a}{u}\right) = 0$.

2. $\left(\frac{ab}{u}\right) = \left(\frac{a}{u}\right)\left(\frac{b}{u}\right)$ unless $u = -1$, one of a,b is zero and other one is negative.

3. $\left(\frac{a}{uv}\right) = \left(\frac{a}{u}\right)\left(\frac{a}{v}\right)$ unless $a = -1$, one of u, v is zero and other one has odd part congruent to 3 $\mod 4$

4. For $u > 0$, we have $\left(\frac{a}{u}\right) = \left(\frac{b}{u}\right)$ whenever $a \equiv b \mod u$ If a,b have same sign, the same also holds for $u < 0$.

5. For $a \not\equiv 3 \mod 4$, $a \neq 0$, we have $\left(\frac{a}{u}\right) = \left(\frac{a}{v}\right)$ whenever

$$u \equiv v \mod \begin{cases} 4|a|, & a \equiv 2 \mod 4 \\ |a|, & \text{otherwise.} \end{cases}$$

Examples of Kronecker symbol

Consider $\left(\frac{2}{21}\right) = \left(\frac{2}{3\times 7}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{7}\right) = (-1)1 = -1$

One more example,

consider $\left(\frac{4}{15}\right) = \left(\frac{4}{3\times 5}\right) = \left(\frac{4}{3}\right)\left(\frac{4}{5}\right) = 1.1 = 1$

3.0.2 Ideal class group

Definition 30 (Discriminant of algebraic number field)**.**

Let K be an algebraic number field of degree n. Let $\{\eta_1, \eta_2, \ldots, \eta_n\}$ *be an integral basis for K. Then* $D(\eta_1, \eta_2, \ldots, \eta_n)$ *is called the discriminant of K and denoted by* $d(K)$*.*

Theorem 10. *Let K be a quadratic number field. Let d be the unique squarefree integer such that* $K = \mathbb{Q}(\sqrt{d})$*. Then discriminant* $d(K)$ *of K is given by*

$$d(K) = \begin{cases} 4d, & \text{if } d \not\equiv 1 \mod 4 \\ d, & \text{if } d \equiv 1 \mod 4 \end{cases}$$

Proof. If $d \not\equiv 1 \mod 4$, an integral basis for K is $\{1, \sqrt{d}\}$ so that

$$d(K) = \begin{bmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{bmatrix}^2 = (-2\sqrt{d})^2 = 4d.$$

If $d \equiv 1 \mod 4$, an integral basis for K is $\{1, \frac{1+\sqrt{d}}{2}\}$ so that

$$d(K) = \begin{bmatrix} 1 & \frac{1+\sqrt{d}}{2} \\ 1 & \frac{1-\sqrt{d}}{2} \end{bmatrix}^2 = (-\sqrt{d})^2 = d.$$

□

Definition 31 (Ideal class group)**.**

In number theory, the ideal class group of algebraic number field K is the quotient group $\frac{J_K}{P_K}$*, where* J_K *is the group of fractional ideals of the ring of integers K, and* P_K *is the subgroup of principal ideals in* J_K*,* $\frac{J_K}{P_K}$ *is denoted by* $H(K)$*.*

If all ideals of the ring of integers of an algebraic number field are principal, then the ring is a principal ideal domain. In such case the ideal class group is trivial.
For example, $\mathbb{Z}$, $\mathbb{Z}[i]$, $\mathbb{Z}[\omega]$, where i is forth root of unity and ω is cube root of unity, are all principal domains so the corresponding fields have ideal class number one, they have trivial class group.
We are going to prove that the ideal class group for any number field K is finite. For this we will need following theorems from geometry of numbers.

Theorem 11 ([1], Theorem 12.5.1)**.** *Let $K = \mathbb{Q}(\theta)$ be an algebraic number field of degree $n = r + 2s$, where θ has r real conjugates and s pairs of nonreal complex conjugates. Let A be an integral or fractional ideal of O_K. Then there exists an element $\alpha(\neq 0) \in A$, such that*

$$|N(\alpha)| \leq \left(\frac{2}{\pi}\right)^s N(A)\sqrt{|d(K)|}$$

.

For the proof we need following lemmas.

Lemma 4. *Let $S(\mathbb{R}^n)$ be a centrally symmetric convex body of volume $V(S) \geq 2^n$. Then S contains a lattice point $\neq 0$.*

The following theorem about linear forms is formulated in the format that is suitable for Theorem 11.

Lemma 5. ***(Minkowski's linear forms theorem)*** *Let $A = [a_{jk}]_{n\times n}$ be a complex matrix, such that $a_{jk} \in \mathbb{R}$ for $j = 1,2,\ldots,r$ and $k = 1,2,\ldots,n$ and*

$$a_{j+sk} = \bar{a}_{jk} \quad for \quad j = r+1,\ldots,r+s; k = 1,2,\ldots,n.$$

Suppose that positive real numbers $\delta_1, \ldots, \delta_n$ satisfy the following conditions

$$\delta_1 \ldots \delta_n \geq \left(\frac{2}{\pi}\right)^s |\det(a_{jk})|$$

and

$$\delta_j = \delta_{j+s}, j = r+1, \ldots, r+s.$$

Then the system of linear in equations

$$\left|\sum_{k=1}^{n} a_{jk} y_k\right| \leq \delta_j, j = 1, 2, \ldots, n$$

has a solution in integers $y_1, \ldots, y_n$, not all zero.

Theorem 12. *Let $K = \mathbb{Q}(\theta)$ be an algebraic number field of degree $n = r+2s$, where θ has r real conjugates and s pairs of nonreal complex conjugates. Let A be an integral or fractional ideal of O_K. Then there exists an element $\alpha(\neq 0) \in A$ such that*

$$|N(\alpha)| \leq \left(\frac{2}{\pi}\right)^s N(A)\sqrt{|d(K)|}$$

.

Proof. Let $\theta_1, \theta_2, \ldots, \theta_n$ be the conjugates of θ. We reorder $\theta_1, \theta_2, \ldots, \theta_n$ in such a way that $\theta_1, \theta_2, \ldots, \theta_r \in \mathbb{R}$ and $\theta_{r+1}, \theta_{r+2}, \ldots, \theta_n \in \mathbb{C} \setminus \mathbb{R}$. The complex conjugate of θ is also an algebraic conjugate of θ,we can further order $\theta_{r+1}, \theta_{r+2}, \ldots, \theta_n$ so that $\theta_{r+s+1} = \bar{\theta}_{r+1}, \ldots, \theta_n = \theta_{r+2s} = \bar{\theta_{r+s}}$ where $r+2s = n$. Let $\sigma_1, \ldots \sigma_n$ be n monomorphism $\sigma_i : K \to \mathbb{C}$ is chosen so that $\sigma_i(\theta) = \theta_i$. Hence $\alpha_{r+s+1} = \bar{\sigma}_{r+t}(t = 1, \ldots, s)$.

Let $\{\alpha_1, \ldots, \alpha_n\}$ be a basis for A. We define linear forms $L_j(\mathbf{x})(j = 1, 2, \ldots, n)$, where $\mathbf{x} = (x_1, \ldots, x_n)$, by

$$L_j(\mathbf{x}) = \sum_{k=1}^{n} \sigma_j(\alpha_k) x_k$$

.

These forms satisfy **Minkowski's linear forms theorem** with $a_{jk} = \sigma_j(\alpha_k)(j,k = 1,2,\ldots,n)$. Moreover,

$$|\det(a_{jk})| = |\det(\sigma_j(\alpha_k))| = \sqrt{|D(A)|} = N(A)\sqrt{|d(K)|} \neq 0$$

.

Let

$$\delta_j = \left(\frac{2}{\pi}\right)^{s/n} N(A)^{1/n} |\det(K)|^{1/2n}, j = 1,2,\ldots,n$$

Then

$$\delta_1 \ldots \delta_n = \left(\frac{2}{\pi}\right)^{s} N(A)|d(K)|^{1/2} = \left(\frac{2}{\pi}\right)^{s} |\det(a_{jk})|$$

so, by **Minkowski's linear forms theorem**, there exist integers $y_1, y_2, \ldots, y_n$, not all zero, such that

$$|L_j(\mathbf{y})| \leq \left(\frac{2}{\pi}\right) N(A)^{1/n} |d(K)|^{1/2n}, j = 1,2,\ldots,n$$

.

Choose $m \in 1,2,\ldots,n$ such that $\sigma_m = I$, where I denotes the identity monomorphism from K to K. Set

$$\alpha = L_m(\mathbf{y}) = \sum_{k=1}^{n} \sigma_m(\alpha_k) y_k = \sum_{k=1}^{n} \alpha_k y_k$$

,

so that $\alpha \in A$ and $\alpha \neq 0$. The conjugates of α are

$$\sigma_j(\alpha) = \sum_{k=1}^{n} \sigma_j(\alpha_k) y_k = L_j(\underline{\mathbf{y}}), j = 1,2\ldots,n$$

.

Hence

$$|\sigma_j(\alpha)| \leq \left(\frac{2}{\pi}\right)^{s/n} N(A)^{1/n} |d(K)^{1/2n}, j = 1,2,\ldots,n$$

and so

$$|N(\alpha)| = |\sigma_1(\alpha)\ldots\sigma_n(\alpha)| \leq \left(\frac{2}{\pi}\right)^{s} N(A)|d(K)|^{1/2}$$

as asserted.

□

3.0.3 Analytic Dirichlet class number formula

Introduction

Initially, the class number formula was found by Dirichlet for binary quadratic forms. He used for this the concepts of multiplicative characters and L-functions which he developed in order to prove the celebrated theorem of the infinitude of prime numbers in arithmetic progression $a+bn$, $n \in \mathbb{N}$, where a and b are relatively prime.

Then, as the algebraic number theory began to develop, the one-to-one correspondence between classes of binary quadratic forms and classes of ideals in rings of algebraic integers in quadratic fields was evident, so that the class number formula for binary quadratic forms turned up to be valid also for class number of ideals. These concepts are discussed below. Our expansion is based on [1] and [2].

Binary quadratic forms

Binary quadratic form is a polynomial in two variables

$f(x,y) = ax^2 + bxy + cy^2$ with $a,b,c \in \mathbb{Z}$ and $x,y \in \mathbb{Z}$

Mathematicians were interested in representations of integers by such forms and questions like:

1. Which integers can be represented by a given form?
2. Which forms can represent a given integer?
3. If an integer n can be represented by a given form $f(x,y)$, then how many solutions in integers x, y are there?

The theory of quadratic forms was developed already by Gauss around 1830.

Equivalent forms

A form $f(x,y)$ can be written in matrix form as

$$f(x,y) = ax^2 + bxy + cy^2 = \begin{bmatrix} x & y \end{bmatrix} A \begin{bmatrix} x \\ y \end{bmatrix}, \text{ where } A = \begin{bmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{bmatrix}$$

corresponds to $f(x,y)$

Let M be 2×2 matrix with integer entries and determinant equal to 1. Such matrices form a group under multiplication and denoted by $SL_2(\mathbb{Z})$.

Definition 32 (Equivalent form)**.**

Two forms $f(x,y) = ax^2 + bxy + cy^2$ and $f'(x',y') = a'x'^2 + b'x'y' + c'y'^2$ are called equivalent if the matrix corresponding to f' is $M^T AM$ where A is a matrix corresponding to f, and

$M \in SL_2(\mathbb{Z})$.

Thus $f(x,y) = \begin{bmatrix} x & y \end{bmatrix} A \begin{bmatrix} x \\ y \end{bmatrix}$

$$f'(x',y') = \left(M \begin{bmatrix} x' \\ y' \end{bmatrix} \right)^T AM \begin{bmatrix} x' \\ y' \end{bmatrix}$$

Clearly f and f' represent exactly the same integers, because if $\begin{bmatrix} x' \\ y' \end{bmatrix} = M \begin{bmatrix} x \\ y \end{bmatrix}$

then $\begin{bmatrix} x \\ y \end{bmatrix} = M^{-1} \begin{bmatrix} x' \\ y' \end{bmatrix}$ with $M^{-1} \in SL_2(\mathbb{Z})$.

If $M = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}$ then the matrix operation correspond simply to the change variable

$x' = \alpha x + \beta y$, $y' = \gamma x + \delta y$.

Definition 33 (Discriminant)**.**

The number $d = b^2 - 4ac$ is called the discriminant of the form $f(x,y) = ax^2 + bxy + cy^2$.

For $d = 0$ the equation $n = f(x,y)$ is trivial and we will not consider this case.

Further we notice that the equivalence relation preserves the discriminant. In fact we have

$d = b^2 - 4ac = -4\det(A) = -4 \begin{bmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{bmatrix}$ for $f(x,y)$,

and for $f'(x',y')$, $d' = -4\det(M^T AM) = d$, because $M \in SL_2(\mathbb{Z})$.

The theory of binary quadratic form splits into two cases, one for $d < 0$ and another for $d > 0$ which differ greatly in nature.

Case d<0

Then $\det(A) = \frac{-1}{4} d > 0$. If $a > 0$ then we must also have $c > 0$ and the symmetric matrix A is called positive definite. This is because in such as

$\begin{bmatrix} x & y \end{bmatrix} A \begin{bmatrix} x \\ y \end{bmatrix} > 0$ for any nonzero $\begin{bmatrix} x \\ y \end{bmatrix} \in \mathbb{R}$

It follows that in such case $f(x,y) > 0$ whenever $(x,y) \neq (0,0)$.

If $d < 0$ and $a < 0$ then $c < 0$ and $f(x,y) < 0$ for any $(x,y) \neq (0,0)$ then we say corresponding matrix is negative definite. However, in this case $-f(x,y)$ is positive definite. Hence there is no need to study such forms separately, so we assume that $a > 0$ (and consequently $c > 0$) in the case $d < 0$.

As we have realized, the set of integers that can be represented by a given form f is exactly the same for any form in the equivalence class containing f.

In order to count the classes of equivalent forms it is convenient to find in such class a special representative, called canonical form, or reduced form.

Definition 34 (Reduced positive form)**.**

A positive definite form is called reduced if $|b| \leq a \leq c$.

Proposition.(This is Theorem 2.4 in [3]) Every positive definite form with discriminant $d < 0$ is equivalent to a unique reduced form.

Note: The uniqueness requires a convention that the coefficient of xy is nonnegative in reduced forms of two exceptions $ax^2 + bxy + ay^2$ and $ax^2 + axy + cy^2$ which otherwise would have two reduced forms.

With fixed discriminant $d < 0$, it follows easily from this theorem that number of classes for $d < 0$ is finite.

Case d>0

In this case $f(x,y)$ can represent positive and negative integers, and we call such form indefinite. The definition of reduced form must be modified.

Definition 35 (Reduced indefinite form)**.**

Suppose that $f(x,y) = ax^2 + bxy + cy^2$ *has discriminant* $d > 0$. *Then we say* f *is reduced if* $0 < b < \sqrt{d}$ *and* $\sqrt{d} - b < 2|a| < \sqrt{d} + b$

With this definition we have

Proposition(Proposition 3.3 of [3]). Any indefinite form is equivalent to a reduced form of the same discriminant.

However, in a given class of equivalent forms there can be several reduced forms. Their number is finite, but unlike in the case of $d < 0$, the reduced form in a given class is not unique.

The total number of reduced forms is finite, and the reduced forms in a given equivalence class form finite cycles. Hence, the number of distinct classes $h(d)$ is still finite for d>0.

One-to-one correspondence between classes of equivalent forms and classes of ideals

Recall that the class group of ideals of an algebraic number field K is given by $H(K) = \frac{I_K}{P_K}$, where I_K is the multiplicative group of fractional ideals in O_K and P_K is its subgroup of principal ideals. Also recall two principal ideals (a) and (b) are identical if and only if $b = ua$, where u is unit in O_K. We shall now focus on quadratic number fields $K = \mathbb{Q}(\sqrt{d})$, where d is squarefree integer, $d \neq 1$.

Narrow class group

Definition 36 (Positive principal ideals)**.**
Let K be a quadratic field, and I be a principal (fractional) ideal of O_K. If $I = (a)$ and $N(a) > 0$, we say that I is positive.

Propostion 12. *The positive principal (fractional) ideals of O_K form a group, denoted by P_K^+*

Proof. Since $(a)(b) = (ab)$, the theorem follows by multiplication of norm, $N(ab) = N(a)N(b)$. □

Note:

1. If $d < 0$ then $P_K^+ = P$. This is because all norms of nonzero algebraic integers are positive

$$N(a + b\sqrt{d}) = a^2 + |d|b^2.$$

2. Suppose that there is a unit u in O_K with negative norm, $N(u) = -1$. Then the ideals (a) and (ua) are the same. If $N(a)$ is negative then $N(ua) = N(u)N(a)$ is positive. Hence we can choose a generator of any principal ideal with a positive norm. Hence again $P_K^+ = P_K$.

3. If $d > 0$ and there is no unit u in O_K with $N(u) = -1$ then P_K^+ is a proper subgroup of P_K of index 2. That is $[P_K : P_K^+] = 2$. Obviously in this case there exists an element $b \in O_K$ with $N(b) < 0$, and the ideal (b) has no generator with positive norm. It is easy to see that in this case there are exactly two cosets of P_K^+ in P_K, namely P_K^+ and bP_K^+, as shown in the following Lemma.

Definition 37 (Narrow ideal class group)**.**

The narrow ideal class group of a quadratic field K is defined by

$$H(K)^+ = \frac{I_K}{P_K^+}.$$

Lemma 6. *P_K^+ is a subgroup of P_K, of index 2, that is, $[P_K : P_K^+] = 2$.*

Proof. Let $n \in O_K$ be element of negative norm. Obviously such element exists, for example $n = a + b\sqrt{d}$, (or $n = a + b\frac{1+\sqrt{d}}{2}$). Then $N(n) = a^2 - b^2 d$ or $(N(n) = a^2 + ab - b^2\frac{d-1}{4})$. So,if b is sufficiently large then $N(n) < 0$. Clearly P_K^+ is subgroup of P_K, and it has two cosets: P_K^+ and $(n)P_K^+$. This is because if an ideal $J \in P_K \setminus P_K^+$, then $J = (a)$ and $N(a) < 0$, but $J = (n)\left(\frac{a}{n}\right)$, and $\left(\frac{a}{n}\right) \in P_K^+$, so $J \in (n)P_K^+$. So, there are exactly two cosets,P_K^+ and $(n)P_K^+$. □

In [3] on page 101 Theorem 6.19 we find the following statement.

Propostion 13. *If $d > 1$ is a squarefree integer, $K = \mathbb{Q}(\sqrt{d})$ and O_K has no unit with norm -1 then the ideals class group $H(K)$ is isomorphic to the subgroup of squares of the narrow class group $H^+(K)$.*

This statement is actually false. In an article in *MathOverflow* [9] the example of $K = \mathbb{Q}(\sqrt{210})$ was considered. In fact $H(K) \cong \mathbb{Z}_2 \bigoplus \mathbb{Z}_2$ where $H(K)^+ \cong \mathbb{Z}_2 \bigoplus \mathbb{Z}_2 \bigoplus \mathbb{Z}_2$. However, the squares of $H(K)^+$ form a trivial group, so $h(K)$ would be equal to 1, while in fact, $h(K) = 4$. We will calculate these values in Chapter 4.

Propostion 14. *$h(K)^+ = 2h(K)$ for any quadratic field $K = \mathbb{Q}(\sqrt{d})$ if $d > 1$ when there is no unit in O_K with norm -1.*

Proof. **First proof**

We have $P(K)$ and $P^+(K)$ are normal subgroup of $I(K)$, $P^+(K) \subseteq P(K)$. So by the third isomorphism theorem for groups we get

$$\frac{\frac{I(K)}{P^+(K)}}{\frac{P(K)}{P^+(K)}} \cong \frac{I(K)}{P(K)}$$

Hence,

$$\frac{H^+(K)}{P(K)/P^+(K)} \cong H(K)$$

Since $[P_K : P_K^+] = 2$ as shown in Lemma 6, we get $h^+(K) = 2h(K)$

Second direct proof

Let $S = \{J_1P^+(K), \ldots, J_mP^+(K)\}$ be the set of all distinct cosets of $P^+(K)$ in $H^+(K)$. Now, $(n)J_1P^+(K)$ must be equal to one of the cosets in S, and it is not equal to $J_1P^+(K)$. Without loss of generality suppose $(n)J_1P^+(K) = J_2P^+(K)$. We can continue this process, now starting with $J_3P^+(K)$, etc...until we obtain a new set of m cosets of the form

$$S = \{J_1P^+(K), (n)J_1P^+(K), \ldots, J_kP^+(K), (n)J_kP^+(K)\}.$$

We conclude that $m = 2k$. By Lemma 6, $J_rP(K) = JP^+(K) \bigcup (n)JP^+(K)$ for $r = 1, 2, \ldots, k$.

Hence $H(K) = \frac{I(K)}{P(K)}$ has k cosets of $P(K)$ where $H^+(K)$ has $m = 2k$ cosets of $P^+(K)$ and the theorem follows. □

The following theorem relates the number of equivalence classes of binary quadratic forms and the ideal class number of an algebraic number field.

Theorem 13. *The narrow ideal class number $h^+(K)$ of an algebraic number field K is equal to the number of equivalence classes of binary quadratic forms $ax^2 + bxy + cy^2$ of discriminant $d(K)$.*

Thus $h(K)$, the class number of K is equal to the number of equivalence classes of binary quadratic forms if O_K has a unit with norm -1 and $h(K)$ equals to the half of the number of equivalence classes of binary quadratic forms otherwise.

Note : In fact, much more than Theorem13 is known:

The equivalence classes of binary quadratic forms form a group under "composition" of forms, which however we are not studying in this thesis. This group is isomorphic to $H^+(K)$.

In what follows we are exploring D.B. Zagier exposition [11]. The isomorphic is in the following way:

Let J be an ideal (integral or fractional) in O_K and let (α, β) be its integral basis then we associate with the following quadratic form

$$J \longmapsto \frac{(x\alpha + y\beta)(x\alpha' + y\beta')}{N(J)},$$

see [11] page(93).

Here α' and β' are algebraic associate of α and β respectively. The quadratic form at the right hand side has integral coefficient, because since $\alpha \in J$ we have $N(J)|(\alpha)$ and similarly $N(J)|(\beta)$.

Example : In Example 1 of Section 1.0.5 we have $J = (3 + 5\sqrt{7}, 5 - 9\sqrt{7})$ we have found integral basis $(1 + \sqrt{7}, 2)$ and $N(J) = 2$. Hence the corresponding form is $\frac{(x(1+\sqrt{7})+y2)(x(1-\sqrt{7})+y2)}{2} = -3x^2 + 2xy + 2y^2$ and its discriminant $D = 2^2 - 4 \times -3 \times 2 = 28$.

which is same as the field discriminant of $K = \mathbb{Q}(\sqrt{7})$ i.e. $d(K) = 4 \times 7 = 28$.

On the other hand, given a binary quadratic form $ax^2 + bxy + cy^2$ with discriminant $D < 0$, we map it into a fractional ideal in the way

$$ax^2 + bxy + cy^2 \longrightarrow J = \mathbb{Z} + \mathbb{Z}\frac{b + \sqrt{D}}{2a} \tag{3.1}$$

or, alternatively, we can map the form into an integral ideal

$$ax^2 + bxy + cy^2 \longrightarrow J' = \mathbb{Z}(2a) + \mathbb{Z}(b + \sqrt{D}) \tag{3.2}$$

Clearly, $J' = (2a)J$, so both ideals are equivalent modulo principal ideals in 3.1 and 3.2. It is easy to check that the sets on right hand sides are ideals indeed and their integral basis are $(1, \frac{b+\sqrt{D}}{2a})$ and $(2a, b + \sqrt{D})$ respectively.

Propostion 15. *$J = \mathbb{Z}(2a) + \mathbb{Z}(b + \sqrt{D})$, where $D = b^2 - 4ac$, and $a, b, c \in \mathbb{Z}$ is in fact an ideal of O_K, $K = \mathbb{Q}(\sqrt{D})$.*

Proof. Case-1 $D \equiv 0 \mod 4$.

In this case $O_K = \{x + y\sqrt{D} : x, y \in \mathbb{Z}\}$. It is clear that J is a group under addition. It remains to show that it is closed under multiplication by elements from O_K. Let $n \in J$, then $n = z_1(2a) + z_2(b + \sqrt{D})$ with integers z_1 and z_2. The product $(x + y\sqrt{D})n$ can be rearranged as $(x + y\sqrt{D})n = z_1 x(2a) + z_1 2ay(b + \sqrt{D}) - z_1 by(2a) + z_2 x(b + \sqrt{D}) + z_2 yb(b + \sqrt{D}) - z_2 2yc(2a)$, where each component belongs to J. This complete the first part of case-1.

Case-2 $D \equiv 1 \mod 4$.

Now $O_K = \{\frac{x+y\sqrt{D}}{2} : x, y \in \mathbb{Z}, x \equiv y \mod 4\}$. If x and y are even we can reduce to case-1, so suppose that x and y are odd. Notice also that $D \equiv 1 \mod 4$ implies that also b is odd. Now we can rearrange $\frac{x+y\sqrt{D}}{2}$ as follows

$$\left(\frac{x + y\sqrt{D}}{2}\right) = \frac{x + y\sqrt{D}}{2}\{z_1(2a) + z_2(b + \sqrt{D})\} =$$

$$z_1 a(x-by)+z_1 ay(b+\sqrt{D})+z_2\left(\frac{x+by}{2}\right)(b+\sqrt{D})+z_2 yc(2a)$$

. This is an element of J because $x-by$ is even and $\frac{x+by}{2}\in\mathbb{Z}$, since x, y and b are odd □

Note: The construction of J provides also its integral basis, which is $\{2a, b+\sqrt{D}\}$. This allows to calculate the norm of J. We use this fact in calculation of the norms of ideals in examples for Carlitz's theorem.

In case of $d>0$ we modify maps 3.1 and 3.2 by multiplying the integral basis of the ideals by any element with negative norm. For this purpose $\lambda=\sqrt{d}$ will do, as $N(\lambda)=-\sqrt{d}\times\sqrt{d}=-d$. So, we have the map $ax^2+bxy+cy^2\longrightarrow \mathbf{Z}\lambda+\mathbb{Z}\frac{b+\sqrt{D}}{2}\lambda$.

L. Dirichlet derived the formulas for ideal class number of quadratic number fields by counting the number of equivalence classes of quadratic forms. However, in the next section, the calculations of using these formulas are presented.

Here, we just show two easy algorithms for counting the equivalence classes for binary quadratic form directly.

In the case if $d<0$ the form $ax^2+bxy+cy^2$ is reduced if $|b|\le a\le c$,

hence $|b|\le[\sqrt{\frac{D}{3}}]$ see [3],Proposition [2.1]

This restriction together with $D=b^2-4ac$, $D=d(K)$, $K=\mathbb{Q}(\sqrt{d})$, and the elimination of ambiguous forms leads to the following procedure

```
> ReducedPositiveForms := proc(Δ)
      #description "Numbers and lists unequivalent reduced positive forms with discriminant
      Delta"
  local a, b, c, n :
  n := 0 :
  for b from floor( -sqrt(Δ/3) ) to floor( sqrt(Δ/3) ) do
  for a from max( |b|, 1 ) to floor( sqrt((b^2+Δ)/4) ) do
  if (b^2+Δ) mod 4 = 0 and (b^2+Δ)/4 mod a = 0 then
  c := (b^2+Δ)/(4·a) :
    if not( (b < 0 and c = a) or (b < 0 and b = -a) ) then
      n := n + 1 :
      print(n, "form", a, b, c) end if: end if:
  end do: end do:
  end proc:
```

In this case the number of classes of quadratic forms equal $h(K)$.

In the case of $d > 0$ we have

```
> IndefiniteReducedForms := proc(Δ)
  local S, a, b, c :
  S := sqrt(Δ) :
  for b from 1 to floor(S) do
  for a from ceil( (S-b)/2 ) to floor( (S+b)/2 ) do
  c := ( (b^2-Δ)/(4·a) ) :
  if floor(c) = c then print(a, b, c) : print(-a, b, -c) end if:
  end do end do:
  end proc:
```

This procedure just lists the reduced forms of discriminant $D = d(K)$. Then we still need to group the reduced forms in chains as shown in the proof of Proposition 3.6 in [3].

We form pairs of equivalent reduced forms according to the rule $(a,b,c) \sim (c,b',c')$ in which

$c < 0$ and a and c' are positive.

For $d = 210$, $D = 4 \times 210$. We can use cycles to determine the structure of the group $H(K)$.

In order to do this we take any form each cycle and convert it into an ideal of O_K, for $K = \mathbb{Q}(\sqrt{d})$, according to the formula $(a,b,c) \sim \mathbb{Z}(2a) + \mathbb{Z}(b + \sqrt{D})$.

Our procedure gives the following results:

Finally, d=210, so d(k)= 840 This is the example showing that a proposotion is false

```
> IndefiniteReducedForms(840)
```

5, 20, −22
−5, 20, 22
10, 20, −11
−10, 20, 11
11, 20, −10
−11, 20, 10
22, 20, −5
−22, 20, 5
3, 24, −22
−3, 24, 22
6, 24, −11
−6, 24, 11
11, 24, −6
−11, 24, 6
22, 24, −3
−22, 24, 3
1, 28, −14
−1, 28, 14
2, 28, −7
−2, 28, 7
7, 28, −2
−7, 28, 2
14, 28, −1
−14, 28, 1

Cycles

1. (5,20,-22) ~ (-22,24,3)~ (3,24,-22)~(-22,20,5)
2. (-5,20,22)~(22,224,-3)~(-3,24,22)~(22,20,-5)
3. (-6,24,11)~(11,20,-10)~(-10,20,11)~ (11,24,-6)
4. (6,24,-11)~(-11,20,10)~(10,20,-11)~(-11,24,6)
5. (1,28,-14)~(-14,28,1)
6. (-1,28,14), (14,(28,-1)
7. (2,28,-7)~(-7,28,2)
8. (-2,28,7)~(7,28,-2)

Fundamental unit $\eta=29-2\sqrt{210}$, $N(\eta)=1$

Hence $h^+(K)=8$, $h(K)=4$.

The first two cycles give the same ideal $J_1=(10,20+\sqrt{4\times 210})$, the cycles [3] and [4] give $J_2=(6,24+\sqrt{4\times 210})$, [5] and [6] give $J_3=(1,28+\sqrt{4\times 210})$ and [7] and [8] give $J_4=(2,28+\sqrt{4\times 210})$.

Since these ideals are representatives of classes modulo principal ideals, we can find equivalent ideals by dividing both generators by an integer. Thus

$J_1=(10,20+2\sqrt{210})=(5,2\sqrt{210})=(2)(5,\sqrt{210})$

$J_1^2=(4)(25,5\sqrt{210},210)=(4)(5,5\sqrt{210})$ because $\gcd(25,210)=5$ further $J_1^2\sim(1,2\sqrt{210})=O_K=1$.

$J_2=(12,24+2\sqrt{210})=(12,2\sqrt{210})\sim(2)(6,\sqrt{210})$, so

$J_2^2=(4)(36,6\sqrt{210},210)=(24)(1,\sqrt{210})$ so $J_2^2=1$.

$J_3=(2,28+2\sqrt{210})=(2,2\sqrt{210})=(2)(1,\sqrt{210})=(2)$, so $J_3=1$.

$J_4=(4,28+2\sqrt{210})=(4,2\sqrt{210})\sim(2)(2,\sqrt{210})$, $J_4^2=(4)(4,2\sqrt{210},210)=(4)(2,2\sqrt{210})=(8)(1,\sqrt{210})=(8)$ so $J_4^2=1$.

We used the fact that if an ideal contains a unit is equal to O_K. Therefore $H(K)$ contains four elements; neutral and three of order 2. Hence $H(K)\equiv\mathbb{Z}_2\bigoplus\mathbb{Z}_2$, which is the four Klein group. As for $H^+(K)$, it contains eight elements, so it can be isomorphic to one of $\mathbb{Z}_8$, $\mathbb{Z}_4\bigoplus\mathbb{Z}_2$, or $\mathbb{Z}_2\bigoplus\mathbb{Z}_2\bigoplus\mathbb{Z}_2$. The squares of these groups form $\mathbb{Z}_4$, $\mathbb{Z}_2$, or one element group respectively, so non of them is $\mathbb{Z}_2\bigoplus\mathbb{Z}_2$, showing that Proposition 13 is false.

The existence of a unit of norm -1 in O_K

For $d \not\equiv 1 \mod 4$, we have

$N(a+b\sqrt{d}) = a^2 - db^2$

Hence there is no unit norm -1 if and only if the negative Pell equation $x^2 - dy^2 = -1$ has no solution. It is known that the negative Pell equation has solution if and only if period of continuous fraction expression of $\sqrt{d}$ is odd.

For $d \equiv 1 \mod 4$, the corresponding equation is $x^2 - dy^2 = -4$. By considering parity of x and y, we conclude that this equation is equivalent to $x^2 - dy^2 = -1$ for $d \not\equiv 1 \mod 4$, so it is more general.

When O_K for $\mathbb{Q}(\sqrt{d})$ does not have a unit of norm -1?

This is important question because for such real $d > 0$, $h(K) \neq h^+(K)$

In general solution to this question is unknown, however there are partial results. For example in [1] we find the following facts;

Theorem 14. *Let d be a prime with $d \equiv 1 \mod 4$. Then the fundamental unit of $O_{\mathbb{Q}(\sqrt{d})}$ has norm -1.*

Theorem 15. *Let d be a prime with $d \equiv 5 \mod 8$. Then the fundamental unit of $O_{\mathbb{Q}(\sqrt{2d})}$ has norm -1.*

Theorem 16. *Let p and q be distinct primes such that*

$$p \equiv q \equiv 1 \mod 4, \left(\frac{p}{q}\right) = -1$$

Then the fundamental unit of $O_{\mathbb{Q}(\sqrt{pq})}$ has norm -1.

3.0.4 Dirichlet's class number formula

Dirichlet's class number formula was conjectured by Jacobi in 1832 and was proved by Dirichlet in 1839. There are many expositions of this proof with variety of shortcuts and simplifications. Here, we follow the detailed proof from [11]. The proof is quite sophisticated and we describe only major steps. The main idea is to relate the class number $h(D)$ of classes of quadratic forms of discriminant D with the number of solution of the equation

$$ax^2 + bxy + cy^2 = n, \tag{3.3}$$

where n is positive integer. We consider only primitive forms (a,b,c) that is with $\gcd(a,b,c) = 1$ and for which D is *a fundamental discriminant* that is either $D \equiv 0 \mod 4$ or $D \equiv 1 \mod 4$. This corresponds to field discriminants $K = \mathbb{Q}(\sqrt{d})$ where d is squarefree integer and field discriminant $d(K) = D = 4d$ if $d \not\equiv 1 \mod 4$ or $D = d$ if $d \equiv 1 \mod 4$.

For a form $f(x,y) = ax^2 + bxy + cy^2$ denoted also by (a,b,c), let $R(n)$ denote the number of solutions in integers (x,y) of the equation 3.3 counted in a way described below.

For a given form $f(x,y) = ax^2 + bxy + cy^2$ with matrix $A = \begin{bmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{bmatrix}$ there are substitution $x = \alpha x' + \beta y'$, $y = \gamma x' + \delta y'$, where $M = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \in SL_2(\mathbb{Z})$ and $M^T A M = A$. So after this substitution we have $f(x,y) = f(x',y')$ where $\begin{bmatrix} x \\ y \end{bmatrix} = M \begin{bmatrix} x' \\ y' \end{bmatrix}$.

We say that such substitution is an automorphism of f, and consider the solutions (x,y) and (x',y') of (3.3) as equivalent. The number R(n) denotes the number of non equivalent solutions. The set of such matrices M forms a group.

$U_f = \{M \in SL_2(\mathbb{Z}) : M^T A M \sim A\}$.

There exist a bijection between the set of solutions of the Pell's equation $t^2 - u^2 D = 4$ and U_f, given by

$$(t,u) \longrightarrow \begin{bmatrix} \frac{t-bu}{2} & -cu \\ au & \frac{t+bu}{2} \end{bmatrix} \in U_f.$$

The equation $t^2 - u^2 D = 4$ gives all the units with norm 1 of O_K for $K = \mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{D})$. The units are of the form $\frac{t \pm u\sqrt{D}}{2}$ for both cases $D \equiv 0 \mod 4$ and $D \equiv 1 \mod 4$.

Thus for $D < 0$ the number of automorphisms $w = |U_f|$ is finite,and U_f is cyclic. We have

$$w(D) = \begin{cases} 6 & if \quad D = -3 \\ 4 & if \quad D = -4 \\ 2 & if \quad D < -4 \end{cases}$$

which is exactly the number of units in O_K for the corresponding field K.

For $D > 0$, U_f is infinite and $U_f \equiv \mathbb{Z} \bigoplus \mathbb{Z}_2$. In either case $R(f,n)$ is finite. Further, let

$$R(n) = \sum_{i=1}^{h(D)} R(f_i, n) \tag{3.4}$$

where $f_1, f_2, \ldots, f_{h(D)}$ denote any representative of non equivalent binary primitive integer with discriminant D.

The next major step is showing that $R(n) = \sum_{m|n} \chi_D(n)$, where $\chi_D = \left(\frac{D}{m}\right)$ is the Kronecker symbol. While it is difficult to obtain a closed form for $R(n)$, it is possible to do so for the average of $R(n)$ when n changes 1 to infinity. We have

$$\lim_{N \to \infty} \frac{1}{N} \sum_{n=1}^{N} R(n) = L(1, \chi_D) \tag{3.5}$$

where $L(s,\chi_D)$ denotes, the so called $L-$series with character χ_D, $L(s,\chi_D) = \sum_{n=1}^{\infty} \frac{\chi_D(n)}{n^s}$. In 3.5 we just take $s = 1$.

Further, for any primitive form of with discriminant D and for $n > 0$ we have

$$\lim_{N \to \infty} \sum_{n=1}^{N} \frac{R(f,n)}{N} = \begin{cases} \frac{2\pi}{w\sqrt{|D|}} & for \quad D < 0 \\ \frac{\log \varepsilon_0}{\sqrt{D}} & for \quad D > 0 \end{cases} \tag{3.6}$$

where $\varepsilon_0 = \frac{t_0+u_0\sqrt{D}}{2}$ is the smallest positive solution of 3.5 with $t_0 > 0$ and $u_0 > 0$.

All solutions of 3.5 are of the form $\pm\varepsilon_0^n$ where $n \in \mathbb{Z}$. Clearly $\varepsilon_0 = \eta$, the fundamental unit.

By connecting (3.5) and (3.6) we get

$$h(D) = \begin{cases} \frac{w\sqrt{|D|}}{2\pi} L(1,\chi_D) & for \quad D < 0 \\ \frac{\sqrt{D}}{\log \varepsilon_0} L(1,\chi_D) & for \quad D > 0 \end{cases} \tag{3.7}$$

It remains to calculate $L(1,\chi_D)$. We are following [11] and we will only outline the main steps.

By using Gauss sum

$$G = \sum_{n=1}^{N} \chi(n) e^{2\pi i n/N}$$

we get

$$\chi(k) = \frac{1}{\bar{G}} \sum_{n=1}^{N} \bar{\chi}(n) e^{-2\pi i n k/N}.$$

This leads to

$$L(1,\chi) = \sum_{k=1}^{\infty} \frac{\chi(k)}{k} = \frac{1}{\bar{G}} \sum_{k=1}^{\infty} \frac{1}{k} \sum_{n=1}^{N-1} \bar{\chi}(n) e^{2\pi i n k/N}.$$

It foils to

$$L(1,\chi) = \frac{1}{\bar{G}} \sum_{n=1}^{N-1} \bar{\chi}(n) \left(-\log(2\sin\frac{\pi n}{N}) - i(\frac{\pi}{2} - \frac{\pi n}{N}) \right).$$

In our case χ_D is a real character (Kronecker symbol) and this formula simplifies to

$$L(1,\chi) = -\frac{\pi}{|D|^{3/2}} \sum_{n=1}^{|D|-1} n\chi(n) \quad \text{for} \quad D < 0,$$

and

$$L(1,\chi) = -\frac{1}{\sqrt{D}} \sum_{n=1}^{|D|-1} \chi(n) \log\sin\frac{\pi n}{D} \quad \text{for} \quad D > 0.$$

For $D > 0$ in the book ([2]) a simplification is given. Namely for $D > 0$, we have $\chi_D = \chi_D(D-n)$, and also $\sin(\pi - \frac{n\pi}{D}) = \sin(\frac{n\pi}{D})$. By combining this remark and equations

(3.4), (3.5), and (3.7) , the formula for $h(D)$ in case $D > 0$ becomes

$$h(D) = -\frac{2}{\log \varepsilon_0} \sum_{n=1}^{n<\frac{D}{2}} \chi_0(n) \log \sin(\frac{n\pi}{D})$$

If the fundamental unit of O_K has norm 1, then $h(K) = \frac{1}{2}h(D)$ where $h(D)$ is the number of classes of quadratic forms and $h(K)$ is the class number of $K(\sqrt{D})$. We get

$$h(K) = -\frac{1}{\log \eta} \sum_{n=1}^{n<\frac{D}{2}} \chi_0(n) \log \sin(\frac{n\pi}{D}) \tag{3.8}$$

with $\eta = \varepsilon_0$. If O_K has fundamental unit η with $N(\eta) = -1$ then $\varepsilon_0 = \eta^2$ so $\log \varepsilon_0 = 2 \log \eta$, again we get same formula 3.8.

The case $D < 0$ is somewhat easier and equations (3.4), (3.5), and (3.7) give

$$h(D) = h(K) = \frac{-w(D)}{2|D|} \sum_{n=1}^{|D|-1} n \left(\frac{D}{n}\right).$$

This formula is the same for the number of classes of quadratic forms and classes of ideals.

3.0.5 Numerical examples of the Dirichlet class number formula

Dirichlet's class number formula for $d < 0$

Let K be quadratic field of discriminant d. Then

$h(K) = \frac{-w(D)}{2|d|} \sum_{n=1}^{|d|-1} n \left(\frac{D}{n}\right)$.

Here $w(D)$ denotes the number of roots of unity in $O_{Q(\sqrt{d})}$ so that

$$w(D) = \begin{cases} 6 & \text{if D = -3} \\ 4 & \text{if D = -4} \\ 2 & \text{if D < -4} \end{cases}$$

Note: Here d corresponds to D used in the case of quadratic forms.

Example 1 Suppose $d = -3 \Rightarrow$ discriminant $D = -3$ and $w(D) = 6$

Put these values in the formula,

$h(K) = \frac{-6}{2.|-3|}\sum_{n=1}^{2} n\left(\frac{-3}{n}\right)$

$= -1\{1\left(\frac{-3}{1}\right) + 2\left(\frac{-3}{2}\right)\}$

$= -1\{1(1) + 2(-1)\}$

$= -1\{-1\} = 1$

Calculation of $h(K)$ by counting the number of classes of quadratic forms by procedure "positive"

```
d=-3,  so d(K) =-3
> ReducedPositiveForms(3)
                                   1, "form", 1, 1, 1
So h(K)=1
```

Example 2

Suppose $d = -10 \Rightarrow$ discriminant $D = -40$ and $w(D) = 2$.

$h(K) = \frac{-2}{2.|-40|}\sum_{n=1}^{39} n\left(\frac{-40}{n}\right)$

$= \frac{-1}{40}\{1\left(\frac{-40}{1}\right) + 2\left(\frac{-40}{2}\right) + \cdots + 39\left(\frac{-40}{39}\right)\}$

$= \frac{-1}{40}\{1\left(\frac{-40}{1}\right) + 3\left(\frac{-40}{3}\right) + 7\left(\frac{-40}{7}\right) + 9\left(\frac{-40}{9}\right) + 11\left(\frac{-40}{11}\right)$

$+ 13\left(\frac{-40}{13}\right) + 17\left(\frac{-40}{17}\right) + 19\left(\frac{-40}{19}\right) + 21\left(\frac{-40}{21}\right) + 23\left(\frac{-40}{23}\right)$

$+ 27\left(\frac{-40}{27}\right) + 29\left(\frac{-40}{29}\right) + 31\left(\frac{-40}{31}\right) + 33\left(\frac{-40}{33}\right) + 37\left(\frac{-40}{37}\right) + 39\left(\frac{-40}{39}\right)\}$

$= \frac{-1}{40}\{1(1) + 3(-1) + 7(1) + 9(1) + 11(1) + 13(1) + 17(-1) + 19(1) + 21(1)$

$+ 23(1) + 27(-1) + 29(-1) + 31(-1) + 33(-1) + 37(1) + 37(1) + 39(-1)\}$

$= \frac{-1}{40}\{120 - 200\}$

$= 2$

Calculation of $h(K)$ by counting the number of classes of quadratic forms by procedure "positive"

```
d=-10,  d(K)=-40
> ReducedPositiveForms(40)
                                        1, "form", 1, 0, 10
                                        2, "form", 2, 0, 5
So h(K)=2
```

Example 3

Suppose $d = -14 \Rightarrow$ discriminant $D = -56$ and $w(D) = 2$.

$h(K) = \frac{-2}{2.|-56|} \sum_{n=1}^{55} n\left(\frac{-56}{n}\right)$

$= \frac{-1}{56}\{1\left(\frac{-56}{1}\right) + 2\left(\frac{-56}{2}\right) \cdots + 55\left(\frac{-56}{55}\right)\}$

$= \frac{-1}{56}\{1\left(\frac{-56}{1}\right) + 3\left(\frac{-56}{3}\right) + 5\left(\frac{-56}{5}\right) + 9\left(\frac{-56}{9}\right) + 11\left(\frac{-56}{11}\right)$

$+ 13\left(\frac{-56}{13}\right) + 15\left(\frac{-56}{15}\right) + 17\left(\frac{-56}{17}\right) + 19\left(\frac{-56}{19}\right) + 23\left(\frac{-56}{23}\right)$

$+ 25\left(\frac{-56}{25}\right) + 27\left(\frac{-56}{27}\right) + 29\left(\frac{-56}{29}\right) + 31\left(\frac{-56}{31}\right) + 33\left(\frac{-56}{33}\right)$

$+ 37\left(\frac{-56}{37}\right) + 39\left(\frac{-56}{39}\right) + 41\left(\frac{-56}{41}\right) + 43\left(\frac{-56}{43}\right) + 45\left(\frac{-56}{45}\right)$

$+ 47\left(\frac{-56}{47}\right) + 51\left(\frac{-56}{51}\right) + 53\left(\frac{-56}{53}\right) + 55\left(\frac{-56}{55}\right)\}.$

$= \frac{-1}{56}\{1(1) + 3(1) + 5(1) + 9(1) + 11(-1) + 13(1) + 15(1) + 17(-1)$

$+ 19(1) + 23(1) + 25(1) + 27(1) + 29(-1) + 31(-1) + 33(-1) + 37(-1) + 39(1)$

$+ 41(-1) + 43(-1) + 45(1) + 47(-1) + 51(-1) + 53(-1) + 55(-1)\}.$

$= \frac{-1}{56}\{224 - 448\}$

$= 4$

Calculation of $h(K)$ by counting the number of classes of quadratic forms by procedure "positive"

```
d=-14,  d(K)=-56
:
> ReducedPositiveForms(56)
                                        1, "form", 3, −2, 5
                                        2, "form", 1, 0, 14
                                        3, "form", 2, 0, 7
                                        4, "form", 3, 2, 5
:
So h(K)=4
```

Drichlet's class formula for $d > 0$

$h(K) = \frac{-1}{\log \eta} \sum_{n=1}^{n<\frac{D}{2}} \left(\frac{D}{n}\right) \log \sin \frac{n\pi}{D}$.

where η is fundamental unit.

Example 1

Suppose $d = 2$, we can calculate $\eta = 1 + \sqrt{2}$ and discriminant $D = 8$

$h(K) = \frac{-1}{\log(1+\sqrt{2})} \sum_{n=1}^{3} \left(\frac{8}{n}\right) \log \sin \left(\frac{n\pi}{8}\right)$

$= \frac{-1}{\log(1+\sqrt{2})} \{\left(\frac{8}{1}\right) \log \sin \left(\frac{\pi}{8}\right) + \left(\frac{8}{2}\right) \log \sin \left(\frac{2\pi}{8}\right) + \left(\frac{8}{3}\right) \log \sin \left(\frac{3\pi}{8}\right)\}$

$= \frac{-1}{\log(1+\sqrt{2})} \{\log \sin \left(\frac{\pi}{8}\right) - \log \sin \left(\frac{3\pi}{8}\right)\}$

$= \frac{-1}{\log(1+\sqrt{2})} \log\{\frac{\sin \frac{\pi}{8}}{\sin \frac{3\pi}{8}}\}$

$= \frac{-1}{\log(1+\sqrt{2})} \frac{1}{2} \log\{\frac{\sin^2 \frac{\pi}{8}}{\sin^2 \frac{3\pi}{8}}\}$

$= \frac{-1}{\log(1+\sqrt{2})} \frac{1}{2} \log\{\frac{1-\cos \frac{\pi}{4}}{1-\cos \frac{3\pi}{4}}\}$

$= \frac{-1}{\log(1+\sqrt{2})} \frac{1}{2} \log\{\frac{1-\frac{1}{\sqrt{2}}}{1+\frac{1}{\sqrt{2}}}\}$

$= \frac{-1}{\log(1+\sqrt{2})} \frac{1}{2} \log\{\frac{\sqrt{2}-1}{\sqrt{2}+1}\}$

$= \frac{-1}{\log(1+\sqrt{2})} \frac{1}{2} \log\{\frac{\sqrt{2}-1}{\sqrt{2}+1} \frac{\sqrt{2}+1}{\sqrt{2}+1}\}$

$= \frac{-1}{\log(1+\sqrt{2})} \frac{1}{2} \log(1+\sqrt{2})^{-2}$

$= \frac{-1}{\log(1+\sqrt{2})} \frac{1}{2} (-2) \log(1+\sqrt{2})$

$= 1$

Calculation of $h(K)$ by counting the number of classes of quadratic forms by procedure "indefinite"

d=2, d(K)=8, N(η)=-1

> *IndefiniteReducedForms*(8)

1, 2, −1

−1, 2, 1

These two forms make one cycle (1,2,-1) ~ (−1, 2, 1).

Hence h(K)=1

Example 2

Suppose $d = 3$, we can calculate $\eta = 2 + \sqrt{3}$ and discriminant $D = 12$

$$h(K) = \frac{-1}{\log(2+\sqrt{3})} \sum_{n=1}^{5} \left(\frac{12}{n}\right) \log \sin \left(\frac{n\pi}{12}\right)$$
$$= \frac{-1}{\log(2+\sqrt{3})} \{ \left(\frac{12}{1}\right) \log \sin \frac{1\pi}{12} + \left(\frac{12}{2}\right) \log \sin \frac{2\pi}{12} + \left(\frac{12}{3}\right) \log \sin \frac{3\pi}{12}$$
$$+ \left(\frac{12}{4}\right) \log \sin \frac{4\pi}{12} + \left(\frac{12}{5}\right) \log \sin \frac{5\pi}{12} \}$$
$$= \frac{-1}{\log(2+\sqrt{3})} \{ \log \sin \frac{\pi}{12} - \log \sin \frac{5\pi}{12} \}$$
$$= \frac{-1}{\log(2+\sqrt{3})} \{ \log \frac{\sqrt{3}-1}{2\sqrt{2}} - \log \frac{\sqrt{3}+1}{2\sqrt{2}} \}$$
$$= \frac{-1}{\log(2+\sqrt{3})} \{ \log \frac{\sqrt{3}-1}{\sqrt{3}+1} \}$$
$$= \frac{-1}{\log(2+\sqrt{3})} \{ -\log(2+\sqrt{3}) \}$$
$$= 1$$

Calculation of $h(K)$ by counting the number of classes of quadratic forms by procedure "indefinite"

d=3, d(K)=12, N(η)=1

```
> IndefiniteReducedForms(12)
                                  1, 2, −2
                                  −1, 2, 2
                                  2, 2, −1
                                  −2, 2, 1
```

Cycles (1,2,-2) ~ (−2, 2, 1) and (2,2,-1) ~ (−1, 2, 2).
We have two cyles and there is no unit with negatve norm, hence h(K)=2/2=1.

Example 3

Suppose $d = 6$, we can calculate $\eta = 5 + 2\sqrt{6}$ and discriminant $D = 24$

$$h(K) = \frac{-1}{\log(5+2\sqrt{6})} \sum_{n=1}^{11} \left(\frac{24}{n}\right) \log \sin \frac{n\pi}{24}$$
$$= \frac{-1}{\log(5+2\sqrt{6})} \{ \left(\frac{24}{1}\right) \log \sin \frac{\pi}{24} + \left(\frac{24}{2}\right) \log \sin \frac{2\pi}{24} + \left(\frac{24}{3}\right) \log \sin \frac{3\pi}{24} + \left(\frac{24}{4}\right) \log \sin \frac{4\pi}{24}$$
$$+ \left(\frac{24}{5}\right) \log \sin \frac{5\pi}{24} + \left(\frac{24}{6}\right) \log \sin \frac{6\pi}{24} + \left(\frac{24}{7}\right) \log \sin \frac{7\pi}{24} + \left(\frac{24}{8}\right) \log \sin \frac{8\pi}{24}$$
$$+ \left(\frac{24}{9}\right) \log \sin \frac{9\pi}{24} + \left(\frac{24}{10}\right) \log \sin \frac{10\pi}{24} + \left(\frac{24}{11}\right) \log \sin \frac{11\pi}{24} \}$$
$$= \frac{-1}{\log(5+2\sqrt{6})} \{ \log \sin \frac{\pi}{24} + \log \sin \frac{5\pi}{24} - \log \sin \frac{7\pi}{24} - \log \sin \frac{11\pi}{24} \}$$
$$= \frac{-1}{\log(5+2\sqrt{6})} \log \{ \frac{\sin \frac{\pi}{24} \sin \frac{5\pi}{24}}{\sin \frac{7\pi}{24} \sin \frac{11\pi}{24}} \}$$
$$= \frac{-1}{\log(5+2\sqrt{6})} \log \{ \frac{\cos \frac{\pi}{6} - \cos \frac{\pi}{4}}{\cos \frac{\pi}{6} - \cos \frac{3\pi}{4}} \}$$
$$= \frac{-1}{\log(5+2\sqrt{6})} \log \{ \frac{\frac{\sqrt{3}}{2} - \frac{1}{\sqrt{2}}}{\frac{\sqrt{3}}{2} + \frac{1}{\sqrt{2}}} \}$$

$$= \frac{-1}{\log(5+2\sqrt{6})} \log\{\frac{\sqrt{6}-2}{\sqrt{6}+2}\}$$
$$= \frac{-1}{\log(5+2\sqrt{6})} \log\{\frac{2}{10+4\sqrt{6}}\}$$
$$= \frac{-1}{\log(5+2\sqrt{6})} \log\{\frac{1}{5+2\sqrt{6}}\}$$
$$= 1.$$

Calculation of $h(K)$ by counting the number of classes of quadratic forms by procedure "indefinite"

d=6, d(K)=24, N(η)=1

> *IndefiniteReducedForms*(24)

1, 4, −2
−1, 4, 2
2, 4, −1
−2, 4, 1

Cycles (1,4,-2) ~ (−2, 4, 1) and (2,4,-1) ~ (−1, 4, 2).

$N(\eta) = 1$, so $h(K) = \frac{2}{2} = 1.$

Chapter 4

Carlitz's theorem

4.0.1 Detailed proof of Carlitz's theorem

Definition 38 (Order of a group)**.**

The order of a group is the number of element present in that group. We denote order of a group by $|G|$.

Theorem 17 (Carltiz's theorem)**.** *Let K be an algebraic number field. Then* $h(K) = 1$ *or* 2 *if and only if whenever a nonzero nonunit* $\alpha \in O_K$ *can be written as*

$$\alpha = ua_1a_2...a_s = u_1b_1b_2...b_t,$$

where u *and* u_1 *are units and* $a_1, a_2, ...a_s, b_1, b_2, ...b_t$ *are irreducible elements of* O_K *then* $s = t$.

Proof. Case I, $h(K) = 1$

If $h(K) = 1$ then every ideal in O_K is principal ideal, we already know that every P.I.D ring is a U.F.D. ring. Hence $s = t$.

Case II, $h(K) = 2$. Now suppose that $h(K) = 2$.

Let α be a non unit in O_K, and suppose that $\alpha = ua_1a_2\ldots a_n$, where u is a unit, and $a_1, a_2, \ldots a_n$, are irreducible elements in O_K. Then

$$(\alpha) = (\alpha_1)(\alpha_2)\ldots(\alpha_n).$$

Some of the ideals (α_1), (α_2),..., (α_n) in (α) may be prime ideals.

Suppose that $(\alpha_1)\ldots,(\alpha_k)$ are prime ideals, but $(\alpha_{k+1}),\ldots,(\alpha_n)$ are not.

We know that the each integral ideal is product of prime ideals, so

$(a_s) = p_{s_1}\ldots p_{s_{m_s}}$ for $s = k+1,\ldots,n$, and all $m_s \geq 2$

where all ideals p_{s_i} are prime.

Hence

$$(\alpha) = (a_1)\ldots(a_k)(p_1)\ldots(p_m),$$

where m is the sum of m_{s_i} and all ideals are prime.

We shall show that for any choice of i and j, p_ip_j is an integral principal ideal. The ideal class group of K has exactly two classes,

$$H(K) = I(K)/P(K) = \{1, A\}$$

where we denoted by 1 the neutral element $P(K)$,

and the class of ideals A is the coset of all non principal ideals

Since $(a_s) = p_{s_1}\ldots p_{s_{mS}}$, and a_s is irreducible, none of the ideals.

$p_{s_1},\ldots,p_{s_{m_s}}$ can not be principal, because if $p_{s_i} = (\Phi)$ with Φ not a unit then Φ would divide a_s, but a_s is irreducible, so we would have $(a_s) = p_{s_i} = (\Phi)$

but this is not possible, because $m_{s_i} \geq 2$.

Claim: Any product of two non principal ideals p_i and p_j is integral principal ideal.

Proof. Denote by $[p_i]$ the class of ideals represented by p_i. Then $[p_i] = A$ and $[p_j] = A$,

because p_i and p_j are not principal ideals so $[p_1] \neq 1$ and $[p_j] \neq 1$.

Hence, $[p_i][p_j] = [p_i p_j] = A^2 = 1$, because $h(K) = 2$.

So $p_i p_j$ is a principal ideal.

This ideal is integral because p_i and p_j are integral ideals. By matching the ideals $p_1, \ldots, p_m$ in pairs in whatever manner we conclude that m must be even, so

$$(\alpha) = (a_1)(a_2)\ldots(a_k)(\pi_1)\ldots(\pi_{m/2}),$$

where $a_1, \ldots, a_k, \pi_1, \ldots, \pi_{m/2}$ are irreducible elements of O_K.

Note that if m were odd, we would have

$$(\alpha) = (a_1)\ldots(a_k)(\pi_1)\ldots(\pi_r)p_i,$$

but (α) is a principal ideal, and p_i is not principal. This leads to a contradiction

$$p_i = (\alpha)(\pi_1^{-1})\ldots(\pi_r^{-1}) = (\alpha\pi_1^{-1}\ldots\pi_r^{-1}),$$

because p_i is not principal.

We conclude that

$$(\alpha) = (a_1)\ldots(a_k)(\pi_1)\ldots(\pi_{m/2}),$$

so

$$(\alpha) = (a_1\ldots a_k\pi_1\ldots\pi_{m/2}).$$

Hence $\alpha = u a_1\ldots a_k\pi_1\ldots\pi_{m/2}$, where u is a unit.

Therefore α factors into $k + m/2$ irreducible factors.

Since the factorization of ideal (α) into prime ideals is unique, every such factorization must have exactly k prime principal ideals and m pairwise non principal ideals factors.

Hence α always factors into $k + m/2$ irreducible elements.

□

Case III $h(K) > 2$.

Part-1

Suppose that $H(K)$ has a class of order $m > 2$.

Let A be such class and the order of A, $|A| = m > 2$.

By Hecke's Lemma [8] there is a prime ideal p_1 in A, so $A = [p_1]$. Since $A^m = I$, then $A^m = [p_1]^m = [p_1^m] = 1$, so $p_1^m = (\pi_1)$ is a principal ideal.

We claim that π is an irreducible element of O_K.

For the contradiction suppose that $\pi = ab$ with nonunits $a, b \in O_K$.

By the theorem on unique factorization of ideals, we conclude that

$(a) = p_1^k$, $(b) = p_1^l$ with integers k, l with $k+l = m, k \geq 1, m \geq 1$.

Then we have $A^k = [p_1^k] = |(a)| = 1$,

but the order of A is $m > k$, and we get a contradiction.

In any group, the order of an inverse element is equal to the order of the element, so we have $|A^{-1}| = |A| = m$.

Similarly to A, A^{-1} also contains a prime ideal, say p_2. Hence $p_2^m = (\pi_2)$, and by the same argument as above π_2 is irreducible.

Now $AA^{-1} = 1$ implies that $[p_1][p_2] = 1$, so $[p_1 p_2] = 1$, and we conclude that $p_1 p_2 = (\pi_3)$.

Again, we claim that π_3 is irreducible.

For a contradiction, suppose $\pi_3 = ab$ with nonunits $a, b \in O_K$. Then

$$p_1 p_2 = (ab) = (a)(b) \tag{4.1}$$

Since p_1 and p_2 are not principal, $(a) \neq p_1$ or p_2, $(b) \neq p_1$ or p_2.

Hence (a) factors into at least two prime ideal factors and so does (b).

Then L.H.S. of (4.1) has two prime ideal factors, while the R.H.S. has at least four ideal factors, a contradiction.

So we have $(p_1 p_2)^m = p_1^m p_2^m = (\pi_1)(\pi_2) = (\pi_1 \pi_2)$.

and $(p_1 p_2)^m = (\pi_3)^m = (\pi_3^m)$.

So $(\pi_3^m) = (\pi_1\pi_2)$.

Hence $\pi_3^m = u\pi_1\pi_2$, with some unit u.

We have $m > 2$ irreducible elements on the L.H.S. and two on the R.H.S.

Part-2

Suppose that every element of $H(K)$ has order 2, except of the class 1.

We conclude that $H(K) = \bigoplus_{i=1}^{n} \mathbb{Z}_2$. Since $H(K) > 2$, then $n \geq 2$,

Therefore $H(K)$ contains a subgroup isomorphic to $\mathbb{Z}_2 \bigoplus \mathbb{Z}_2$.

Hence there are classes A_1, A_2 in $H(K)$ such that

$|A_1| = |A_2| = 2$, and $A_1A_2 = A_3, |A_3| = 2$.

Similarly as Part-1,

let p_i be a prime ideal in A_i for $i = 1,2,3$,

Then $p_i^2 = (\pi_i)$ for $i = 1,2,3$.

with irreducible elements π_1, π_2, π_3.

Now $A_1A_2 = A_3$, and

$A_1A_2A_3 = A_3A_3 = A_3^2 = 1$.

Hence $[p_1][p_2][p_3] = 1$, and $p_1p_2p_3 = (\pi)$, with some $\pi \in O_K$.

By the same argument as in Part-1,

we conclude that π is irreducible,

$p_1p_2p_3 = (\pi)$, and $p_1^2p_2^2p_3^2 = (\pi^2)$.

Thus $(\pi_1\pi_2\pi_3) = \pi^2$.

Hence $\pi^2 = u\pi_1\pi_2\pi_3$, and

we have different number of irreducible elements at both sides.

□

4.0.2 Examples illustrating Carlitz's theorem

Example 1 $K = \mathbb{Q}(\sqrt{-5})$.

This is most popular example in most textbooks on introductory number theory.

It is known that $h(K) = 2$, which can be checked by the method shown in Chapter 3.

The only units in O_K are ± 1. We have $(2)(3) = (1+\sqrt{-5})(1-\sqrt{-5})$. Clearly all factor on both sides are irreducible, for example if

$2 = (a+b\sqrt{-5})(c+d\sqrt{-5})$ then $\bar{2} = (a-b\sqrt{-5})(c-d\sqrt{-5})$, so

$4 = (a^2+5b^2)(c^2+5d^2)$. Hence $b = d = 0$, $a = \pm 2$ and $c = \pm 1$ or $a = \pm 1$ and $c = \pm 2$. So that $a+b\sqrt{-5}$ or $c+d\sqrt{-5}$ is unit. So 2 is irreducible. In a similar way we can show that 3 and $1+\sqrt{-5}$ and $1-\sqrt{-5}$.

Example 2 $K = \mathbb{Q}(\sqrt{-13})$ here again $h(K) = 2$. The group units is $\{\pm 1\}$. We have

$(2)(7) = (1+\sqrt{-13})(1-\sqrt{-13})$.

We conclude again that these elements are not associated. Further, if

$7 = (a+b\sqrt{-13})(c+d\sqrt{-13})$, then

$\bar{7} = (a-\sqrt{-13})(c-d\sqrt{-13})$ and

$49 = (a^2+13b^2)(c^2+13d^2)$.

The right hand side can not factor as 7×7 and we conclude that one of that $b = d = 0$ and one of factors is a unit. The case for factor 2 is completely analogous.

Also $1 \pm \sqrt{-13} = (a+b\sqrt{-13})(c+d\sqrt{-13})$ leads to

$14 = (a^2+13b^2)(c^2+13d^2)$

and we rule out factorization as 2×7 on right hand side. Hence one of the factors there is a unit.

Example 3 $K = \mathbb{Q}(\sqrt{15})$.

Here also $h(K) = 2$. We have $(-1) \times (1-\sqrt{15}) \times (1+\sqrt{15}) = (2) \times (7)$. The elements 2 or 7 are not associated with $\sqrt{15}-1$ or $\sqrt{15}+1$, because these elements have different norms; $N_{\frac{K}{\mathbb{Q}}}(2) = 2^2 = 4$, $N_{\frac{K}{\mathbb{Q}}}(7) = 7^2 = 49$, but $N_{\frac{K}{\mathbb{Q}}}(1 \pm \sqrt{15}) = 14$.

It remains to show that these elements are irreducible.

Suppose that $2 = (a+b\sqrt{15})(c+d\sqrt{15})$. Since $\phi(x+y\sqrt{15}) = x-y\sqrt{15}$ is an automorphism of K and identity on $\mathbb{Q}$ we get $\bar{2} = (a-b\sqrt{15})(c-d\sqrt{15})$. Hence $4 = (a^2-15b^2)(c^2-15d^2)$. We cannot have $a^2-15b^2 = \pm 2$ because ± 2 is not a square modulo 15 so one of the factors is a unit and 2 is irreducible in O_K.

Similarly, 7 is irreducible, because $a^2-15b^2=\pm 7$ has no solution in integers, since ± 7 is not a square modulo 15.

Finally, if $1\pm\sqrt{15}=(a+b\sqrt{15})(c+d\sqrt{15})$ then $-14=(a^2-15b^2)(c^2-15d^2)$.

For the reasons stated above, right hand side cannot factor as $\pm 2\times\pm 7$, so adjoin one of the factor there must be a unit. Hence also elements $1\pm\sqrt{15}$ are irreducible.

In the first three examples, we showed factorization of same length (equal 2), but with not associated factors. Now we are going to follow Part 2 of the proof Carlitz's theorem to show a factorizations of distinct lengths for a field with $h(K)=4$.

Example 4 Let $K=\mathbb{Q}(\sqrt{210})$, so $D=4\times 210$. Let $J_1=10\mathbb{Z}+(20+2\sqrt{210})\mathbb{Z}$, H is the ideal from example on page 60 of chapter 3.

Let $A_1=[J_1]$. We need to find a prime ideal in this class. We have

$[J_1]=[10\mathbb{Z}+(20+2\sqrt{210})\mathbb{Z}]=[10\mathbb{Z}+2\sqrt{210}\mathbb{Z}]=[5\mathbb{Z}+\sqrt{210}]=[(5,\sqrt{210})]$.

Let $P_1=(5,\sqrt{210})$. We claim that P_1 is prime ideal. For this, notice that the construction of P_1 implies that $\{5,\sqrt{210}\}$ is its integral basis,and $P_1^2=(5)$ so we have

$N(P_1)=\sqrt{\frac{\triangle(5,\sqrt{210})}{2\times 210}}=5$. Since 5 is a prime number, we conclude that P_1 is prime.

Let J_2 be the ideal corresponding to the form $(10,24,-11)$ so $J_2=(12,24+2\sqrt{210})$ and we get $A_2=[J_2]$. Hence $A_2=[(6,12+\sqrt{210})]=[(12-\sqrt{210})(6,12+\sqrt{210})]=[(6(12-\sqrt{210}),66)]=[12-\sqrt{210},11]=[1-\sqrt{210},11]$. Let $P_2=(1-\sqrt{210},11)$. We can check that $\{1-\sqrt{210},11\}$ is an integral basis of P_2, and $N(P_2)=\sqrt{\frac{\triangle(1-\sqrt{210},11)}{2\times 210}}=11$. Hence P_2 is a prime ideal.

As J_3 we take the ideal corresponding to the form $(2,28,-7)$, so $J_3=(4,28+2\sqrt{210})=(4,2\sqrt{210})=(2)(2,\sqrt{210})$. Let $A_3=[J_3]$. Hence $A_3=[(2,\sqrt{210})]$. Let $P_3=(2,\sqrt{210})$. We check that $N(P_3)=2$, and $P_3^2=(2)$ so P_3 is prime as well.

Following the Part 2 of the proof of Carlitz theorem, we conclude

$P_1P_2P_3=(5,\sqrt{210})(1-\sqrt{210},11)(2,\sqrt{210})=(10,\sqrt{210})(1-\sqrt{210},11)$

$=(10-10\sqrt{210},110,\sqrt{210}-210,11\sqrt{210})$

$= (10+\sqrt{210}, 110, \sqrt{210}-210, 11\sqrt{210})$ (by adding forth generator to the first)

$= (10+\sqrt{210}, 110, 220, 11\sqrt{210})$ (by subtracting first generator from the three)

$= (10, +\sqrt{210}, 110, 11\sqrt{210})$

$= (10+\sqrt{210}, 11\sqrt{210})$ (because $110 = -(10+\sqrt{210})(10-\sqrt{210})$

$= (10+\sqrt{210})$.

For the last equality we have

$(10+\sqrt{210}, 11\sqrt{210}) = (10-\sqrt{210})(10+\sqrt{210}, 11\sqrt{210})(\frac{1}{10-\sqrt{210}})$

$= (-110, 110(\sqrt{210}-21))(\frac{1}{10-\sqrt{210}})$

$= (110)(-1, \sqrt{210}-21)(\frac{1}{10-\sqrt{210}})$

$= (110)(\frac{1}{10-\sqrt{210}})$, because $(-1, \sqrt{210}-21) = O_K$.

$= (10+\sqrt{210})$.

We claim that $P_2^2 = (31+2\sqrt{210})$.

For this we have $P_2^2 = (1-\sqrt{210}, 11)^2 = (211-2\sqrt{210}, 11-11\sqrt{210}, 121)$.

Now $211-2\sqrt{210} = (61-4\sqrt{210})(31+2\sqrt{210})$,

$11-11\sqrt{210} = (41-3\sqrt{210})(31+2\sqrt{210})$,

$121 = (31-2\sqrt{210})(31+2\sqrt{210})$.

Hence $P_2^2 = (31+2\sqrt{210})J$, where $J = (61-4\sqrt{210}, 41-3\sqrt{210}, 31-2\sqrt{210})$.

The norms of the generators of J are 19^2, -10×11 and 121 respectively. Since $\gcd(19^2, 19\times 11, 11^2) = 1$, we conclude that $J = O_K$. Hence $P_2^2 = (31+2\sqrt{210})$.

Finally, $P_1^2P_2^2P_3^2 = (10+\sqrt{210})^2$. Therefore, $(2)(5)(31+2\sqrt{210}) = u(10+\sqrt{210})^2$ where u is a unit in O_K. On the left hand side we have three irreducible factors, while on the right hand side two. Moreover, we check by direct calculation that $u = 1$. The irreducibility of the factors is guarantied by the proof of Carlitz's theorem, but can also be checked directly.

Chapter 5

Conclusions

The application of binary quadratic forms appears to be a promising approach to study the class number problem for quadratic fields. I will try to study this approach more in depth in the future, also the problem of finding conditions when a quadratic field has a fundamental unit with norm -1 seems very interesting.

Bibliography

[1] Ş.Alaca and K.S.Wlliams, *Introdctory Agebraic Number Theory*,Cambridge University Press 2004.

[2] Z.I.Borevich and I.R.Shafrevich, *Number Theory,* Academic Press, New York and London, 1966

[3] D.A. Buell, *Binary Quadratic Forms: Classical Theory and Modern Computations*, United states of America.

[4] L. Carlitz, *A characterization of algebraic number fields with class number two,* Proc. Amer. Math. Soc. 11 (1960), pp.391-392.

[5] K. Conrad, *Ideal Factorization*, public domain: https://kconrad.math.uconn.edu/blurbs/gradnumthy/idealfactor.pdf

[6] H. Davenport, *Multiplicative Number Theory*, Charendon Press Oxford 1986.

[7] B. Green, *Algebrac Number Theory*,

{http:course-archve.maths.x.ac.uk/view_material/48320}

[8] E.Hecke, *Über die L-funktionen und den Dirichletschen Primzahlsatz für einen beliebigen Zahlkörper,* Nachr.Akad. Wiss. Göttingen. Math.-Phys. Kl. IIa (1917), pp. 299-318.

[9] MathOverflow (public domain)

{https://mathoerfolw.net/questions/172432/class-number-for-binary\\
-quadratic-forms-discriminant-delta-to-class-number}

[10] I. Stewart and D.Tal, *Algebraic Number Theory and Fermat's Last Teorem*, 3-d edition, A K Peters, Ltd., 2001

[11] D. B. Zagier, *Zetafunktionen und qadratische Körper,* Springer-Verlag 1981.