VIETNAM NATIONAL UNIVERSITY
UNIVERSITY OF SCIENCE
FACULTY OF MATHEMATICS, MECHANICS AND INFORMATICS

Nguyen Tho Tung

ON THE NORM OF THE FUNDAMENTAL UNITS IN REAL QUADRATIC NUMBER FIELDS

Undergraduate Thesis

Honors Program in Mathematics

Hanoi - 2013

VIETNAM NATIONAL UNIVERSITY
UNIVERSITY OF SCIENCE
FACULTY OF MATHEMATICS, MECHANICS AND INFORMATICS

Nguyen Tho Tung

ON THE NORM OF THE FUNDAMENTAL UNITS IN REAL QUADRATIC NUMBER FIELDS

Undergraduate Thesis
Honors Program in Mathematics

Thesis advisor: Prof. Ralph Greenberg

Hanoi - 2013

Acknowledgments

First of all, I wish to express my sincere thanks to my parents for all their encouragement and support in the past 4 years. It is my honor to dedicate this thesis to them.

I would like to express my gratitude to Professor Ralph Greenberg for being my advisor. Not only did he introduce a very interesting problem to me to work on, but he also gave me helpful advice when I attempted to solve the problem. It is not an exaggeration to say that the dream of becoming a number theorist has been kindled in me with his guidance and support.

I would like to offer my special thanks to lecturers and professors at the faculty of Mathematics-Informatics-Mechanics for their unwavering support and encouragement during my 4 years at this university. They have opened many new windows to the wonderful world of mathematics to me.

Besides, I also want to say thanks to all of my friends for their assistance and cooperation. Among them, I want to express special thanks to Huyen and Ha- my two best friends, for reading the thesis and giving much useful advice. In addition, I want to thank Thinh, a member in my class, for helping me produce some experimental codes.

My special thanks are extended to Professor Nguyen Quoc Thang at Vietnam Institute of Mathematics for providing me with a wonderful chance to present my thesis at his department of number theory. I learned a great deal from giving the presentation, and further improved by thesis to a great extent.

Finally, I am particularly grateful towards Professor Le Minh Ha and Professor Moshe Rosenfeld for helping me to produce this thesis. Moreover, they gave me advice not only in mathematics but also in many other aspects of life. Without their guidance and support I could hardly achieve what I have today.

Nguyen Tho Tung
Hanoi, Oct 2013

Introduction

Mathematicians, or even high school students who are interested in mathematics would perhaps know the following theorem. For any positive integer d which is not a square, the equation

$$X^2 - dY^2 = 1,$$

has infinitely many solutions where X, Y are both integers.

This is known as Pell's equation, even though it was Euler's error to attribute its study to John Pell. In fact, Lord Brouncker was the first European mathematician who gave a general solution to this equation. More surprisingly, much evidence (see [19] or [20]) suggests that this problem was known to Archimedes. This and related problems attract researchers even today, after 2000 years since it was conceived.

This thesis deals with a closely related problem. To be more precise, we are interested in the solvability of the so called negative Pell equation

$$X^2 - dY^2 = -1, \tag{1}$$

where d is a positive squarefree integer. Unlike Pell's equation, this equation is not always solvable. For example, we can prove that the equation

$$X^2 - 7Y^2 = -1,$$

does not have any integer solution no matter how far we let X, Y go. This fact can be easily checked by considering modulo 8.

Many researchers have been studying on this problem. Some mathematicians who have made great contributions to answer the above question are Dirichlet, Redei, Helmut Hasse, Peter Stevenhagen, Franz Lemmermeyer etc (see [21]). For example, Dirichlet gave some elementary arguments to show that (1) has solutions in some special cases such as d is a prime number. Redei was perhaps the first mathematician who used results in Class Field Theory to tackle this problem. In his series of papers, he gave some beautiful criteria for the solvability of (1). Peter Stevenhagen and Franz Lemmermeyers and many other mathematicians have introduced new ideas and obtained new results. For more historical references, readers can consult [19].

A more insightful way to look at this problem is to investigate a similar one using tools in Algebraic Number Theory and Class Field Theory. Let d refer to the squarefree number that we introduced in Pell's equation, Diriclet's theorem on the structure of units in a number field asserts that the ring of algebraic integers $O_{\mathbb{Q}(\sqrt{d})}$ has the group of units isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$. In other words, there exists an element $\theta > 1$ such that every unit in $O_{\mathbb{Q}[\sqrt{d}]}$ can be written in the form $\pm\theta^k$ where k is some integer.

Let's denote by N the norm function on K. By results in algebraic number theory, if θ itself is a unit, we can conclude that $N(\theta)$ is either equal to 1 or -1. With this information in mind, we can ask ourselves a very natural question which is when $N(\theta) = 1$ and when $N(\theta) = -1$. Surprisingly, this question is equivalent to the question of the solvability of the negative Pell's equation

$$x^2 - dy^2 = -1.$$

To be more specific, the negative Pell equation is solvable if and only if the fundamental unit of the ring $O_{\mathbb{Q}[\sqrt{d}]}$ has negative norm. By this remark, our question can be now transferred into an equivalent question: for which d the fundamental unit of the quadratic ring $O_{\mathbb{Q}[\sqrt{d}]}$ has negative norm?

The purpose of this thesis is to try to answer the above question, at least partially. Most results we present in this thesis are already known but we produce new proofs and propose a promising approach to go deeper into this questions. The organization of this thesis is demonstrated below.

In the first chapter, we will provide some background and essential theorems in Algebraic Number Theory which are used throughout the thesis. For instance, we will introduce the notion of integral extensions, Galois extensions and the unique factorization of ideals in a Dedekind domain etc. The main reference for this chapter is [1], [2], [3], [4] and [5].

In the second chapter, we will apply results from chapter 1 to the case of quadratic number fields. We also show that the existence of solutions for the negative Pell equation is equivalent to the fact that the fundamental unit has negative norm. We will also include a table for the signature of the fundamental units of real quadratic fields $\mathbb{Q}[\sqrt{d}]$ for $2 \leq d \leq 40$.

The third chapter presents some basic facts about the Hilbert Class Field of a number field. Results provided there are fundamental in Class Field Theory. These include the notion of Hilbert Class Fields in the usual and strict sense and their special subfields.

The forth chapter is the heart this thesis. We will apply the results from the previous chapters to our problem. For instance, we compute the $4-$ rank explicitly in term of prime factors of D and give some criteria for the solvability of equation (1). We also present some new concepts to reveal more information about the 8 rank in a special case and show how to use this information to solve our original problem.

In the fifth chapter, we propose a new approach to our problem. This is based on our observation described in theorem 5.2.1.

Contents

Chapter 1

Some basic facts in algebraic number theory

The main purpose of this chapter is to give some essential facts in algebraic number theory that we will use throughout this thesis.

1.1 Algebraic Field Extensions

Definition 1.1.1. Let K be a field. We say that L is a field extension of K if $K \subset L$. Let us denote by $[L : K]$ the dimension of the vector space L considered as a K-vector space. This number is called the degree of the extension L/K. If $[L : K]$ is finite then we say that L/K is a finite extension.

Example 1.1.1. The field of complex numbers $\mathbb{C}$ is a field extension of the real field $\mathbb{R}$. As a vector space over $\mathbb{R}$, $\mathbb{C}$ has a basis consisting of $\{1, i\}$. Hence, $[\mathbb{C} : \mathbb{R}] = 2$ or $\mathbb{C}$ / $\mathbb{R}$ is an extension of degree 2.

Let $K \subset L$ is a field extension and $\alpha \in L$. We say that α is algebraic over K if there exist elements $a_0, \ldots, a_n$ belonging to K such that $a_n \neq 0$ and

$$a_n\alpha^n + \ldots + a_1\alpha + a_0 = 0.$$

Moreover, we have the following theorem.

Theorem 1.1.1. *Suppose α is an algebraic element over a field K. Then there exists a unique monic polynomial $f \in K[X]$ such that $f(\alpha) = 0$ and whenever $g \in K[X]$ and $g(\alpha) = 0$, we always have $f|g$.*

Proof. See [2], chapter 1, page 10. □

Definition 1.1.2. The above polynomial f is called the minimal polynomial of α over $K[X]$.

Example 1.1.2. Consider the extension $\mathbb{Q} \subset \mathbb{C}$ and $\alpha = \sqrt{2}$. Then α is algebraic over $\mathbb{Q}$ since $f(\sqrt{2}) = 0$ for $f(X) = X^2 - 2$. It is easy to see that the minimal polynomial of $\sqrt{2}$ over $\mathbb{Q}[X]$ is $X^2 - 2$.

Definition 1.1.3. We say that the extension $K \subset L$ is algebraic if for any $\alpha \in L$, α is algebraic over K.

We illustrate this definition by an example.

Example 1.1.3. Let $K = \mathbb{Q}$ be the field of rational numbers and $L = Q[\sqrt{2}] = \{a + b\sqrt{2} | a, b \in \mathbb{Q}\}$. We can easily see that $\mathbb{Q}[\sqrt{2}]$ is a field extension of $\mathbb{Q}$. We will show that it is also an algebraic extension of $\mathbb{Q}$. Indeed let $\alpha = a + b\sqrt{2}$ belong to $\mathbb{Q}[\sqrt{2}]$. Then α is a root of the polynomial $f(X) = X^2 - 2aX + (a^2 - 2b^2)$. As $a, b \in \mathbb{Q}$, we can see that $f(X) \in \mathbb{Q}[X]$. Thus, $\mathbb{Q}[\sqrt{2}]$ is an algebraic extension of $\mathbb{Q}$.

The following proposition is important in realizing algebraic extension.

Proposition 1.1.1. *If L is a finite extension of K then L/K is an algebraic extension.*

Proof. See [2], chapter 1, page 11-12. □

We have the following important corollaries.

Corollary 1.1.1.

1. *Suppose $K \subset L \subset M$ be a chain of field extensions. Suppose further that L/K and M/L are both algebraic. Then M/K is also algebraic.*
2. *Let L/K be a field extension. The set of all $\alpha \in L$ such that α is algebraic over K is a subfield of L containing K.*

When the ground field K is the field of rational numbers, we have the following definition.

Definition 1.1.4. A finite extension of $\mathbb{Q}$ is called an algebraic number field. An element α which is algebraic over $\mathbb{Q}$ is called an algebraic number.

Example 1.1.4. From example 1.1.3 we see that $\mathbb{Q}[\sqrt{2}]$ is an algebraic number field. The element $\sqrt{2}$ is an algebraic number.

Definition 1.1.5 (Galois Extension)**.** An algebraic extension L/K is called Galois if for all $\alpha \in L$, the minimal polynomial of α can be written as a product

$$f = (x - \alpha_1) \dots (x - \alpha_r),$$

where $\alpha_i \in L, \forall 1 \leq i \leq r$.

Example 1.1.5. We claim that $\mathbb{Q}[\sqrt{2}]$ is a Galois extension of $\mathbb{Q}$. Indeed, let $\alpha = a + b\sqrt{2}$ be any element in $\mathbb{Q}[\sqrt{2}]$. If $b = 0$ then the minimal polynomial of α is $X - a$ which obviously satisfies the condition given in 1.1.5. If $b \neq 0$ then the minimal polynomial of α is

$$X^2 - 2aX + (a^2 - 2b^2),$$

which can factor as

$$(X - \alpha)(X - \beta),$$

where $\beta = a - b\sqrt{2}$.

Definition 1.1.6 (Galois Group)**.** Let L/K be a Galois extension. The set of all field homomorphisms from L to itself which fix K (i.e for any $x \in K$, $f(x) = x$) forms a group. This group is called the Galois group of the extension L/K.

Example 1.1.6. Consider the extension $\mathbb{Q}[\sqrt{2}]/\mathbb{Q}$. Let σ be some element in $\mathrm{Gal}(\mathbb{Q}[\sqrt{2}]/\mathbb{Q})$. From the relation

$$(\sqrt{2})^2 - 2 = 0,$$

we see that

$$\left[\sigma(\sqrt{2})\right]^2 = 2.$$

Thus, $\sigma(\sqrt{2}) = \sqrt{2}$ or $\sigma(\sqrt{2})) = -\sqrt{2}$. Since the field $\mathbb{Q}[\sqrt{2}]$ is generated by $\sqrt{2}$, any homomorphism from $\mathbb{Q}[\sqrt{2}]$ to itself is determined by the image of $\sqrt{2}$. Therefore, we can easily see that the Galois group consists of two elements

$$Id : a + b\sqrt{d} \mapsto a + b\sqrt{d},$$

and

$$\sigma : a + b\sqrt{d} \mapsto a - b\sqrt{d}.$$

We have an important theorem, know as the Galois correspondence

Theorem 1.1.2 (Galois correspondence)**.** *Let L/K be a Galois extension and $G = Gal(L/K)$. We define two natural maps*

$$\theta : H \mapsto L^H,$$

where

$$L^H = \{x \in L | \sigma(x) = x, \forall \sigma \in H\},$$

and

$$\phi : M \mapsto Gal(L/M),$$

where M is some intermediate field between L and K. Then these two maps are inverse bijections which give us a correspondence

$$\{subgroups\ of\ G\} \longleftrightarrow \{intermediate\ fields\ K \subset M \subset L\}.$$

Moreover,

1. *This correspondence is inclusion-reversing: $H_1 \subset H_2 \Longleftrightarrow L^{H_2} \subset L^{H_1}$.*
2. *Indexes equal degrees: $[H_1 : H_2] = [L^{H_2} : L^{H_1}]$.*
3. *H is normal in G if and only if L^H is Galois over K, in which case*

$$Gal(L^H/K) = G/H.$$

Proof. See [2], chapter 3, page 29. □

1.2 Integral extension

In general, we can also study integral extension which somehow generalizes the concept of algebraic extension.

Definition 1.2.1. Let A and B be integral domains with $A \subseteq B$. An element $b \in B$ is called integral over A if there exists a monic polynomial $f(X) \in A[X]$ such that $f(b) = 0$. Equivalently, b is integral over A if it satisfies a polynomial equation

$$x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0,$$

where $a_{n-1}, \ldots, a_0$ are in A.

We say that B/A is an integral extension if each $b \in B$ is integral over A.

Remark 1.2.1. We can see that if A, B are both fields then the above definition coincides with the one defined in previous section.

Definition 1.2.2. (Algebraic integer) A complex number which is integral over $\mathbb{Z}$ is called an algebraic integer.

Remark 1.2.2. It is easy to see that an algebraic integer is also algebraic over $\mathbb{Q}$. However, there are some algebraic numbers which are not algebraic integers. For example, $\frac{1}{2}$ is an algebraic number but not an algebraic integer.

Similar to corollary 1.1.1, we also have the following proposition.

Proposition 1.2.1. *1. Let $A \subseteq B \subseteq C$ be chain of integral domains. Suppose further that B is integral over A and C is integral over B. Then C is integral over A.*

2. *The set of all elements that are integral over A is a subdomain of B containing A. We call it the integral closure of B over A.*

Proof. See [1], chapter 4, page 61. □

For each integral domain A, there exists a smallest field containing A called the fraction field of A. We will denote by $Fr(A)$ this fraction field. The following definition will be used in the next section.

Definition 1.2.3. A is said to be integrally closed if the integral closure of $Fr(A)$ in A is exactly A. In other words, if an element in $Fr(A)$ is integral over A then this element must belong to A.

Example 1.2.1. Let $A = \mathbb{Z}$. The field of fraction of A is $\mathbb{Q}$. An element in $\mathbb{Q}$ is integral over $\mathbb{Z}$ if and only if it belongs to $\mathbb{Z}$. By definition A is integrally closed. More generally, a unique factorization domain is integrally closed.

An algebraic integer is characterized by the following useful criteria.

Proposition 1.2.2. *Let α be an algebraic number and f be the minimal polynomial of α over $\mathbb{Q}$. Then, α is an algebraic integer if and only if $f \in \mathbb{Z}[X]$.*

Proof. See [3], chapter 2, page 26. □

Remark 1.2.3. Let K be an algebraic number field, the set of all algebraic integers in K is denoted by O_K.

Example 1.2.2. Consider $\alpha \in \mathbb{Q}[\sqrt{2}]$ and $\alpha = a + b\sqrt{2}$ where $a, b \in \mathbb{Q}$. Suppose further that $b \neq 0$. We will find conditions on a, b such that a is an algebraic integer.

The minimal polynomial of α over $\mathbb{Q}$ is

$$X^2 - 2aX + (a^2 - 2b^2).$$

By proposition 3, α is an algebraic integer if and only if $2a, a^2 - 2b^2$ are both integers. This happens only when both a, b are integers. Thus, we conclude that $O_{\mathbb{Q}[\sqrt{2}]} = \mathbb{Z}[\sqrt{2}]$.

1.3 Dedekind domains

Definition 1.3.1. Let A be an integral domain. We say that A is Noetherian if every ideal of A is finitely generated.

Example 1.3.1. The ring $\mathbb{Z}$ is Noetherian.

Definition 1.3.2. Let A be an integral domain. We say that A is a Dedekind domain if it satisfies the following three properties

1. A is Noetherian.

2. A is integrally closed.

3. Every non-zero prime ideal of A is maximal.

Example 1.3.2. We will show that $\mathbb{Z}$ is a Dedekind domain. First, $\mathbb{Z}$ is Noetherian since every ideal of $\mathbb{Z}$ is generated by a single element. Second, let I be any non-zero prime ideal of $\mathbb{Z}$, there exists some $n > 0$ such that $I = \langle n \rangle$. Moreover, since I is a prime ideal, n is a prime number. Consequently, I is also a maximal ideal. Finally, the fact that $\mathbb{Z}$ is integrally closed is proved in 1.2.1.

In general, we have the following proposition

Proposition 1.3.1. *The ring of algebraic integers O_K of a number field K is a Dedekind domain.*

Proof. See [3], chapter 3, page 41. □

Definition 1.3.3. A fractional ideal of K is a non-zero O_K submodule I of K that is finitely generated as an O_K-module.

Remark 1.3.1. If I is a fractional ideal of K such that $I \subset O_K$ then we call I an integral ideal. It is easy to show that all fractional ideal is of the form aI where I is an integral ideal and $a \in K^\star$.

The following theorems are standard. Proofs of these theorems can be found in [3].

Theorem 1.3.1. *Let I be a non-zero integral ideal of O_K. Then I can be written uniquely (up to order) as a product*

$$I = \mathfrak{p}_1 \mathfrak{p}_2 \ldots \mathfrak{p}_r,$$

where $\mathfrak{p}_i$ are prime ideals of O_K.

Theorem 1.3.2. *The set of fractional ideals of a number field K is an abelian group under multiplication with identity element O_K. The invert of a fractional ideal I is given by*

$$I^{-1} = \{a \in K | aI \in O_K.\}.$$

With these two theorems, we are now able to define the class group of a number field.

Definition 1.3.4 (Class Group)**.** The class group of a number field K is the group of all fractional ideals modulo the subgroup of principal fractional ideals.

Theorem 1.3.3. *The class group of a number field has finite order.*

1.4 Decomposition, Inertia Groups and Frobenius element

Let L/K be a finite extension of number fields. Let $\mathfrak{p}$ be a prime ideal in O_K, we denote by $\mathfrak{p}\, O_L$ the integral ideal of O_L generated by $\mathfrak{p}$. Since O_L is Dedekind domain, every integral ideal can be factored as product of prime ideals. In particular, we have

$$\mathfrak{p}\, O_L = \mathfrak{q}^{e_1} \ldots \mathfrak{q}^{e_r},$$

where $\mathfrak{q}_i$ are distinct prime ideals of O_L such that $\mathfrak{q}_i \cap O_K = \mathfrak{p}$. e_i is called the ramification index of $\mathfrak{q}_i$ over $\mathfrak{p}$. If $e_i = 1$ then we say that $\mathfrak{q}_i$ is unramified over $\mathfrak{p}$.

We have a natural homomorphism

$$O_K / \,\mathfrak{p} \longrightarrow O_K / \,\mathfrak{q}_i,$$

sending $a + \mathfrak{p} \longrightarrow a + \mathfrak{q}_i$. This maps is well-defined because $O_K \subset O_L$ and $\mathfrak{p} \subset \mathfrak{q}_i$. Moreover, since both $O_K / \,\mathfrak{p}$ and $O_L / \,\mathfrak{q}_i$ are finite fields, this homomorphism is an embedding. We define f_i to be

$$f(\mathfrak{q}_i \,|\, \mathfrak{p}) = [O_K / \,\mathfrak{p} : O_L / \,\mathfrak{q}_i],$$

and call it the residue degree of $\mathfrak{q}_i$ over $\mathfrak{p}$.

With these notations, we have the following theorem

Theorem 1.4.1 (Multiplicative properties of the inertia index and residue degree)**.** *Let $K \subset L \subset M$ be a finite extension of number fields, $\mathfrak{p}$ be a prime ideal in O_K, $\mathfrak{q}$ be a prime ideal in O_L lying above $\mathfrak{p}$ and $\wp$ be some prime ideal in O_M lying above $\mathfrak{q}$. Then we have*

1. $e(\wp|\mathfrak{p}) = e(\wp|\mathfrak{q})e(\mathfrak{q}\,|\,\mathfrak{p})$.
2. $f(\wp|\mathfrak{p}) = f(\wp|\mathfrak{q})f(\mathfrak{q}\,|\,\mathfrak{p})$.

Proof. See [3], chapter 9, page 99 for a proof. □

Now, suppose that L/K is a Galois extension. Let $\mathfrak{p}$ be a prime ideal of O_K, S be the set of all prime ideals of O_L lying above $\mathfrak{p}$ and $G = \text{Gal}(L/K)$ then we have a natural action of G on S given by

$$\sigma(\mathfrak{q}) = \{\sigma(x)|x \in \mathfrak{q}\}, \forall \sigma \in G, \mathfrak{q} \in S.$$

We have the following proposition

Proposition 1.4.1. *Let L/K be a Galois extension of degree n, $\mathfrak{p}$ be a prime ideal in O_K, $S = \{\mathfrak{q}_1, \ldots, q_r\}$ be the set of all prime ideals in O_L lying above $\mathfrak{p}$. We also denote by G the Galois group of L/K. Then we have the following*

1. *G acts transitively on S.*
2. *$e_1 = e_2 = \ldots = e_r$ and $f_1 = f_2 = \ldots = f_r$.*
3. *$n = efr$*

Proof. See [3], chapter 9, page 99. □

From now on, we always assume that L/K is a Galois extension of number fields. For simplicity, we will denote by $\mathfrak{q}$ a representative prime ideal of O_L lying above a prime ideal $\mathfrak{p}$ of O_K. With this convention, we have the following definition

Definition 1.4.1 (Decomposition group)**.** The set

$$D(\mathfrak{q}\,|\,\mathfrak{p}) = \{\sigma \in G|\sigma(\mathfrak{q}) = \mathfrak{q}\},$$

is called the decomposition group of $\mathfrak{q}$.

Proposition 1.4.2. *Let σ be an element of G. Then*

$$D(\sigma(\mathfrak{q})|\,\mathfrak{p}) = \sigma D(\mathfrak{q}\,|\,\mathfrak{p})\sigma^{-1}.$$

Proof. By definition, we have

$$D(\sigma(\mathfrak{q})|\,\mathfrak{p}) = \{\tau \in G|\tau(\sigma(\mathfrak{q})) = \sigma(\mathfrak{q})\} = \{\tau \in G|\sigma^{-1}\tau\sigma(\mathfrak{q}) = \mathfrak{q}\}.$$

Thus, by definition

$$D(\sigma(\mathfrak{q})|\,\mathfrak{p}) = \{\tau \in G|\sigma^{-1}\tau\sigma \in D(\mathfrak{q}\,|\,\mathfrak{p})\} = \sigma D(\mathfrak{q}\,|\,\mathfrak{p})\sigma^{-1}.$$

□

Two direct corollaries of this fact are

Corollary 1.4.1. *The order of $D(\mathfrak{q}\,|\,\mathfrak{p})$ is ef.*

Corollary 1.4.2. *If G is abelian then $D(\mathfrak{q}\,|\,\mathfrak{p})$ only depends on $\mathfrak{p}$.*

We also denote by k, l the residue fields $O_K/\,\mathfrak{p}$ and $O_L/\,\mathfrak{q}$ respectively. Then l/k is a Galois extension of finite fields. Let σ be some element in $D(\mathfrak{q}\,|\,\mathfrak{p})$, we will show that σ induces an element of $\text{Gal}(l/k)$. Let $\overline{x}$ be some element of l and x is a lift of $\overline{x}$ in O_L. We define

$$\overline{\sigma}(\overline{x}) = \sigma(x) + \mathfrak{q}\,.$$

This is well-defined because σ fixes $\mathfrak{q}$. Moreover, for any $\overline{x} \in k$, we can easily see that $\overline{\sigma}(\overline{x}) = \overline{x}$. Thus, we have a map from $D(\mathfrak{q}\,|\,\mathfrak{p})$ to $\text{Gal}(l/k)$. Indeed, we have the following theorem

Theorem 1.4.2. *The map from $D(\mathfrak{q} \mid \mathfrak{p})$ to Gal(l/k) described above is a surjective group homomorphism.*

Proof. See [3], chapter 9, page 104. □

The kernel of the above map is denoted by $I(\mathfrak{q} \mid \mathfrak{p})$ and called the inertia group of $\mathfrak{q}$ in G. By definition,

$$I(\mathfrak{q} \mid \mathfrak{p}) = \{\sigma \in G | \sigma(x) \equiv x \pmod{\mathfrak{q}}, \forall x \in O_L\}.$$

To summary, we have the following important exact sequence

$$1 \longrightarrow I(\mathfrak{q} \mid \mathfrak{p}) \longrightarrow D(\mathfrak{q} \mid \mathfrak{p}) \longrightarrow \mathrm{Gal}(l/k) \longrightarrow 1.$$

From this exact sequence, we can conclude that the order of $I(\mathfrak{q} \mid \mathfrak{p})$ is e. Thus, if $e = 1$ then we have an isomorphism from $D(\mathfrak{q} \mid \mathfrak{p})$ to Gal(l/k). In addition, we know that the Galois group Gal(l/k) is cylic and generated by the Frobenius element. Therefore, there exists a unique element $(\mathfrak{q}, L/K)$ in $D(\mathfrak{q} \mid \mathfrak{p})$ such that $(\mathfrak{q}, L/K)$ is mapped to this Frobenius element. This homomorphism can be characterized by

Proposition 1.4.3. *$(q, L/K)$ is the unique element in $D(\mathfrak{q} \mid \mathfrak{p})$ such that*

$$(q, L/K)(x) \equiv x^{N(\mathfrak{p})} \pmod{\mathfrak{q}}, \forall x \in O_L,$$

where $N(\mathfrak{p})$ is the order of the finite field k.

As we noted before 1.4.2, the decomposition group $D(\mathfrak{q} \mid \mathfrak{p})$ only depends on $\mathfrak{p}$ if G is abelian. Consequently, $(\mathfrak{q}, L/K)$ also only depends on $\mathfrak{p}$ if G is abelian. In this case, we denote this element by

$$\left(\frac{L/K}{\mathfrak{p}}\right),$$

and call it the Frobenius element with respect to $\mathfrak{p}$.

Definition 1.4.2. Let L/K be a Galois extension. $\mathfrak{p}$ and $\mathfrak{q}$ are two prime ideals of O_K and O_L described above. Then the field L^D, L^I are respectively called the decomposition and inertia subfields of L where $D = D(\mathfrak{q} \mid \mathfrak{p})$ and $I = I(\mathfrak{q} \mid \mathfrak{p})$.

By Galois correspondence (see 1.1.2), we have a chain of inclusions

$$K \subset L^D \subset L^I \subset L.$$

Let M be any intermediate field between K and L and $\mathfrak{p}'$ be the prime ideal $\mathfrak{q} \cap O_M$ of O_M. It is easy to see that $\mathfrak{p}'$ lying above $\mathfrak{p}$. Let $D' = D(\mathfrak{q} \mid \mathfrak{p}'), I' = I(\mathfrak{q} \mid \mathfrak{p}')$. Then we have the following proposition

Proposition 1.4.4. *Let H be some subgroup of $G =$ Gal(L/K) and $M = L^H$. Then $D' = D \cap H$ and $I' = I \cap H$.*

Proof. From the definition, D' of all $\sigma \in \mathrm{Gal}(L/L^H)$ such that $\sigma(\mathfrak{q}) = \mathfrak{q}$. By the Galois correspondence 1.1.2, we know that $\mathrm{Gal}(L/L^H) = H$. In addition, since $\sigma(\mathfrak{q}) = \mathfrak{q}$, $\sigma \in D$. Therefore, we must have $D' = D \cap H$. Similarly, we can also show that $I' = I \cap H$. □

Chapter 2

Quadratic Fields

2.1 Ring of algebraic integers in a quadratic field

Definition 2.1.1. A quadratic field is a field extension of $\mathbb{Q}$ of degree 2.

The following proposition is standard.

Proposition 2.1.1. *Let K be a quadratic field. Then there exists a unique square-free integer d such that $K = \mathbb{Q}[\sqrt{d}]$.*

Proof. It is rather obvious. □

With the above notation, we say that K is a real quadratic field if $d > 0$ and K is an imaginary quadratic field if $d < 0$. From now on, we will only consider the case $d > 0$.

Algebraic integers in K can be described explicitly in term of d. More precisely, we have the following proposition.

Proposition 2.1.2.

$$O_K = \begin{cases} \mathbb{Z}[\sqrt{d}], & \textit{if } d \equiv 2,3 \pmod 4 \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}], & \textit{if } d \equiv 1 \pmod 4. \end{cases}$$

Proof. Every element in $\mathbb{Q}[\sqrt{d}]$ is of the form $a + b\sqrt{d}$ where $a, b \in \mathbb{Q}$. If $b = 0$ then α is an algebraic integer if and only if $a \in \mathbb{Z}$.

Suppose that $b \neq 0$, then the minimal polynomial of α is $X^2 - 2aX + (a^2 - db^2)$. We know that α is an algebraic integer if and only if its minimal polynomial has integer coefficients. Thus, α is an algebraic integer if and only if $2a, a^2 - db^2 \in \mathbb{Z}$. By working modulo 4, we can easily get the above assertion. □

Let us note

$$\omega = \begin{cases} \sqrt{d}, & \text{if } d \equiv 2,3 \pmod 4 \\ \frac{1+\sqrt{d}}{2}, & \text{if } d \equiv 1 \pmod 4. \end{cases}$$

The previous proposition states that every element in O_K can be written uniquely in the form $a + b\omega$ for $a, b \in \mathbb{Z}$. By this observation, we have the following proposition.

Proposition 2.1.3. *Let $K = \mathbb{Q}[\sqrt{d}]$ be a quadratic number field. Then the discriminant of K is*

$$d(K) = \begin{cases} 4d, & \textit{if } d \equiv 2,3 \pmod 4 \\ d, & \textit{if } d \equiv 1 \pmod 4. \end{cases}$$

2.2 The fundamental unit of a real quadratic field

Let K be an algebraic number field and O_K be its ring of algebraic integers. An element $u \in O_K$ is said to be a unit if there exists $v \in O_K$ such that $uv = 1$. The set of all units in this ring will be denoted by $U(K)$. We will give a criterion for an element in O_K to be a unit. However, first we need to introduce some important concepts.

Definition 2.2.1. Let $F \subset K$ be a field extension. For each $\alpha \in K$, we define an $F-$ linear map by sending y to αy. The determinant of this map is called the norm of α and is denoted by $N(\alpha)$.

We will illustrate the norm by an explicit example.

Example 2.2.1. Consider $K = \mathbb{Q}[\sqrt{d}]$ and $\alpha = a + b\sqrt{d}$. We will show that $N(\alpha) = a^2 - db^2$. Indeed, $\{1, \sqrt{d}\}$ is a basis of K as a vector space over $\mathbb{Q}$. The action of α on 1 and $\sqrt{d}$ is

$$\alpha \times 1 = a + b\sqrt{d}, \quad \alpha \times \sqrt{d} = bd + a\sqrt{d}.$$

Hence, with respect to the basis $\{1, \sqrt{d}\}$, the matrix of the linear map defined by α is

$$\begin{bmatrix} a & bd \\ b & a \end{bmatrix}.$$

Thus the determinant of this linear map is $a^2 - db^2$. In other words, $N(\alpha) = a^2 - db^2$.

Proposition 2.2.1. *Let L/K be a field extension, $\alpha \in L$, $\beta \in K$. Then we have*

$$N(\alpha\beta) = N(\alpha)N(\beta).$$

Proof. It is a direct consequence of the fact that

$$\det(AB) = \det(A)\det(B),$$

where A, B are two square matrix of the same size with coefficients in a field L □

In case $F \subset K$ is a Galois extension, we have the following remarkable result.

Theorem 2.2.1. *Let $F \subset K$ be a Galois extension with Galois group $G = \{\sigma_1, \ldots, \sigma_n\}$. For any $\alpha \in K$, we have*

$$N(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha).$$

Proof. See [2], chapter 5, page 63. □

We will illustrate this theorem by the previous example.

Example 2.2.2. Consider $K = \mathbb{Q}[\sqrt{d}]$ and $\alpha = a + b\sqrt{d}$. We know in example 1.1.6, the Galois group of K over $\mathbb{Q}$ consists of two elements. The first one is the identity map and the second one is defined by

$$\sigma(u + v\sqrt{d}) = u - v\sqrt{d}.$$

Thus for $\alpha = a + b\sqrt{d}$ the norm of α is

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

This result is what we proved in previous example.

We can now state a criterion for an element to be a unit in a real quadratic number field.

Theorem 2.2.2. *Let K be a quadratic number field. A number $\alpha = a + b\sqrt{d} \in O_K$ is a unit if and only if $N(\alpha) = \pm 1$.*

Proof. Let σ be the nontrivial element in $\mathrm{Gal}(K/\mathbb{Q})$. The previous example tells us that the norm of α is

$$N(\alpha) = \alpha\sigma(\alpha).$$

Suppose α is a unit, there exists β such that $\alpha\beta = 1$. Hence

$$1 = N(1) = N(\alpha\beta) = N(\alpha)N(\beta).$$

Since $N(\alpha) \in \mathbb{Z}$ it must be either 1 or -1.

Conversely, suppose that $N(\alpha) = \pm 1$ then we have

$$\alpha\sigma(\alpha) = \pm 1.$$

which simply says that α is a unit with its inverse is either $\sigma(\alpha)$ or $-\sigma(\alpha)$. □

The following famous theorem tells us about the structure of the unit group.

Theorem 2.2.3 (Dirichlet theorem)**.** *Let K be an algebraic number field degree n and O_K is the ring of algebraic integers in K. Let $r_1, 2r_2$ be the number of real (complex) embedding of K into $\mathbb{C}$. Then the group of units in O_K contains $r_1 + r_2 - 1$ units $\omega_1, \ldots, \omega_{r_1+r_2-1}$ such that each unit in O_K can be expressed uniquely in the form $\zeta{\omega_1}^{n_1} \ldots {\omega_{r_1+r_2-1}}^{n_{r_1+r_2-1}}$ where ζ is a root of unity in O_K and n_i are integers. In other words, the group of units in O_K being isomorphic to $\underbrace{\mathbb{Z} \bigoplus \mathbb{Z} \ldots \bigoplus \mathbb{Z}}_{r_1+r_2-1} \oplus \mathbb{W}$ where W is the group of roots of unity in K.*

Proof. See [3], chapter 8, page 85. □

Consider our case where $K = \mathbb{Q}[\sqrt{d}]$ where d is a square-free integer and $d > 0$. We see that $r_1 = 2, r_2 = 0$. Moreover, the 1 and -1 are the root of unity in K. Hence, we have the group of units of K is isomorphic to $\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. Therefore, there exists an element $\theta \in O_K$ such that every unit in O_K can be expressed uniquely in the form $\pm\theta^k$ for some $k \in \mathbb{Z}$. We have the following simple observation.

Lemma 2.2.1. *The above θ can be chosen uniquely so that $\theta > 1$.*

Proof. Let θ be any element such that all other units can be written in the form $\pm\theta^k$. Then there exists exactly one element in the set $\{\theta, -\theta, \frac{1}{\theta}, -\frac{1}{\theta}\}$ that is bigger than 1. Thus, we can choose that element as a new generator. □

With this convention we have the following definition.

Definition 2.2.2. Let K be a quadratic number field. The number θ in which $\theta > 1$ and every unit in O_K can be expressed uniquely in the form $\pm\theta^k$ is called the fundamental unit of K.

Remark 2.2.1. It is not always true that the fundamental unit of a real quadratic belongs to the ring $\mathbb{Z}[\sqrt{d}]$. This is when $d \equiv 2, 3 \pmod 4$ but may not be true when $d \equiv 1 \pmod 4$. For example, the fundamental unit of $\mathbb{Q}[\sqrt{5}]$ is $\frac{1+\sqrt{5}}{2}$ which does not belong to $\mathbb{Z}[\sqrt{5}]$.

From lemma 2.2.2 we know that the norm of the fundamental unit is either 1 or -1. The following theorem will show that in some sense the norm of other units will be determined by the norm of this fundamental unit.

Theorem 2.2.4. *The real quadratic field contains a unit of norm -1 iff the fundamental unit has norm -1.*

Proof. Suppose ω is a unit in O_K then ω is of the form $\pm\theta^k$. Hence

$$N(\omega) = N(\pm\theta^k) = N(\theta)^k.$$

Suppose that the real quadratic field contains a unit of norm -1 then the equation

$$N(\theta)^k = -1,$$

is solvable. This happens only when $N(\theta) = -1$. □

The following theorem will tell us the relation between the solvability of the negative Pell equation and the norm and the fundamental unit.

Theorem 2.2.5. *The Pell equation $X^2 - dY^2 = -1$ is solvable in $\mathbb{Z}$ if and only if the fundamental unit of the quadratic field $\mathbb{Q}[\sqrt{d}]$ has norm -1.*

We need the following lemma.

Lemma 2.2.2. *Let d be a squarefree integer and $K = \mathbb{Q}[\sqrt{d}]$ be a quadratic number field. Let $R = Z[\sqrt{d}]$ and $S = O_K$. Suppose θ is an element in O_K such that $N(\theta)$ is odd. Then θ^3 is in R.*

Proof. In case $d \equiv 2, 3 \pmod 4$ then we have $O_K = \mathbb{Z}[\sqrt{d}]$, the above statement immediately follows. Hence, we only need to consider the case $d \equiv 1 \pmod 4$. In this case, the discriminant of K is d (see [2.1.3]) and therefore by [6.3.1], we see that 2 is unramified in O_K.

Let $\mathfrak{p}$ be any prime lying above 2 in S, then the field $S/\mathfrak{p}$ either has 2 or 4 elements. Therefore, the group of invertible elements in $S/\ \mathfrak{p}$ either has 1 or 3 elements. By Lagrange theorem, for any element $a \in (S/\ \mathfrak{p})^\times$ we have $a^3 = 1$. In particular, since $\theta \notin \mathfrak{p}$ we have

$$\overline{\theta}^3 = \overline{1},$$

where $\overline{\theta}$ and $\overline{1}$ are $\theta + \mathfrak{p}$ and $1 + \mathfrak{p}$ in $S/\ \mathfrak{p}$ respectively. In other words, we obtain the following relation

$$\theta^3 \equiv 1 \pmod{\mathfrak{p}}.$$

Hence, we easily see that $\theta^3 \equiv 1 \pmod{2S}$. Since $\mathbb{Z} + 2S = R$, we can conclude that $\theta^3 \in R$. □

Now coming back to the proof of theorem 2.2.5.

Theorem 2.2.5. Suppose that the negative Pell equation is solvable. Then there exists $(a, b) \in \mathbb{Z}^2$ such that

$$a^2 - db^2 = -1.$$

Lemma 2.2.2 implies that $a + b\sqrt{d}$ is a unit in O_K. By applying theorem 2.2.4, we can conclude that the fundamental unit has negative norm.

Conversely, suppose that the fundamental unit has negative norm. By lemma 2.2.2 we see that $\theta^3 \in \mathbb{Z}[\sqrt{d}]$. Moreover, $N(\theta^3) = N(\theta)^3 = -1$. Therefore, if we write $\theta^3 = u + v\sqrt{d}$ then $u, v \in \mathbb{Z}$ and

$$u^2 - dv^2 = -1.$$

In other words, (u, v) is a solution of the negative Pell equation. □

We illustrate here some numerical data about the signature of norm of the fundamental units in real quadratic number fields $\mathbb{Q}[\sqrt{d}]$ for $1 \le d \le 40$. This will somehow illustrate that our problem is not an easy one.

d	θ	sign
2	$1+\sqrt{2}$	-1
3	$2+\sqrt{3}$	1
5	$\frac{1+\sqrt{5}}{2}$	-1
6	$5+\sqrt{6}$	1
7	$8+3\sqrt{7}$	1
10	$3+\sqrt{10}$	-1
11	$10+3\sqrt{11}$	1
10	$3+\sqrt{10}$	-1
13	$\frac{3+\sqrt{13}}{2}$	-1
14	$15+4\sqrt{14}$	1
15	$4+\sqrt{15}$	1
17	$4+\sqrt{17}$	-1
19	$170+39\sqrt{10}$	1
21	$\frac{5+\sqrt{21}}{2}$	1
23	$24+5\sqrt{23}$	1
26	$5+\sqrt{26}$	-1
29	$\frac{5+\sqrt{29}}{2}$	-1
30	$11+2\sqrt{30}$	1
31	$1520+273\sqrt{31}$	1
33	$23+4\sqrt{33}$	1
34	$35+6\sqrt{34}$	1
35	$6+\sqrt{35}$	1
37	$6+\sqrt{37}$	-1
38	$37+6\sqrt{38}$	1
39	$25+4\sqrt{39}$	1

2.3 A necessary condition

In this section, we will give a necessary condition for the solvability of the equation

$$X^2 - dY^2 = -1,$$

and show that in this case, this is equation always has rational solutions by using Hasse-Minkowski principle 6.1.1.

Theorem 2.3.1. *If the negative Pell's equation*

$$X^2 - dY^2 = -1,$$

where d is a squarefree positive integer then d has no prime divisor of the form $4k+3$.

Proof. Suppose d has some prime divisor, say p, of the form $4k+3$ and (x_0, y_0) is some integers such that

$$x_0^2 - dy_0^2 = -1.$$

From this relation, we have $d | x_0^2 + 1$. Since p is a divisor of d, we have $p | x_0^2 + 1$. Thus, -1 is a quadratic residue modulo p, which is impossible. □

The above condition is just a necessary condition. As we can see from the table 2.2, when $d = 34$ the equation

$$X^2 - 34Y^2 = -1,$$

has no integer solutions even though no prime divisor of 34 is of the form $4k+3$.

However, when d has no prime divisor of form $4k+3$, the equation

$$X^2 - dY^2 = -1,$$

is always solvable over $\mathbb{Q}$. This can be proved by using Hasse-Minkowski principle (see [6.1.1]). We do not provide a full proof here but roughly speaking, checking that this equation is solvable over $\mathbb{Q}_p$ for $p > 2$ is essentially equivalent to checking that it is solvable over $\mathbb{F}_p$. The case $p = 2$ is more complicated but still can be verified quite easily.

2.4 Some elementary proofs

In this section we will provide some elementary proofs for the solvability of the negative Pell equation in some simple cases. We first start with the following theorem.

Theorem 2.4.1. *Let p be a prime number. The Pell equation*

$$X^2 - pY^2 = -1, \tag{2.1}$$

is solvable if and only if $p \equiv 1 \pmod 4$ or $p = 2$.

Proof. For $p = 2$ we can see from the table 2.2 that the fundamental unit of the quadratic field $\mathbb{Q}[\sqrt{2}]$ is $1+\sqrt{2}$ which has negative norm. Thus, we only need to prove the above theorem for p odd.

First, from the last section, we know that the if above equation is solvable in $\mathbb{Z}$ then $p \equiv 1 \pmod 4$.

Conversely, suppose that $p \equiv 1 \pmod 4$. We will show that the negative Pell equation is solvable. Let (x_0, y_0) be the smallest positive solution of the equation

$$|X^2 - pY^2| = 1.$$

If $x_0^2 - py_0^2 = -1$ then we are done. Otherwise, we have

$$x_0^2 - py_0^2 = 1.$$

This equation can be rewritten in the form

$$(x_0 - 1)(x_0 + 1) = py_0^2.$$

It is easy to see that x_0 must be odd and therefore $\gcd(x_0 - 1, x_0 + 1) = 2$. We consider two cases.

1. $p | x_0 - 1$, then there exists $u, v \in \mathbb{Z}$ such that

$$\begin{cases} x_0 - 1 = 2pu^2 \\ x_0 + 1 = 2v^2 \end{cases}$$

By subtracting the second equality by the first one, we get

$$v^2 - pu^2 = 1.$$

Thus (v, u) is also a solution of the original Pell's equation. However, since $x_0 + 1 = 2v^2$, we have $x_0 = 2v^2 - 1 > v$ which contradicts our assumption that (x_0, y_0) is the smallest positive solution.

2. $p | x_0 + 1$, there there exists $u, v \in \mathbb{Z}$ such that

$$\begin{cases} x_0 + 1 = 2pu^2 \\ x_0 - 1 = 2v^2 \end{cases}$$

By a similar argument, we have

$$v^2 - pu^2 = -1,$$

Furthermore, it is also clear that $1 < v + \sqrt{p}u < x_0 + y_0\sqrt{p}$. This contradicts our assumption that (x_0, y_0) is the smallest positive solution of the equation

$$|X^2 - pY^2| = 1.$$

□

By a similar argument, we can also prove the following theorems.

Theorem 2.4.2. *Let p_1, p_2 be two primes of the form $4k+1$ such that $\left(\frac{p_1}{p_2}\right) = -1$. Then the negative Pell equation is solvable.*

In case $p_1 = 2$, we also have a similar result

Theorem 2.4.3. *Suppose p is a prime of the form $8k+5$. Then the negative Pell equation*

$$X^2 - 2pY^2 = -1,$$

is solvable.

Chapter 3

Hilbert Class Field and its special subfields

3.1 Hilbert Class Field

Let K be a number field of degree n. Let $\sigma_1, \sigma_2, \ldots, \sigma_n$ be the set of all embeddings of K into $\mathbb{C}$. We say that an embedding σ is real if $\sigma(K) \subset \mathbb{R}$. Otherwise, σ is called a complex embedding.

Remark 3.1.1. Note that complex embedding comes in pair. That means, if σ is a complex embedding, so is $\overline{\sigma}$ where $\overline{\sigma}$ is defined by

$$\overline{\sigma}(\alpha) = \overline{\sigma(\alpha)}.$$

Definition 3.1.1. A real embedding is called an infinite real prime.

We have the following important definition

Definition 3.1.2. If σ is an infinite real prime, we say that $\alpha > 0$ with respect to σ if $\sigma(\alpha) > 0$.

We define a cycle in K as some formal product of the form $c_0 c_\infty$ where $c_0 = \prod_{i=1}^r \mathfrak{p_i}_i^{e_i}$ and each $\mathfrak{p}_i$ is a prime ideal, and c_∞ is a formal product of real infinite primes. Let a be a nonzero element in K, we say $a \equiv 1 \pmod{c}$ if

1. $v_{\mathfrak{p}_i}(a-1) \geq e_i$ for all $i \in \{1, \ldots, r\}$.
2. $a > 0$ for all real infinite primes in c_∞

Let I_c be the set of all fractional ideals in O_K which is relatively prime to c_0 and P_c be the set of all principal fractional ideals which are generated by some element a satisfying $a \equiv 1 \pmod{c}$. The quotient group I_c/P_c is called the extended class group with respect to c.

Example 3.1.1. Let K be a number field. If we define $c = 1$ then $I_c = I$ the set of all fractional ideals in O_K and $P_c = P$ the set of all principal ideals. In this case I_c/P_c is just the familiar class group of K.

If $c = 1.\infty_1 \cdots \infty_m$ where $\{\infty_1, \ldots, \infty_m\}$ is the set of all real embedding of K then $I_c = I$ and P_c is the set of all principal ideals which can be generated by some a such that $\infty_i(a) > 0$ for all $i \in \{1, \ldots, r\}$. In this case I_c/P_c is called the extended or strict class group of K.

We have the following fundamental theorems in Class Field Theory.

Theorem 3.1.1. *Let L/K be a finite Abelian extension. Then there is a cycle f of K (called the minimal conductor of L/K) such that the following hold*

1. *A prime p of K ramifies in $L/K \iff p|f$.*

2. *If c is a cycle such that $f|c$ then there is a subgroup H with $P_c \subset H \subset I_c$ such that H is the kernel of the Artin map*

$$I_c \longrightarrow Gal(L/K).$$

In particular, we have $I_c/H \cong Gal(L/K)$

Proof. See [18], chapter 6. □

We also have the following theorem.

Theorem 3.1.2. *Let c be a cycle of K and H be any subgroup of I_c with $P_c \subset H \subset I_c$. Then there exists a unique Abelian extension L/K ramified only at primes dividing c such that*

$$I_c/H \cong Gal(L/K).$$

Proof. See [18], chapter 6. □

Example 3.1.2. If we take $c = 1$ as in example 1 and $H = P$, then by theorem 3 there exists a unique abelian extension of K which is unramified everywhere. We call it the Hilbert class field of K and denote it by K^1. It is the maximal Abelian extension of K in which every prime is unramified.

If we take c to be the product of all real infinite primes and $H = I_c$ then we obtain the so-called strict Hilbert Class Field. It is the maximal Abelian extension in which every finite prime is unramified. We denote it by K^1_+.

We have the following chain of field extensions

$$Q \subset K \subset K^1 \subset K^1_+.$$

Moreover, we also have

$$\text{Gal}(K^1/K) \cong C,$$

where C is the class group of K. We also have

$$\text{Gal}(K^1_+/K) \cong C_+.$$

where C_+ is the strict class group of K. We will give an explicit computation of the Hilbert Class Field of a number field.

Proposition 3.1.1. *Let $K = \mathbb{Q}(\sqrt{-5})$ and $H = K(\sqrt{5})$. Then*

1. *K has class number equal to 2.*

2. *H/K is unramified at all primes of K.*

In other words, we can conclude that H is the Hilbert Class Field of K.

Proof. By Minkowski's theorem [see appendix], each class group in O_K contains an integral ideal with norm bounded by the Minkowski's bound

$$\left(\frac{4}{\pi}\right)^s \frac{n!}{n^n}\sqrt{|d_K|}.$$

where $n = [K : Q]$, s is the number of conjugate complex embedding and d_K is the discriminant of the number field K. In this particular case, $n = 2$, $s = 1$ as there is exactly one pair of complex embedding. Finally, $d_K = 20$ since $\{1, \sqrt{-5}\}$ forms an integral basis for O_K and

$$D(1, \sqrt{-5}) = 20.$$

So the Minkowski's bound is

$$\left(\frac{4}{\pi}\right)\frac{2!}{2^2}\sqrt{20} < 3.$$

So in order to find the class group of K, we only need to investigate the factorization of primes in $\mathbb{Z}$ which are smaller than 3. There is only one possibility, that is $p = 2$.

The minimal polynomial of $\sqrt{-5}$ in $\mathbb{Z}$ is $X^2 + 5$. In the finite field $\mathbb{Z}/2\mathbb{Z}$, this polynomial factors as $(X+1)^2$, so we have

$$2O_K = \langle 2, \sqrt{-5}+1\rangle^2.$$

Let us denote by A the ideal $\langle 2, 1+\sqrt{-5}\rangle \in O_K$. The above argument shows that the class group of K is generated by $[A]$. From the factorization of 2, we see that $[A]$ has order 2. In order to show that the class group of K is 2, we only need to show that $[A]$ has order 2. Suppose A does not have order 2 then it must have order 1. In other words, it is a principal ideal. Assume that A is generated by $x + \sqrt{-5}y$, then since $2 \in A$, we must have

$$2 = (x+\sqrt{-5}y)\gamma,$$

for some γ in O_K. Consequently, $x^2 + 5y^2 = N(x+\sqrt{-5}y)|N(2) = 4$. This happens only if $|x| = 2, y = 0$. We then have $A = \langle 2\rangle$, which is impossible. Thus, the class group of K is a cyclic group of order 2 generated by $[A]$.

For part 2, we need the following lemmas.

Lemma 3.1.1. *Suppose G is a torsion free, finitely generated $A-$ module where A is a PID. Then G is isomorphic to A^r for some $r \geq 0$.*

Proof. See [7], chapter 12, page $462 - 463$. □

Lemma 3.1.2. *Suppose $K \subset L$ be number fields. Then O_L is a torsion free and finitely generate O_K module. In particular, if O_K is a principal ideal then O_L is a free O_K module.*

Proof. O_L is a finitely generated $\mathbb{Z}$ module so it is also a finitely generated O_K module as $\mathbb{Z} \subset O_K$. In addition, O_L is obviously a torsion free O_K module. By the previous lemma, O_L is a free O_K module if O_K is principal. □

Lemma 3.1.3. *Let K be a number field and we assume that O_K is a principal ideal domain. Suppose further that there exists a basis of L consisting of elements lying in O_L, namely $(x_1, \ldots, x_n)$ such that $D_{L|K}(x_1, \ldots, x_n)$ is a square-free number in O_K. Then $(x_1, \ldots, x_n)$ is an integral basis for O_L over O_K, i.e, every element x of O_L can be written uniquely in the form*

$$x = x_1\mu_1 + \cdots + x_n\mu_n.$$

where $\mu_i \in O_K$.

Proof. As O_L is a free module over O_K as shown in lemma 3.1.2, there exists a basis $(y_1, \ldots, y_n)$ of O_L as a free module over O_K. As $(y_1, \ldots, y_n)$ is a basis, there exists a matrix A with coefficients in O_K such that

$$(x_1, \ldots, x_n) = (y_1, \ldots, y_n)A.$$

It is easy to prove that

$$D_{L|K}(x_1, \ldots, x_n) = det(A)^2 D_{L|K}(y_1, \ldots, y_n).$$

As $(x_1, \ldots, x_n)$ is a basis for L over K, its discriminant is non-zero. Thus, we have $\det(A) \neq 0$. Moreover, since $D_{L|K}(x_1, \ldots, x_n)$ is a square-free number in O_K we must have $\det(A)$ being a unit in O_K. By Crammer Rule, its invert matrix also has entries with coefficients in O_K. Thus, $(x_1, \ldots, x_n)$ is also a basis for the free module O_L over the principal domain O_K. □

We put $F = \mathbb{Q}(\sqrt{-1})$ then O_F is a principal domain. We have

$$H = K(\sqrt{5}) = \mathbb{Q}(\sqrt{-1}, \sqrt{5}) = F(\sqrt{5}).$$

So H is a quadratic extension of F. Thus, it is Galois over F with the Galois group isomorphic to $\mathbb{Z}/2$. More precisely, there are two F-automorphisms of K, namely the trivial one and the one sending $\sqrt{5}$ to $-\sqrt{5}$.

By lemma 3.1.2, we see that O_H is a free $O_F = \mathbb{Z}[\sqrt{-1}]$- module. Considering the basis $\{1, \frac{1+\sqrt{5}}{2}\}$ of H over F, we have $D_{H|F}(1, \frac{1+\sqrt{5}}{2}) = 5$. Since $5 = (2+i)(2-i)$ and $(2+i)$ and $2-i$ are both prime elements in $\mathbb{Z}[i]$, we conclude that 5 is a square free Gaussian integer in $\mathbb{Z}[i]$. By lemma 2, $\{1, \frac{1+\sqrt{5}}{2}\}$ form a $Z[i]$ basis for O_H. Combining with the fact that $\{1, i\}$ forms a basis for $\mathbb{Z}[i]$ over $\mathbb{Z}$, we obtain an integral basis for H over $\mathbb{Z}$, namely $\{1, i, \frac{1+\sqrt{5}}{2}, i\frac{1+\sqrt{5}}{2}\}$. Thus, the discriminant of O_L over $\mathbb{Z}$ is

$$D_{H|\mathbb{Q}}(1, i, \frac{1+\sqrt{5}}{2}, i\frac{1+\sqrt{5}}{2}) = 20.$$

Theorem 6.3.1 tells us that the only primes ramified in O_H are 2 and 5. In addition, since K has no real embedding, H/K is automatically unramified at infinite primes. So in order to show that H/K is an unramified extension, we only to consider the ramification of prime ideals of O_K lying above 2 and 5.

O_K is a monogenic number field having $\{1, \sqrt{-5}\}$ as an integral basis. The minimal polynomial of $\sqrt{-5}$ over $\mathbb{Z}$ is $X^2 + 5$. By a theorem about the factorization of prime ideals in a monogenic number field (see [6.5.1]) in O_K we have

$$2O_K = \langle 2, \sqrt{-5} + 1 \rangle^2,$$

and

$$5O_K = \langle \sqrt{-5} \rangle^2.$$

So we only need to show that $P = \langle 2, \sqrt{-5} + 1 \rangle$ is unramified in O_H. Suppose it is ramified then $e(2|H) = e(2|K)e(P|H) \geq 4$. By the equality

$$e(2|H).f(2|H)g(2|H) = [K : Q] = 4.$$

we conclude that $e(2|H) = 4, f(2|H) = 1, g(2|H) = 1$. However, in O_M where $M = \mathbb{Q}(\sqrt{5})$, 2 is inert. By the multiplicative property of the inertia indices (see [1.4.1]), we also have

$$4 = e(2|H) = (2|M)(2O_M|H) = e(2O_M|K).$$

(All field towers are Galois so the above notations make sense). In addition, we have

$$e(2O_M|H)f(2O_M|H)g(2O_M|H) = [H : M] = 2.$$

which is a contradiction to the above argument that $e(2O_M|H) = 4$.

Similarly, for prime ideal 5 we consider the tower $\mathbb{Q} \subset Q(i) \subset H$. For the first tower, 5 splits completely

$$5 = (2+i)(2-i).$$

so $g(5|H) \geq 2$. By a similar argument as above, we can show that $e(5|K) = 2$ and all prime ideals lying above 5 in O_H are unramified in K. □

A basic property of the Hilbert Class Field is the following.

Lemma 3.1.4. *If K is Galois over Q then K^1 and K^1_+ are Galois over Q.*

Proof. We only give a proof that K^1 is Galois over $\mathbb{Q}$. The same argument applies for K^1_+.

We embed K and K^1 into $\bar{\mathbb{Q}}$. For any field homomorphism from K^1 to $\bar{\mathbb{Q}}$, we have $\sigma(K^1)$ being unramified over $\sigma(K)$. However, since K is Galois over $\mathbb{Q}$, $\sigma(K) = K$. Thus, $\sigma(K^1)$ is also unramified over K. By the maximality of K^1, we must have $\sigma(K^1) \subset K^1$. Since it happens for all σ we can conclude that $\sigma(K^1) = K^1$. By definition, K^1 is Galois over $\mathbb{Q}$. □

Remark 3.1.2. We note that even K^1 is Galois over Q, it is not necessarily abelian over Q. For example, for $K = \mathbb{Q}(\sqrt{-23})$. Its Hilbert Class Field is the splitting field of $X^3 - X - 1$ over K. It can be shown that the Galois group of K^1 over $\mathbb{Q}$ is S_3 which is not abelian. In the next section, we will discuss a special subfield of K called the genus class field which is the largest abelian extension of $\mathbb{Q}$ contained in K^1.

3.2 Genus Class Field

Definition 3.2.1. Let K/Q be an abelian extension. The genus class field of K over Q is the largest abelian extension E of Q contained in K^1. We will denote this field by K_{gen}. Similarly, the strict genus class field is the largest abelian extension E_+ of Q contained in K^1_+ and denoted by K^+_{gen}.

Let D be the discriminant of a quadratic number field. We say that D is a prime discriminant if it is a prime power (up to sign). In other words, $d \in \{\ldots, -11, -8, -7, -4, -3, 5, 8, 13, \ldots\}$. Like prime numbers, these discriminant play an important role in our study of quadratic fields. Indeed, we have the following theorem.

Theorem 3.2.1. *Let d be the discriminant of a quadratic number field. Then d can be written uniquely (up to order) as product of prime discriminant.*

Proof. See [6], chapter 4, page 45. □

In case K is quadratic, the genus class field of K can be computed explicitly in terms of its discriminant.

Theorem 3.2.2. *Suppose d is the discriminant of a real quadratic number field and d decomposes as $d = \prod_{i=1}^{t} p_i$ where p_i are prime discriminant. Then the strict genus class field is*

$$K^+_{gen} = \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_t}).$$

In addition, suppose $p_1, \ldots, p_r < 0$ and $p_{r+1}, \ldots, p_t > 0$. Then

$$K_{gen} = \mathbb{Q}(\sqrt{p_i p_j}, \sqrt{p_{r+1}}, \ldots, \sqrt{p_t}), \forall 1 \leq i, j \leq r.$$

Example 3.2.1. Let's take $d = 21$. Then, we have $21 = (-3) \times (-5)$. By the above theorem, the genus class field in the strict sense is $\mathbb{Q}(\sqrt{-3}, \sqrt{-5})$ and the genus class field in the usual sense is just $\mathbb{Q}(\sqrt{21})$. The reason is that in the Hilbert Class Field in the strict sense we allow ramification at infinity.

Before proving this theorem, we need some preparations. First of all, by the reciprocity map, we have the following isomorphism

$$\left(\frac{K^1_+/K}{\cdot}\right) : C_+ \longrightarrow \mathrm{Gal}(K^1_+/K).$$

Let us denote by Δ the Galois group of K/Q. Since K is quadratic, Δ is generated by the map $\sigma : \mathbb{Q}(\sqrt{d}) \longrightarrow \mathbb{Q}(\sqrt{d})$ given by

$$\sigma(a + b\sqrt{d}) \mapsto a - b\sqrt{d}.$$

First of all, we can observe that Δ acts on C_+ in the natural way. That is it sends an ideal β in O_K to $\sigma(\beta)$. However, we know that $\beta\sigma(\beta) = N(\beta)$ for any ideal β in O_K, so σ acts like inversion on the class group (both in usual and strict senses). The action of Δ in the Galois group $\mathrm{Gal}(K^1_+/K)$ is more subtle. First, since K^1_+ is a Galois extension of $\mathbb{Q}$, we have the following exact sequence

$$1 \longrightarrow \mathrm{Gal}(K^1_+/K) \longrightarrow \mathrm{Gal}(K^1_+/Q) \longrightarrow \mathrm{Gal}(K/Q) \longrightarrow 1.$$

From now on let us denote by G the Galois group $\mathrm{Gal}(K^1_+/\,\mathbb{Q})$. The above exact sequence can be written in the form

$$1 \longrightarrow C_+ \longrightarrow G \longrightarrow \Delta \longrightarrow 1.$$

Since C_+ is abelian, Δ acts on C_+ by conjugation. The following proposition is very interesting.

Proposition 3.2.1. *The reciprocity map is Δ equivariant. More precisely, for any ideal class (both in the strict and usual senses), we have*

$$\sigma([\beta]) = \sigma\left(\frac{K^1_+/K}{\beta}\right)\sigma^{-1}.$$

By Galois correspondence, the genus class field corresponds to a subgroup H of G. Moreover, since the genus class field is the maximal abelian extension of Q contained in the Hilbert Class field (both in usual and strict senses), H has the properties that it is the smallest subgroup of G in which G/H is abelian. By group theory, we know that H is the derived group of G. In other words, H is the group generated by all commutators in G. We consider the following exact sequence

$$1 \longrightarrow C_+ \longrightarrow G \longrightarrow \Delta \longrightarrow 1.$$

Then by the above remark, we have $\sigma n \sigma^{-1} = n^{-1}$ for any $n \in C_+$. So in particular, we have

$$\sigma n \sigma^{-1} n^{-1} = n^{-2}.$$

Thus, we have $C^2_+ \subset [G, G]$. In addition, it is also easy to observe that C^2_+ is a normal subgroup of G. Thus, we also obtain the following exact sequence

$$1 \longrightarrow C_+/C^2_+ \longrightarrow G/C^2_+ \longrightarrow \Delta \longrightarrow 1.$$

However, by the relation $[\sigma, n] = n^{-2}$, we conclude that the action of Δ on C_+/C^2_+ is trivial. By group theory, we know that

$$G/C^2_+ \cong \Delta \times C_+/C^2_+.$$

So in particular, G/C^2_+ is abelian and hence $[G, G] \subset C^2_+$. So in conclusion, we have $[G, G] = C^2_+$. Moreover, we also have

$$G/C^2_+ \cong \Delta \times C_+/C^2_+.$$

So G/C^2_+ is an elementary $2-$ abelian group. By Galois theory, the genus class field is the composite of quadratic fields. Suppose $\mathbb{Q}(\sqrt{m})$ where m is a square-number is a subfield of K^+_{gen}. Then we claim that $m|d$. Indeed, take any prime $p|m$ such that $p \nmid d$. Then the by looking at the diagram

$$\begin{tikzcd}
K(\sqrt{p}) \arrow[d, dash] \\
K = \mathbb{Q}(\sqrt{d}) \arrow[d, dash] \\
\mathbb{Q}
\end{tikzcd}$$

we can conclude that $\mathfrak{p}$ is ramified in $K(\sqrt{p})$ where $\mathfrak{p}$ be some prime ideal in O_K lying above p. Thus, we must have $m|d$. In particular, we always have

$$K_{gen}^{+} \subset \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_t}).$$

In order to finish the proof we need the following lemma.

Lemma 3.2.1. *Let $a_1, a_2, \ldots, a_n$ be integers such that for any subset I of $\{1, 2, \ldots, n\}$, the product $\prod_{i \in I} |a_i|$ is not a square. Then $Q(\sqrt{a_1}, \ldots, \sqrt{a_n})$ is a Galois extension of Q of order 2^n with Galois group being $(\mathbb{Z}/2\mathbb{Z})^n$.*

Proof. First, we observe that every homomorphism from $\mathbb{Q}(\sqrt{a_1}, \ldots, \sqrt{a_n})$ to $\overline{\mathbb{Q}}$ depends completely on its action on the generator $\{\sqrt{a_1}, \ldots, \sqrt{a_n}\}$. However, the only conjugate of $\sqrt{a_i}$ is $-\sqrt{a_i}$ which also lies in $\mathbb{Q}(\sqrt{a_1}, \ldots, \sqrt{a_n})$. Thus, each homomorphism from $\mathbb{Q}(\sqrt{a_1}, \ldots, \sqrt{a_n})$ to $\overline{\mathbb{Q}}$ sends $\mathbb{Q}(\sqrt{a_1}, \ldots, \sqrt{a_n})$ to itself. Accordingly, $\mathbb{Q}(\sqrt{a_1}, \ldots, \sqrt{a_n})$ is a Galois extension over $\mathbb{Q}$. Moreover, it is also easy to see that each automorphism of $\mathbb{Q}(\sqrt{a_1}, \ldots, \sqrt{a_n})$ has order at most 2. Therefore, if we can show that this field is an extension of Q of degree 2^n then we are done.

We can prove this claim by induction on n. For $n = 1$ it is obvious. Suppose it has been show that $Q(\sqrt{a_1}, \ldots, \sqrt{a_n})$ is an extension of $\mathbb{Q}$ of degree 2^n. We will show that it is also true for $n+1$. Consider the field extension $H = Q(\sqrt{a_1}, \ldots, \sqrt{a_{n+1}})$ over Q. If there exists an index i, for instance $n+1$ such that

$$\sqrt{a_{n+1}} \notin \mathbb{Q}(\sqrt{a_1}, \ldots, \sqrt{a_n}),$$

then we have

$$\mathbb{Q}(\sqrt{a_1}, \ldots, \sqrt{a_{n+1}}) : Q] = [K(\sqrt{a_{n+1}}) : K][K : Q] = 2.2^{n-1} = 2^n,$$

where $K = \mathbb{Q}(\sqrt{a_1}, \ldots, \sqrt{a_n})$. Thus, we are done in this case. Now, we suppose that for any i we have $\sqrt{a_i} \notin H_i$ where $H_i = \mathbb{Q}[S_i]$ and $S_i = \{a_1, \ldots, a_{n+1}\} - \{a_i\}$. Then in particular, we have $\sqrt{a_{n+1}} \in \mathbb{Q}(\sqrt{a_1}, \ldots, \sqrt{a_{n-1}})(\sqrt{a_n})$. Thus, by definition, there exist $p, q \in \mathbb{Q}(\sqrt{a_1}, \ldots, \sqrt{a_{n-1}})$ such that

$$\sqrt{a_{n+1}} = p + q\sqrt{a_n}.$$

If $p = 0$ then $\sqrt{a_{n+1}} = q\sqrt{a_n}$. It is then followed that

$$\sqrt{a_{n+1}a_n} = pa_n \in \mathbb{Q}(\sqrt{a_1}, \ldots, \sqrt{a_{n-1}}).$$

This is impossible by inductive hypothesis that $\mathbb{Q}(\sqrt{a_1}, \ldots, \sqrt{a_{n-1}})$ is an extension of degree 2^{n-1} while $\mathbb{Q}(\sqrt{a_1}, \ldots, \sqrt{a_n a_{n+1}})$ is an extension of degree 2^n. Thus, we have shown that $p \neq 0$. Similarly, q is not zero. In addition, from the equality we have

$$\sqrt{a_{n+1}a_n} = p\sqrt{a_n} + qa_n,$$

and

$$a_{n+1} = p\sqrt{a_{n+1}} + q\sqrt{a_{n+1}a_n}.$$

By multiplying the first equation with q and then add side to side, we get

$$a_{n+1} = pq\sqrt{a_n} + q^2 a_n + p\sqrt{a_{n+1}}.$$

We can rewrite this as

$$a_{n+1} - q^2 a_n = p(q\sqrt{a_n} + \sqrt{a_n + 1})$$

As $p \neq 0$, we find that $q\sqrt{a_n} + \sqrt{a_{n+1}}$ is an element in $\mathbb{Q}(\sqrt{a_1}, \ldots, \sqrt{a_{n-1}})$. We also have $\sqrt{a_{n+1}} = p + q\sqrt{a_n}$, so $2q\sqrt{a_n} + p$ lies in $\mathbb{Q}(\sqrt{a_1}, \ldots, \sqrt{a_{n-1}})$. However, since $2q$ is not 0 we must have $\sqrt{a_n} \in \mathbb{Q}(\sqrt{a_1}, \ldots, \sqrt{a_{n-1}})$ which is impossible by inductive hypothesis. Thus, we must have $\mathbb{Q}(\sqrt{a_1}, \ldots, \sqrt{a_{n+1}})$ being an extension of degree 2^{n+1}. By induction principle, we prove that the claim holds for any n. □

We have an important corollary.

Corollary 3.2.1. *$\mathbb{Q}(\sqrt{p_1},\dots,\sqrt{p_t})$ is an abelian extension of $\mathbb{Q}$, containing K and unramified over K*

In order to prove this corollary, we need a lemma.

Lemma 3.2.2. *Suppose L_1 and L_2 are finite extensions of a number field K and $\wp$ is a nonzero prime ideal in O_K. Then $\wp$ is unramified in L_1 and L_2 if and only if it is unramified in L_1L_2.*

Proof. If $\wp$ is unramified in L_1L_2 then it is obviously unramified in both L_1 and L_2 by multiplicative property of ramification indexes in field towers. Now suppose that $\wp$ is both unramified in L_1 and L_2. We will show that it is also unramified in L_1L_2. Let $\wp'$ be any prime in $O_{L_1L_2}$ lying above $\wp$. Suppose further that M is the Galois closure of L_1L_2 and P is a prime ideal lying above $\wp'$. We also denote $I = I_{P|\wp}$. Then M^I be the corresponding inertia field. It is the maximal subfield of M in which $\wp$ is unramified. By our assumption, we must have $L_1 \subset M^I$ and $L_2 \subset M^I$. Hence, $L_1L_2 \subset M^I$. In particular, we have $e(\wp'|p) = 1$. □

A proof for corollary 3.2.1. We can now come to our proof. Since the field $\mathbb{Q}(\sqrt{p_1},\dots,\sqrt{p_t})$ is the composition of $K(\sqrt{p_i})$ for $i = 1,\dots,t$, in order to show that $\mathbb{Q}(\sqrt{p_1},\dots,\sqrt{p_t})$ is unramfied over K, it is sufficient to show that $K(\sqrt{p_i})/K$ is an unramified extension for any $i = 1,\dots,t$. Indeed, let $\wp$ be any ideal in O_K. Let $p = \wp \cap Z$ the prime ideal lying below $\wp$. In addition, we also denote by $\wp'$ the prime ideal in $K(\sqrt{p_i})$ lying above $\wp$. We can see that if $p \nmid d$ then the prime ideal p is unramified in the extension $K(\sqrt{p_i})/Q$ since p is unramified over K and $\mathbb{Q}(\sqrt{p_i})$. Now suppose $p|d$. If $p \neq p_i$ then the prime ideal p is not ramified in $Q(\sqrt{p_i})$. By the multiplicative property of the inertia indices in towers, we see that $e(\wp'|p) \leq 2$. However, we have

$$e(\wp'|p) = e(\wp'|\wp)e(\wp|p) = 2e(\wp'|\wp).$$

Combining these facts, we can conclude that $e(\wp'|\wp) = 1$. Now consider the case when $p = p_i$. Then p is unramified over $\mathbb{Q}(\sqrt{\frac{d}{p_i}})$, and by the same argument we still have $e(\wp'|\wp) = 1$. By using theorem 3.2.2, we complete the lemma. □

The lemma and the fact that $K^+_{gen} \subset \mathbb{Q}(\sqrt{p_1},\dots,\sqrt{p_t})$ simply imply that

$$K^+_{gen} = \mathbb{Q}(\sqrt{p_1},\dots,\sqrt{p_t}).$$

A similar argument can also be applied to show that

$$K_{gen} = \mathbb{Q}(\sqrt{d_id_j},\sqrt{d_{r+1}},\dots,\sqrt{d_t}), \forall 1 \leq i,j \leq r.$$

Thus, if d satisfies the necessary condition given in 2.3 (i.e no prime divisor of d is of the form $4k+3$) then we can conclude that the genus class field and the genus class field in the strict sense coincide. Moreover, we have a natural isomorphism

$$C/C^2 \cong C_+/C_+^2 \cong \mathrm{Gal}(K_{gen}/K) \cong (\mathbb{Z}/2\mathbb{Z})^{t-1}.$$

3.3 2-Hilbert Class Field

Let S be the $2-$ Sylow subgroup of the Galois group $\mathrm{Gal}(K^1/K)$ and H^2 be the corresponding intermediate field. With this notation, H^2 is called the $2-$ Hilbert Class Field of K. Similarly, we also denote by H^2_+ the strict $2-$ Hilbert class field of K. The following proposition is standard.

Theorem 3.3.1. *Suppose that K is Galois over $\mathbb{Q}$ then so are H^2 and H^2_+.*

Proof. We will prove that H^2 is Galois over $\mathbb{Q}$. The fact that H^2_+ is also Galois over $\mathbb{Q}$ can be proved similarly.

Since K^1/H^2 is a Galois extension of finite degree, every K homomorphism from H^2 to $\overline{\mathbb{Q}}$ is indeed the restriction of some homomorphism from K^1 to $\overline{\mathbb{Q}}$. Let σ be any such homomorphism. We see that $\sigma(H^2)$ being an intermediate subfield of $\sigma(K) = K$ and $\sigma(K^1) = K^1$. In addition, we know that $\mathrm{Gal}(\sigma(H^2)/\sigma(K) \cong \mathrm{Gal}(H^2/K)$. Furthermore, since K is Galois $\sigma(K) = K$, we can conclude that

$$\mathrm{Gal}(\sigma(H^2)/K \cong \mathrm{Gal}(H^2/K).$$

Thus $\sigma(H^2)$ corresponds to the unique 2-Sylow subgroup of C. As a result, we must have $\sigma(H^2) = H^2$. By definition, H^2 is Galois over $\mathbb{Q}$. □

The reason we are concerned with these sub-fields is the following theorem.

Theorem 3.3.2. *The fundamental unit of the number ring O_K where K is real quadratic field has norm -1 if and only if $H^2 = H^2_+$.*

Before proving this theorem, we need the following important lemma.

Lemma 3.3.1. *Let us denote by J the group generated by ideal class $[\sqrt{d}]_+$ in the strict sense then we have the following exact sequence*

$$1 \longrightarrow J \longrightarrow C_+ \xrightarrow{\pi} C \longrightarrow 1.$$

where π is the projection map sending a class group in the strict sense to the corresponding class group in the usual sense. Furthermore, J is trivial if and only if the fundamental unit has norm -1. Otherwise, it is isomorphic to $\mathbb{Z}/2\mathbb{Z}$.

Proof. We only need to show that the kernel of π is $[\sqrt{d}]_+$. In other words, if a class group in the strict sense induces a trivial class group in the usual sense by the homomorphism described above then it is either 1 or $[\sqrt{d}]_+$. Suppose that $[\alpha] = [1]$. We need to show that $[\alpha]_+ = [1]_+$ or $[\sqrt{d}]_+$. Indeed, by definition, $[\alpha] = [1]$ means that there exists $\lambda \in K$ such that $\alpha = (\lambda)$. Without loss of generality, we can assume that $\lambda > 0$. Let σ be the the isomorphism of $\mathbb{Q}[\sqrt{d}]$ defined by

$$\sigma : a + b\sqrt{d} \mapsto a - b\sqrt{d}, \forall a, b \in \mathbb{Q}.$$

We consider two cases.

- $\sigma(\lambda) > 0$. By definition α is equivalent to λ in the strict sense so $[\alpha] = [1]_+$.
- $\sigma(\lambda) < 0$. Then it is easy to see that $\sigma(\sqrt{d}.\lambda) > 0$. In addition, $\sqrt{d}\lambda > 0$. Thus, $\sqrt{d}\lambda$ is totally positive. It is then easy to show that $[\alpha]_+ = [\sqrt{d}]_+$.

Now suppose that the fundamental unit, say ϵ, has norm -1, then $\epsilon\sqrt{d}$ is totally positive since $\epsilon\sqrt{d} >$ and $\sigma(\epsilon\sqrt{d}) = d > 0$. Thus, $[\sqrt{d}]_+$ is trivial.

In case the fundamental unit has norm 1, every unit has norm 1. Then every other unit has norm 1 (see [2.2.4]). Thus, $\eta\sqrt{d}$ cannot be totally positive for all choice of unit η. Equivalently, $(\sqrt{d})$ cannot be principal in the strict sense. Since $[\langle\sqrt{d}\rangle]^2_+ = 1$, we can conclude that J has order 2. In other words, $J = \mathbb{Z}/2\mathbb{Z}$. □

A direct corollary of this lemma is that.

Corollary 3.3.1. *The fundamental unit of the real quadratic field $\mathbb{Q}[\sqrt{d}]$ has negative norm if and only if $|C| = |C_+|$.*

We come back to our main theorem. Consider the following chain of field extension

$$\begin{tikzcd}
K_{+}^{1} \arrow[d, dash] \\
K^{1} \arrow[d, dash] \\
K \arrow[d, dash] \\
Q
\end{tikzcd}$$

By definition, we have $C = \mathrm{Gal}(K^1/K)$ and $C_+ = \mathrm{Gal}(K_+^1/K)$ so by Galois correspondence, we have

$$C_+/C \cong \mathrm{Gal}(K_+^1/K)/\,\mathrm{Gal}(K^1/K).$$

Furthermore since $\mathrm{Gal}(K_+^1/K)$ and $\mathrm{Gal}(K^1/K)$ are both abelian, we have

$$\mathrm{Gal}(K_+^1/K)/\,\mathrm{Gal}(K^1/K) \cong S_+/S,$$

where S_+ and S are the $2-$ Sylow subgroup of $\mathrm{Gal}(K_+^1/K)$ and $\mathrm{Gal}(K^1/K)$ respectively. By Galois correspondence, we once again have

$$S_+/S \cong \mathrm{Gal}(H_+^2/H^2).$$

Thus, in summary, we have

$$C_+/C \cong \mathrm{Gal}(H_+^2/H^2).$$

By corollary 4.3.1, we conclude that the fundamental unit has negative norm if only if the Galois group $\mathrm{Gal}(H_+^2/H^2)$ is trivial or in other words, $H_+^2 = H^2$.

Finally, we have the following important theorem

Theorem 3.3.3. *The fundamental unit of a real quadratic field has negative norm if and only if its strict* 2-*Hilbert Class Field is totally real.*

This theorem is crucial in our investigation in the next chapter.

Chapter 4

Some results achieved

In this chapter, we will present some results that we have achieved so far using tools that we developed in the previous chapters.

4.1 The case that D is a prime number

When D is a prime number, we have the following theorem

Theorem 4.1.1. *Suppose p is a prime number of the form $4k+1$ then the fundamental unit of the quadratic field $\mathbb{Z}[\sqrt{p}]$ has negative norm.*

Proof. By results from previous chapter, it is sufficient to show that $C = C_+$. Indeed, we know that

$$C/C^2 \cong C_+/C_+^2 \cong (\mathbb{Z}/2\mathbb{Z})^{t-1},$$

In this case $t = 1$ so C/C^2 and C_+/C_+^2 are trivial. Therefore, $S = S_+ = \{1\}$ and consequently $H^2 = H_+^2$. By theorem 3.3.2, we conclude that the fundamental unit has negative norm. □

4.2 D is product of two prime numbers

When D is product of two prime numbers of form $4k+1$ and each of these primes is not a quadratic residue of the other then we have the following theorem.

Theorem 4.2.1. *Suppose $D = p_1 p_2$ where p_1, p_2 are of the form $4k+1$ and $\left(\frac{p_1}{p_2}\right) = -1$. Then the fundamental unit of the quadratic field $\mathbb{Q}[\sqrt{p_1 p_2}]$ has negative norm.*

We will prove this theorem by a series of argument. A second proof for this theorem is also introduced in the next section.

First, we notice that

$$S/S^2 \cong \mathrm{Gal}(K_{gen}/K) \cong \mathbb{Z}/2\mathbb{Z}.$$

Since S is a $2-$ abelian group, it must be $\mathbb{Z}/2^n\mathbb{Z}$ for some $n \geq 1$. Similarly, S_+ is also of the form $\mathbb{Z}/2^m\mathbb{Z}$ for some m. We have the following lemma.

Lemma 4.2.1. *Let G be a cyclic group of prime power order (i.e $G = \mathbb{Z}/p^n\mathbb{Z}$). Then for any two subgroups of G, one of them is a subgroup of the other one.*

Proof. Let x be a generator for G. In group theory, we know that every subgroup of G is a cyclic group generated by x^d for some $d > 0$ and $d|p^n$. Thus $d = p^m$ for some $m \geq 0$. Suppose we have two subgroups G_1 and G_2. By the previous remark, we can assume that G_1 is generated by $x^{p^{m_1}}$ and G_2 is generated by $x^{p^{m_2}}$. Without loss of generality, we can suppose that $m_1 \leq m_2$. Then it is immediately implied that $G_2 \subset G_1$. Since it is true for any two subgroups, we complete the proof. □

We now can come to our proof. Consider the following diagram

$$\begin{tikzcd}
H_+ \arrow[d, dash] \\
K_{gen}^+ \arrow[d, dash] \\
K \arrow[d, dash] \\
\mathbb{Q}
\end{tikzcd}$$

where H_+ is the $2-$ Hilbert Class Field of K in the strict sense. Let $\wp$ be a prime ideal lying above p_2. Then we can see that $\wp$ is inert in K_{gen}^+. Let $\wp'$ be a prime ideal lying above $\wp$ in O_{H_+} and D be the decomposition group of $\wp'$ over $\wp$. We will show that $D = \mathrm{Gal}(H_+/K)$. It is sufficient to show that $H_+^D = K$. By Galois correspondence, we observe that one of two fields K_{gen}^+ and H_+^D is a subfield of another. Suppose that $K_{gen} \subset H_+^D$. Since H_+^D is the largest subfield in which $\wp$ splits completely, it contradicts the fact that $\wp$ is inert in K_{gen}^+. Thus, we must have $H_+^D = K$. In other words, we have $D = \mathrm{Gal}(H_+/K)$. Combining with the fact that $p_2 O_K = \wp^2$ we can easily conclude that $D(\wp'|p_2) = \mathrm{Gal}(H_+/Q)$. Let I be the inertia group of $\wp'$ over p_2 then by the multiplicative property of ramification indices in a tower of field extensions (see [1.4.1]) , we have $|I(\wp'|p_2)| = 2$. Moreover, we have

$$D(\wp'|p_2)/I(\wp'|p_2) \cong \mathrm{Gal}(l/k).$$

where $l = O_{H_+}/\wp'$ and $k = \mathbb{F}_p$ are all finite fields. The Galois group $\mathrm{Gal}\,(l/k)$ is cyclic and generated by the Frobenius element, hence D/I is a cyclic group. Since I has order 2, we can conclude that D is an abelian group. By definition, we must have $K_{gen}^+ = H_+$. In particular, we have H_+ being totally real. By theorem 3.3.3, we can conclude that the fundamental unit has negative norm.

4.3 The 4-rank of the narrow class group

Let $K = \mathbb{Q}(\sqrt{d})$ and $d = \prod_{i=1}^{t} p_i$ be the decomposition of d into prime discriminant. For each $0 \leq i \leq t$ consider the field $F_i = K(\sqrt{p_i})$. In this section, we will determine some properties of the restriction of the Artin map to extension F_i/K. Let us recall the definition of the Artin map. Let $\mathfrak{p}$ be any prime ideal in O_K. Let $\mathfrak{q}$ be any prime ideal of O_{F_i} lying above $\mathfrak{p}$ then we have the following isomorphism

$$D(\mathfrak{q}|\mathfrak{p}) \longrightarrow \mathrm{Gal}(l/k).$$

where $l = O_{F_i}/\mathfrak{q}$ and $k = O_K/\mathfrak{p}$. Since the extension is abelian, the Artin symbol only depends on $\mathfrak{p}$. Thus, for each prime ideal in O_K, we can find a corresponding element in $\mathrm{Gal}(F_i/K)$ which is simply $\mathbb{Z}/2\mathbb{Z}$. Since the set of all ideals in O_K can be considered as a free group generated by the set of all prime ideals, the above map can be extended to all ideals. We denote this map by χ_i.

$$\chi_i : I(K) \longrightarrow \mathbb{Z}/2\mathbb{Z}.$$

The main theorem in this section is the following.

Theorem 4.3.1. *With the above notation, for every ideal $\mathfrak{p}$ in O_K, we have*

$$\chi_i(\mathfrak{p}) = \begin{cases} (\frac{p_i}{N(\mathfrak{p})}) & \textit{if } \gcd(p_i, N\mathfrak{p}) = 1 \\ (\frac{d/d_i}{N(\mathfrak{p})}) & \textit{if } \gcd(d/p_i, N\mathfrak{p}) = 1. \end{cases}$$

Here $\left(\frac{p}{q}\right)$ *denotes the Legendre symbol and*

$$\left(\frac{d}{2}\right) = \begin{cases} 1 & \textit{if } d \equiv 1 \pmod 8 \\ -1 & \textit{if } d \equiv 5 \pmod 8. \end{cases}$$

First of all, we notice that the above definition makes sense. That is, we need to verify that if $N\mathfrak{p} \nmid d$ then

$$\left(\frac{p_i}{N(\mathfrak{p})}\right) = \left(\frac{d/p_i}{N(\mathfrak{p})}\right).$$

Indeed, if $N\mathfrak{p}$ is a square then the equality is obvious. In case $N\mathfrak{p} = p$ is a prime then p splits in O_K. That is equivalent to $\left(\frac{d}{p}\right) = 1$. Since $d = p_i \times d/p_i$, we have the above equality by the multiplicative property of the Legendre symbol. We can now come to a proof for this theorem.

Proof. Let $p = \mathfrak{p} \cap Z$, that is, p is the prime ideal lying below $\mathfrak{p}$ in $\mathbb{Z}$. Since F_i/K is an unramified extension, the prime ideal $\mathfrak{p}$ is either inert or splits completely in O_{F_i}. We only give our proof for the case that $\mathfrak{p}$ is inert since a similar argument could also be applied for the case $\mathfrak{p}$ that splits completely.

Suppose now that $\mathfrak{p}$ is inert in O_{F_i}. In other words, $\mathfrak{p}O_{F_i} = \mathfrak{q}$. In this case the extension l/k mentioned above has degree 2 and therefore the Frobenius homomorphism is a non-trivial automorphism of l. By definition, we have $\chi_i(\mathfrak{p}) = -1$. Thus, in order to show the equality it suffices to show that either $\left(\frac{d_i}{N(\mathfrak{p}}\right) = -1$ or $\left(\frac{d/d_i}{N(\mathfrak{p}}\right) = -1$. We consider the following cases.

Case 1. p is an unramified prime in O_K. Since p is unramified in F_i it is unramified over all subfields of F_i.

In this case p neither splits completely in $Q(\sqrt{d/p_i})$ nor $\mathbb{Q}(\sqrt{p_i})$. Indeed, if p splits completely both in $\mathbb{Q}(\sqrt{d/p_i})$ and $\mathbb{Q}(\sqrt{p_i})$ then it would split completely in $\mathbb{Q}(\sqrt{p_i}, \sqrt{d/p_i}) = F_i$. In other words, we must have $e(\mathfrak{q}|p) = f(\mathfrak{q}|p) = 1$ and $g(\mathfrak{q}|p) = 4$. This is impossible since $\mathfrak{p}$ is inner in K and hence $f(\mathfrak{q}|p) = f(\mathfrak{q}|\mathfrak{p})f(\mathfrak{p}|p) \geq 2$. Therefore, p is either inert in $\mathbb{Q}(\sqrt{p_i})$ or $\mathbb{Q}(\sqrt{d/p_i})$. Since we have pointed out the correctness of definition in theorem 1, we can conclude

$$\left(\frac{p_i}{N(\mathfrak{p})}\right) = \left(\frac{d/p_i}{N(\mathfrak{p})}\right) = -1.$$

Case 2. p is ramified in O_K. Then, we have

$$e(\mathfrak{q}|p) = 2, \quad f(\mathfrak{q}|p) = 2, \quad g(\mathfrak{q}|p) = 1.$$

Since p is a prime and $p|d$, it is relatively prime to exactly one of the two numbers p_i and d/p_i. Without loss of generality, we can assume that $p|p_i$ and $\gcd(p, d/p_i) = 1$. Then the prime ideal p is unramified over the extension $\mathbb{Q}(\sqrt{d/d_i})$ over $\mathbb{Q}$. We will show that p is indeed inert in this extension. Now suppose to the contrary that p splits completely in $\mathbb{Q}(\sqrt{d/p_i})$. Then $g(\mathfrak{q}|p) \geq 2$, which is impossible. Therefore, p is inert over $\mathbb{Q}(\sqrt{d/p_i})$. By definition, we have

$$\left(\frac{d/p_i}{N(\mathfrak{p})}\right) = -1.$$

□

Definition 4.3.1. χ_i is called a genus character of $\mathbb{Q}[\sqrt{d}]$.

The following theorem is about the relation between genus characters.

Theorem 4.3.2. *Let the notation as above. We have*

$$\prod_{i=1}^{t} \chi_i = 1.$$

In other words, for any ideal I in O_K, we have

$$\prod_{i=1}^{n} \chi_i(I) = 1.$$

Proof. By definition, we only need to show that.

$$\prod_{i=1}^{n} \chi_i(\mathfrak{p}) = 1.$$

for any prime ideal $\mathfrak{p}$. Let $\mathfrak{p}$ be any prime ideal in O_K. If $N(\mathfrak{p})$ is a square then the equality is automatically valid. If $N(\mathfrak{p}) = p$ is not a square then either $\mathfrak{p}$ is ramified or splits completely. Suppose that $\mathfrak{p}$ splits completely then we have $\gcd(p, d) = 1$ and $\left(\frac{d}{p}\right) = 1$. By definition, we have

$$\chi_i(\mathfrak{p}) = \left(\frac{p_i}{p}\right).$$

And hence

$$\prod_{i=1}^{t} \left(\frac{d_i}{p}\right) = \left(\frac{d}{p}\right) = 1.$$

Suppose that $\mathfrak{p}$ is ramified. Then $p|d$, or equivalently there exists some i such that $p = |p_i|$. Hence by definition, for all $j \neq i$

$$\chi_j(\mathfrak{p}) = \left(\frac{p_i}{p}\right),$$

and for $i = j$, we have

$$\chi_i(\mathfrak{p}) = \left(\frac{d/p_i}{p}\right).$$

And hence

$$\prod_{j=1}^{t} \chi_j(\mathfrak{p}_j) = \left(\frac{d/p_i}{p}\right) \prod_{j \neq i} \left(\frac{p_i}{p}\right) = \left(\frac{(d/p_i)^2}{p}\right) = 1.$$

□

Let α be an element in O_K. We define $\chi(\alpha)$ to be $\chi(\alpha O_K)$. We also have an important observation

Lemma 4.3.1. *Let χ be the character described above and λ be a totally positive element in $\mathbb{Q}[\sqrt{d}]$. Then $\chi(\lambda) = 1$.*

Proof. See [6], chapter 2, page $52 - 53$. □

From this lemma, we conclude that we can define a group homomorphism from C_+ to $(\mathbb{Z}/2\mathbb{Z})^t$ in a natural way. More precisely, we can define

$$\chi : \quad C_+ \xrightarrow{\oplus \chi_i} (\mathbb{Z}/2\mathbb{Z})^t,$$

sending

$$[\mathfrak{p}] \mapsto (\chi_1(\mathfrak{p}), \ldots, \chi_t(\mathfrak{p}))$$

Remark 4.3.1. In our discussion, $\mathbb{Z}/2\mathbb{Z} = \{-1, 1\}$ and the binary operation is the multiplication. This group can also be equipped with a natural structure of a field with two elements. The multiplication table for this field is given by

+	1	-1
1	1	1
-1	1	-1

We have the following propositions.

Proposition 4.3.1. *The image of the map χ defined above is the set of all $(\epsilon_1, \dots, \epsilon_t)$ such that*

$$\prod_{i=1}^{t} \epsilon_i = 1.$$

In other words, if we regard $(\mathbb{Z}/2\mathbb{Z})^t$ as a vector space over $\mathbb{F}_2$ then the image of χ is the hypersurface $\prod_{i=1}^{n} X_i = 1$.

Proof. First of all, by theorem 4.3.2 the image of χ lies on the hypersurface $\prod_{i=1}^{n} X_i = 1$. Conversely, we will show that for any point in this hypersurface we can always find a class group whose image is that point. More precisely, we need to show that for any $(\epsilon_1, \dots, \epsilon_t)$ there always exists $\mathfrak{p}$ such that

$$\chi(\mathfrak{p}) = (\epsilon_1, \dots, \epsilon_t).$$

To do so, we can use Dirichlet's theorem on arithmetic progressions. The precise statement of Dirichlet's theorem is

Theorem 4.3.3 (Dirichlet, 1837)**.** *For any pairs (a, b) where $a > 0$ and $\gcd(a, b) = 1$. There are infinitely many prime numbers in the arithmetic progressions $an + b$ where $n \in \mathbb{N}$.*

Proof. See [10], chapter 6 for a proof. □

First of all, we show that we can always find a prime p such that

$$\left(\left(\frac{p_i}{p}\right), \dots, \left(\frac{p_t}{p}\right) \right) = (\epsilon_1, \dots, \epsilon_t).$$

here $\left(\frac{p}{q}\right)$ denotes the Legendre symbol. By the quadratic reciprocity law, for all odd prime discriminant it is easy to show that

$$\left(\frac{p_i}{p}\right) = \left(\frac{p}{|p_i|}\right).$$

Indeed, it is a consequence of the quadratic reciprocity law when $p_i > 0$ and $p_i \equiv 1 \pmod 4$. When $p_i = -q$ where $q \equiv -1 \pmod 4$, we have

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

We also know that the number of quadratic residues (as well as non quadratic residues) modulo q is $\frac{q-1}{2}$ when q is odd. Thus, for any $\epsilon \in \{1, -1\}$ there always exists $a \in \mathbb{Z}$ such that $\left(\frac{a}{q}\right) = \epsilon$.

In case p is an even prime discriminant, namely $-4, 8, -8$, we can also see that the Legendre symbol $\left(\frac{p_i}{p}\right)$ takes both values 1 and -1.

So in summary, for any ϵ_i we can always find some numbers p_i such that $\left(\frac{a_i}{p_i}\right) = \epsilon_i$. The existence of p is now a consequence of the Chinese Remainder theorem and Dirichlet's theorem on arithmetic progressions.

We now come back to our problem. We have seen that for any $(\epsilon_1, \dots, \epsilon_t)$, we can always find p such that

$$\left(\left(\frac{p_i}{p}\right), \dots, \left(\frac{p_t}{p}\right)\right) = (\epsilon_1, \dots, \epsilon_t).$$

Then we can easily see that

$$\left(\frac{d}{p}\right) = \prod_{i=1}^{t}\left(\frac{p_i}{p}\right) = \prod \epsilon_i = 1.$$

Therefore, p splits completely in O_K. Let $\mathfrak{p}$ be a prime ideal lying above p in O_K. Since $\mathfrak{p}$ splits completely, we have $N(\mathfrak{p}) = p$. By theorem 4.3.1, we obtain that

$$\chi(\mathfrak{p}) = \left(\left(\frac{p_1}{p}\right), \dots, \left(\frac{p_t}{p}\right)\right) = (\epsilon_1, \dots, \epsilon_t).$$

□

In addition, we also have

Proposition 4.3.2. *The kernel of the map* $\chi : \quad C_+ \xrightarrow{\oplus \chi_i} (\mathbb{Z}/2\mathbb{Z})^t$ *is* C_+^2.

So in particular, we have an isomorphism

$$C_+/C_+^2 \cong (\mathbb{Z}/2\mathbb{Z})^{t-1}.$$

Proof. First of all, we make the following observation. The map χ defined above can be interpreted as the composition of the following maps

$$\chi : \quad C_+ \xrightarrow{\text{Art}} \text{Gal}(K_+^1/K) \xrightarrow{\oplus\text{res}} \oplus \text{Gal}(F_i/K).$$

The Artin map is an isomorphism between C_+ and $\text{Gal}(K_+^1/K)$ and the res is just the restriction map from $\text{Gal}(K_+^1/K)$ to $\text{Gal}(F_i/K)$. Hence, in order to find the kernel of χ, it is sufficient to find the kernel of the second map

$$\text{Gal}(K_+^1/K) \xrightarrow{\oplus\text{res}} \bigoplus \text{Gal}(F_i/K).$$

By Galois theory, we know that the kernel of this map is the Galois group $\text{Gal}(K_+^1/F_1 \dots F_t) = \text{Gal}(K_+^1/K_{gen}^+)$. However, we know that $\text{Gal}(K_+^1/K_{gen}^+) = C_+^2$. It is then easy to see that $\ker(\chi) = C_+^2$. □

Let's denote by Δ the Galois group $\text{Gal}(K/\mathbb{Q})$. First, we observe that Δ acts on C_+ in a natural way. More specifically, let $[I]$ be some ideal class group, we define the action of Δ on $[I]$ by

$$\sigma([I]) = [\sigma(I)].$$

If we denote by σ the generator for Δ then from the relation

$$I\sigma(I) = N(I),$$

we see that σ acts on C_+ just like inversion.

Consider the following maps

$$\rho : \quad C_+[\sigma - 1] \xrightarrow{\text{inclusion}} C_+ \xrightarrow{\text{projection}} C_+/C_+^{\sigma-1}.$$

where $C_+[\sigma - 1]$ is the set of all ideal classes such that $(\sigma - 1)[\beta] = 1$, i.e $\sigma(\beta) = \beta$ and $C_+^{\sigma-1}$ is just the subgroup $(\sigma - 1)C_+$ of C_+. Since σ acts on C_+ just like the inversion, the group $C_+/C_+^{\sigma-1}$ is exactly C_+/C_+^2. Thus the map ρ can be considered as the map between two 2− elementary group and hence, a linear map over $\mathbb{F}_2$. We have the following very important proposition.

Proposition 4.3.3. *The* 4*-rank of the class group in the strict sense* C_+ *is exactly* $\dim_{\mathbb{F}_2}$ *ker*(ρ).

Proof. It is a straightforward proof. Suppose $x \in \ker\rho$. Then by definition, there exists $y \in C_+$ such that $x = (\sigma - 1)y$. However, we know that $(\sigma - 1)(x) = 1$ by definition of x. Hence, we have $(\sigma - 1)^2(y) = 1$. Since the above relation holds for every $x \in C_+$, we have

$$\ker(\rho) \subset \{(\sigma - 1)y | (\sigma - 1)^2 y = 1\}$$

. Conversely, suppose that y has properties that $(\sigma - 1)^2 y = 1$. Then by definition, $(\sigma - 1)y \in C_+[\sigma - 1]$. So we also have

$$\{(\sigma - 1)y | (\sigma - 1)^2 y = 1\} \subset \ker(\rho).$$

Hence, $\ker(\rho) = C_+^{\sigma-1}/C_+^{(\sigma-1)^2} = C_+^2/C_+^4$. It is then easy to see that the $4-$ rank of the class group in the strict sense C_+ is equal to $\dim_{\mathbb{F}_2}\ker(\rho)$. □

We need another lemma.

Lemma 4.3.2. $C_+[\sigma - 1]$ *is a vector space over* $\mathbb{F}_2$ *of dimension* $t - 1$ *and it is generated by the ideal classes* $[\mathfrak{p}_i]$ *where* $p_i = \mathfrak{p}_i{}^2$.

Proof. See [6], chapter 2. □

We can now compute the 4 rank of the class group in the strict sense. The idea is to find a surjective map from $(\mathbb{Z}/2\mathbb{Z})^t$ to $C_+[\sigma - 1]$. Regarding this fact, we define the first Redei map as follow

$$R: \quad \mathbb{F}_2^t \xrightarrow{\epsilon} C_+[\sigma - 1] \xrightarrow{\rho} C_+/C_+^{\sigma-1} \xrightarrow{\chi} \mathbb{F}_2^t.$$

Here take a basis $\{e_1, \ldots, e_t\}$ of $\mathbb{F}_2^t$ and define the map ϵ by

$$e_i \mapsto [\mathfrak{p}_i], \forall 1 \leq i \leq t.$$

For any L from a vector space V to a vector space W, we always have

$$V/\ker L \cong \mathrm{im} L.$$

So in particular, we have

$$\dim V = \dim \ker L + \dim \mathrm{im} L.$$

If we put $\mathrm{nul}L = \dim\ker L$ and $\mathrm{rank}L = \dim \mathrm{im}L$ then the above equality can be written as

$$\dim V = \mathrm{nul}L + \mathrm{rank}L.$$

We have

$$\mathrm{rank}R = \mathrm{rank}(\chi \circ \rho \circ \epsilon) = \mathrm{rank}(\chi \circ \rho).$$

The second equality comes from the fact that ϵ is surjective. Similarly, since χ is injective we have

$$\dim\ker(\chi \circ \rho) = \dim\ker(\rho).$$

By the above remark, we also have

$$\dim\ker(\chi \circ \rho) + \mathrm{rank}(\chi \circ \rho) = t - 1.$$

By these equality, we have

$$\dim\ker(\rho) + \mathrm{rank}(R) = t - 1.$$

or in other words

$$\dim\ker(\rho) = t - 1 - \mathrm{rank}(R).$$

We are now ready to compute the rank of rank(R). For simplicity, we will take the canonical basis of $\mathbb{F}_2^t$ as a basis. We can actually compute the matrix representation of R with respect to the two bases $\{e_1, \ldots, e_t\}$ and $\{f_1, \ldots, f_t\}$. Indeed, we have

$$R(e_j) = \chi([\mathfrak{p}_j]) = (\chi_1(\mathfrak{p}_j), \ldots, \chi_t(\mathfrak{p}_j)).$$

By definition, we have

$$\chi_i(\mathfrak{p}_j) = \left(\frac{p_j}{|p_i|}\right), \forall i \neq j.$$

However, since we are only concerned about the case where d has no prime divisor of form $4k + 3$ we have

$$\chi_i(\mathfrak{p}_j) = \left(\frac{p_i}{p_j}\right).$$

In addition, we also know that the map χ sends every element in C_+/C_+^2 to the hypersurface $\prod_{i=1}^t X_i = 1$, we can also compute the diagonal entries by the equality

$$\prod_j a_{ij} = 1.$$

Thus the matrix representation of R with respect to the two above bases is

$$R = \left(a_{ij}\right)_{1\leq i,j\leq n},$$

where

$$a_{ij} = \left(\frac{p_i}{p_j}\right), \forall i \neq j.$$

and

$$\prod_j a_{ij} = 1.$$

In summary, we have the following theorem.

Theorem 4.3.4 (Redei). *The* 4− *rank of the class group in the strict sense is equal to* $t - 1 - \mathrm{rank}(R)$ *where R is the $n \times n$ matrix with the ij entry being defined by*

$$a_{ij} = \left(\frac{p_i}{p_j}\right), \forall i \neq j.$$

and $a_{ii} = \prod_{j\neq i} a_{ij}$

For example in case $d = p_1p_2$ where both p_1 and p_2 are of the form $4k + 1$ and $\left(\frac{p_1}{p_2}\right) = -1$ then the Redei matrix is

$$\begin{pmatrix} -1 & -1 \\ -1 & -1 \end{pmatrix}$$

So the rank of this matrix is 1. Hence, the 4-rank of the class group in the strict sense is 0. The reason we are concerned the 4-rank is the following theorem.

Theorem 4.3.5. *If the* 4*-rank of the class group in the strict sense equals to* 0 *then the fundamental unit has negative norm.*

Proof. Since the 4-rank of C_+ is 0, the 2− Sylow subgroup of C_+ is of the form $(\mathbb{Z}/2\mathbb{Z})^{t-1}$. We also know that in our cases the genus class field and the genus class field in the strict sense of K are the same, so we have

$$C_+/C_+^2 = C/C^2.$$

Furthermore, we also already showed that C is a subgroup of C_+ of index at most 2. Hence $C = (\mathbb{Z}/2\mathbb{Z})^m$ for some m. The above equality immediately implies that $m = t-1$. Thus $C = C_+$. As we have pointed out, this information implies that the fundamental unit has negative norm. □

By the above theorem, we have the following corollaries.

Corollary 4.3.1. *Let $d = p_1p_2$ where p_1, p_2 are prime of form $4k+1$. Suppose that $\left(\frac{p_1}{p_2}\right) = -1$ then the fundamental unit of the number field of $K = \mathbb{Q}(\sqrt{d})$ has negative norm.*

In case $p_1 = 2$ and $p_2 \equiv 5 \pmod 8$ the above statement is also true.

Corollary 4.3.2. *Let $d = p_1p_2p_3$ where p_i are prime of form the $4k+1$ such that*

$$\left(\frac{p_1}{p_2}\right) = \left(\frac{p_1}{p_3}\right) = \left(\frac{p_2}{p_3}\right) = -1,$$

then the fundamental unit of $\mathbb{Q}[\sqrt{d}]$ has negative norm.

Proof. By theorem 4.3.4, the Redei matrix with respect to d is

$$\begin{pmatrix} 1 & -1 & -1 \\ -1 & 1 & -1 \\ -1 & -1 & 1 \end{pmatrix}$$

It is easy to see that this matrix has rank 2. Hence, the 4-rank of the class group in the strict sense is 0. Thus, the fundamental unit of $\mathbb{Q}[\sqrt{d}]$ has negative norm by theorem 4.3.5 □

Example 4.3.1. Let $d = 3145 = 5 \times 17 \times 37$. An explicit computation shows that the fundamental unit of this quadratic field is $x + y\omega$ where

$$x = 1320803827, y = 47959210, \omega = \frac{1+\sqrt{3145}}{2}.$$

This unit has negative norm.

The above theorem only gives us answers in case the 4− rank of the Redei matrix is 0. In many other cases, it is not enough to tell us about the signature of the fundamental unit. We will demonstrate it by another concrete example.

Example 4.3.2. In this example we will work with $d = 34$. We can see that in this case the 4-rank of the class group in the strict sense is 1 since the Redei matrix has rank 0. The fundamental unit in this case is $35 + 6\sqrt{34}$. A direct computation shows that it has norm 1.

In addition, the class group of O_K is $\mathbb{Z}/2\mathbb{Z}$. More precisely, the class group of O_K is generated by the ideal class $P_0 = [(3, \sqrt{34}+2)]$. We can easily show that

$$P_0^2 = (\sqrt{34}-5)^2.$$

So in the usual sense $[P_0]$ is of order 2. However, in the strict sense it is of order 4. Thus $C_+ = \mathbb{Z}/4\mathbb{Z}$. This can also be seen by the fact that the 4-rank is 1.

The above example shows that the knowledge of the 4 rank does not always provides us the answer about the signature of the fundamental unit. In order to investigate more, we need to find similar results for the higher rank.

The same idea applies here. In order to investigate the 8 rank, we can determine the kernel of the canonical map.

$$\mathrm{ker}\rho \longrightarrow C_+^{\sigma-1}/C_+^{(\sigma-1)^2}.$$

where ρ is the map we have defined before. By definition of ρ, we can see that the map we are looking for is

$$\ker(\rho) = C_+[\sigma - 1] \cap C_+^{\sigma-1} \longrightarrow C_+^{\sigma-1}/C_+^{(\sigma-1)^2}.$$

4.3.1 A construction for the $4-$ Hilbert Class Field

In the last section, we have determined the 4-rank of S based on the prime factorization of d. In case the 4-rank of S is 0, we already showed that the fundamental unit has negative norm. In this section, we will consider the case d is the product of two primes p_1, p_2 of the form $4k+1$ and the $4-$ rank of the C_+ is 1 (equivalently, each of p_1 and p_2 is a quadratic residue of the other). We will construct explicitly a $\mathbb{Z}/4\mathbb{Z}$ which is unramified over $K = \mathbb{Q}[\sqrt{p_1 p_2}]$. We begin with a theorem.

Theorem 4.3.6. *Let $K \subset L$ be a Galois extension of number fields. Suppose further that $L = K(\alpha)$ where $\alpha \in O_L$. Let $f(x)$ be the monic minimal polynomial of α over K. As $x \in O_L$, we can conclude that $f(x) \in O_K[X]$. If $\mathfrak{p}$ is a prime ideal O_K and $f(x)$ is separable modulo $\mathfrak{p}$ then*

1. *$\mathfrak{p}$ is unramified in L.*

2. *If $f = f_1 \dots f_g$ modulo $\mathfrak{p}$ where f_i are all irreducible then*

$$\mathfrak{p}O_L = \wp_1 \dots \wp_g,$$

where $\wp_i = \mathfrak{p}O_L + f_i(\alpha)O_L$ are prime ideals in O_L.

3. *$\mathfrak{p}$ splits completely if any only $f(x) \equiv 0 \pmod{\mathfrak{p}}$ has a solution in O_K.*

Proof. 1. Let us denote by $D_\wp$ the decomposition group of $\wp$. In other words,

$$D_\wp = \{\sigma \in \mathrm{Gal}(L/K) | \sigma(\wp) = \wp\}.$$

We know that $|D_\wp| = ef$ where e is the ramification index and f is the residue degree.

By our assumption, we have $0 = f(\alpha) = f_1(\alpha)\dots f_g(\alpha) \pmod{\mathfrak{p}O_K}$. As $\mathfrak{p} \subseteq \wp$, we have $f_1(\alpha)\dots f_g(\alpha) \equiv 0 \pmod{\wp}$. As $\wp$ is a prime ideal in O_K, there exists some i such that $f_i(\alpha)$ belongs to $\wp$. Without loss of generality, we may assume that $f_1(\alpha) \in \wp$.

With this assumption, it is easy to see that $f_1 \pmod{\mathfrak{p}}$ is the minimal polynomial of $\alpha + \wp$ over the finite field $O_K/\mathfrak{p}$. Galois theory tells us that

$$\deg(f_1) = [O_K/\mathfrak{p}[\alpha + \wp] : O_K/\mathfrak{p}] \leq [O_L/\wp : O_K/\mathfrak{p}] = f.$$

Besides, as $\wp$ is fixed by every $\sigma \in D_\wp$ we can conclude that $f_1(\sigma(\alpha)) \in \wp$ for any $\sigma \in D_\wp$. By definition, $\sigma(\alpha) + \wp$ is also a solution of f_1 in $O_L/\wp$ considered as a field extension of $O_K/\mathfrak{p}$. Since L/K is a Galois extension and $L = K(\alpha)$, we can conclude that $\{\tau(\alpha) | \tau \in \mathrm{Gal}\, L/K\}$ is the set of all roots of f. Suppose we number elements in this Galois group by $\{\sigma_1, \dots, \sigma_n\}$. Then the discriminant of f is

$$D = \prod_{1 \leq i < j \leq n} (\sigma_i(\alpha) - \sigma_j(\alpha))^2.$$

If $\sigma_i(\alpha) \equiv \sigma_j(\alpha) \pmod{\wp}$ then $D \in \wp$. Since $\mathfrak{p} = \wp \cap O_K$ and $D \in O_K$, we can conclude that $D \in \mathfrak{p}$. This would imply that f is not separable modulo $\mathfrak{p}$ which contradicts our assumption. Therefore, we showed that all the elements $\sigma(\alpha) + \wp$ are different in the field $O_L/\wp$ for $\sigma \in D_\wp$. Hence, these elements are roots of $f_1 \pmod{\mathfrak{p}}$. In particular, we have $\deg(f_1) \geq |D_\wp| = ef$. Combining with the fact that $\deg(f_1) \leq f$ we obtain $\deg(f_1) = f$ and $e = 1$. Thus, by definition, $\mathfrak{p}$ is unramified in L.

2. Suppose that $\mathfrak{p}\, O_L$ factors as
$$\mathfrak{p}\, O_L = \wp_1 \ldots \wp_h.$$
For each $i \in \{1, \ldots, h\}$ we have $f_1(\alpha) \ldots f_g(\alpha) \in \wp_i$. Since $\wp_i$ are all prime ideals, there must exist some $s(k)$ such that $f_{s(k)}(\alpha) \in \wp_i$. Moreover, such $s(k)$ is unique. Otherwise, for some i there exist j, k such that $f_j(\alpha), f_k(\alpha) \in \wp_i$. Since these two polynomial are relatively prime there exist g, h in $O_K/\,\mathfrak{p}$ such that
$$gf_i + hf_k = 1.$$
So in particular, $g(\alpha)f_i(\alpha) + h(\alpha)f_k(\alpha) = 1$ and hence $1 \in \wp_i$, which is impossible. Thus for each i the number $i(k)$ is unique. Consequently, the map s is a bijection. In particular, we have $g = h$. After rearrangement we can assume that $i = s(k)$. The argument at the beginning states that
$$\deg(f_1) = \ldots = \deg(f_g) = f.$$
For the final part, let denote $I_i = \mathfrak{p}\, O_L + f_i(\alpha)O_L$. We will show that $I_i = \wp_i$. First, since $f_i(\alpha) \in \wp_i$ and $\mathfrak{p}\, O_L \subset \wp_i$, we have $I_i \subset \wp_i$. We have the following observation.

Lemma 4.3.3. *Suppose $x, y \in O_L$. Then*
$$(\mathfrak{p}\, O_L + xO_L)(\mathfrak{p}\, O_L + yO_L) \subset \mathfrak{p}\, O_L + xyO_L.$$

Using this lemma, we have
$$I_1 \ldots I_g \subset \mathfrak{p}\, O_L + f_1(\alpha) \ldots f_g(\alpha)O_L = \mathfrak{p}\, O_L = \wp_1 \ldots \wp_g.$$
Combining with the fact that $I_i \subset \wp_i$ we can conclude that $I_i = \wp_i$.

3. This is just a direct consequence of part 2.

□

An immediate application of this theorem is the following proposition.

Proposition 4.3.4. *Let $L = K(\sqrt{\alpha})$ be an extension of number fields with $\alpha \in O_K$. Suppose $\mathfrak{p}$ is an ideal in O_K. Then we have the following*

1. *If $2\alpha \notin \mathfrak{p}$ then $\mathfrak{p}$ is unramified in L.*

2. *If $2 \in \mathfrak{p}$, $\alpha \notin \mathfrak{p}$ and there exist $b, c \in O_K$ such that $\alpha = b^2 - 4c$ then $\mathfrak{p}$ is also unramified in L.*

Proof. Since L/K is a Galois extension, we can apply theorem 4.3.6.

1. The minimal polynomial of α is $X^2 - \alpha$ which is easily seen to be separable modulo $\mathfrak{p}$. Therefore, $\mathfrak{p}$ is unramified over L.

2. Suppose that $\alpha = b^2 - 4c$. Let $\mu = \frac{b+\sqrt{\alpha}}{2}$ then μ is a root of
$$X^2 - bX + c.$$
Since $b, c \in O_K$, we know that $\mu \in O_K$. Moreover, we can easily see that $L = K(\mu)$.
The discriminant of this polynomial is α which is not in $\mathfrak{p}$. Hence $X^2 - bX + c$ is separable modulo $\mathfrak{p}$. By theorem 4.3.6, we conclude that $\mathfrak{p}$ is unramified in L.

□

Proposition 4.3.5. *Suppose p_1, p_2 are two prime numbers of the form $4k+1$ such that $\left(\frac{p_1}{p_2}\right) = 1$. Then there exists $(x, y, z) \in \mathbb{Z}^3$ such that*

$$x^2 - p_1 y^2 - p_2 z^2 = 0.$$

Furthermore, we can choose (x, y, z) in such way that the following conditions are satisfied.

1. *$x, p_1 y, p_2 z$ are pairwisely relatively prime.*

2. *x, z are odd and y is even.*

3. *$x + y \equiv 1 \pmod 4$.*

Proof. By Hasse-Minkowski principle, there exist rational numbers x, y, z such that

$$x^2 - p_1 y^2 - p_2 z^2 = 0,$$

Multiply these numbers with the least common multiple of their denominators we can assume that $\gcd(x, p_1 y) = 1$. It is then easy to observe that

$$\gcd(x, p_1 y) = \gcd(x, p_2 z) = \gcd(p_1 y, p_2 z) = 1.$$

The first part is therefore valid.

We can observe that exactly one of the numbers x, y, z can be even simply by looking modulo 8. Moreover, by considering modulo 4 we can show that x must be odd. Without loss of generality, we can assume that y is even and z is odd (otherwise we interchange the role of y and z).

Finally, we see that since x is odd, $x + y$ and $-x + y$ have different values with respect to modulo 4. Since these numbers are both odd, exactly one of them is congruent to 1 modulo 4. By interchanging the role of x and $-x$ if necessary, we can assume that $x + y \equiv 1 \pmod 4$. □

Let us denote by $H^1 = \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2})$ the genus class field of $K = \mathbb{Q}(\sqrt{p_1 p_2})$. Let $\alpha = x + y\sqrt{p_1}$, $\beta = 2(x + \sqrt{p_2} z)$. We have the following claim.

Proposition 4.3.6. *With the above notations, we have*

$$H^1(\sqrt{\alpha}) = H^1(\sqrt{\beta}).$$

Proof. It is sufficient to show that $\alpha\dot{\beta}$ is a square in H^1. First, we have

$$(y\sqrt{p_1} + z\sqrt{p_2})^2 = p_1 y^2 + p_2 z^2 + 2\sqrt{p_1 p_2} yz = x^2 + 2\sqrt{p_1 p_2} yz.$$

Hence, we have

$$2\sqrt{p_1 p_2} yz = (y\sqrt{p_1} + z\sqrt{p_2})^2 - x^2.$$

Consequently, we have

$$\alpha\beta = (x + y\sqrt{p_1 y})(2x + 2\sqrt{p_2} z) = 2x^2 + 2x(y\sqrt{p_1} + z\sqrt{p_2}) + 2yz\sqrt{p_1 p_2}.$$

By substituting $2yz\sqrt{p_1 p_2}$ by $(y\sqrt{p_1} + z\sqrt{p_2})^2 - x^2$, we get

$$\alpha\beta = x^2 + 2x((y\sqrt{p_1} + z\sqrt{p_2}) + (y\sqrt{p_1} + z\sqrt{p_2})^2 = (x + y\sqrt{p_1} + z\sqrt{p_2})^2.$$

Thus $\alpha\beta$ is a square in H^1. As we have noted, it simply implies that

$$H^1(\sqrt{\alpha}) = H^1(\sqrt{\beta}).$$

□

We have the following theorem.

Theorem 4.3.7. *The extension $H^1(\alpha)$ is unramified over H^1 and hence unramified over K.*

Proof. We have already showed that the genus class field H^1 is unramified over K. Thus in order to show that $H = H^1(\sqrt{\alpha})$ is unramified over K, it is sufficient to show that it is unramified over H^1. To do this we will make use of theorem 4.3.6 and proposition 4.3.4.

Let $\mathfrak{p}$ be any prime ideal in O_{H^1}. We will show that $\mathfrak{p}$ is unramified over H^1. First, we note that the ideal generated by 2 and $x + y\sqrt{p_1}$ is the whole number rings O_{H^1}. This is because x is odd and y is even. We consider the following cases.

Case 1. $2\alpha \notin \mathfrak{p}$. By proposition 4.3.4, we know that p is unramified over H^1.

Case 2. $2 \in \mathfrak{p}$ but $\alpha \notin \mathfrak{p}$. We need to show that there exist $b, c \in O_{H^1}$ such that

$$\alpha = b^2 - 4c.$$

It is equivalent to the fact that the equation

$$X^2 \equiv \alpha \pmod{4O_{H^1}}, \tag{4.1}$$

is solvable. We consider two subcases.

Case 2.1. $x \equiv 1 \pmod 4$. Then we have $y \equiv 0 \pmod 4$. The equation 4.1 is therefore equivalent to

$$X^2 \equiv 1 \pmod{4O_{H^1}}.$$

This equation has $X = 1$ as a solution.

Case 2.2. $x \equiv 3 \pmod 4$. Then $y \equiv 2 \pmod 4$. Let $a = \frac{x-1}{2}, b = \frac{y}{2}$ then both a, b are odd. We know that if $a \equiv b \equiv 1 \pmod 2$ then $a + b\sqrt{p_1} \in O_{\mathbb{Q}(\sqrt{p_1})}$. Since $O_{\mathbb{Q}(\sqrt{p_1})} \subset O_{H^1}$, we must have $a + b\sqrt{p_1} \in O_{H^1}$. Combining these facts, we can conclude that $x - 1 + y\sqrt{p_1} \equiv 0 \pmod{4O_{H^1}}$. Thus $X = 1$ is also a solution of 4.1.

Case 3. $2 \notin \mathfrak{p}$ but $\alpha \in \mathfrak{p}$. If $x + z\sqrt{p_2} \notin \mathfrak{p}$ then the same argument shows that $\mathfrak{p}$ is unramfied over $H^1(\sqrt{2\beta})$. However, we know that $H^1(\sqrt{\alpha}) = H^1(\sqrt{2\beta})$. Thus $\mathfrak{p}$ is unramified over H. Suppose that $x + z\sqrt{p_2} \in \mathfrak{p}$. Then we have both elements $(x + y\sqrt{p_1})(x - y\sqrt{p_1}) = p_2z^2$ and $(x + \sqrt{p_2}z)(x - \sqrt{p_2}z) = p_1y^2$ are in $\mathfrak{p}$. However, since these elements are relatively prime, this happens only when $\mathfrak{p} = O_{H^1}$, which is impossible.

Thus in any cases, we always have $\mathfrak{p}$ being unramified over the extension $H^1(\sqrt{\alpha})/H^1$. □

We also have the following theorem.

Theorem 4.3.8. *$H^1(\sqrt{\alpha})$ is a Galois extension of K with Galois group being equal to $\mathbb{Z}/4$.*

Proof. This is rather obvious. □

By the 4− rank theorem that we discussed before, the 4− rank of the quadratic number field $\mathbb{Q}(\sqrt{p_1p_2})$ with $p_1 \equiv p_2 \equiv 1 \pmod 4$ and $\left(\frac{p_1}{p_2}\right) = 1$ is 1. The above theorems help us construct explicitly this the 4− Hilbert Class Field (in the strict sense) of the number field K. In conclusion, we have the following theorem

Theorem 4.3.9. *Let p_1, p_2 be two primes of the form $4k+1$ such that $\left(\frac{p_1}{p_2}\right) = 1$. Then the 4 rank of the class group in the strict sense is 1. The corresponding 4− strict Hilbert Class Field is given by*

$$H = H^1\left(\sqrt{x + y\sqrt{p_1}}\right),$$

where H^1 is the genus class field of K and x, y are given in proposition 4.3.5.

4.3.2 The 8 rank of the Hilbert Class Field in the strict sense

We can go further to find the 8 rank of the class group in the strict sense. Before going on, we give a definition.

Definition 4.3.2. Let p be an odd prime of the form $4k+1$ and a be an integer. We define

$$[a,p]_4 = \begin{cases} 1 & \text{if } \left(\frac{a}{p}\right) = 1, \text{ and } a \text{ is a fourth power modulo p} \\ -1 & \text{if } \left(\frac{a}{p}\right) = 1, \text{ and } a \text{ is not a fourth power modulo p} \\ 0 & \text{ifotherwise.} \end{cases}$$

Remark 4.3.2. This concept is different from the concept generalized Legendre symbols (see [4.3.3]). The reason is that the field H^1 does not contain a 4 primitive root of 1. The above symbol simply tells us when a is a fourth power modulo p.

Example 4.3.3. Let's consider the case $a = 5$ and $p = 29$. We know that 29 is a quadratic modulo 5. The two solutions of the equation

$$X^2 \equiv 29 \pmod 5,$$

are $X = 2 \pmod 5$ and $X = 3 \pmod 5$. We can easily see that $2, 3$ are not quadratic residue modulo 5 and therefore the equation

$$X^4 \equiv 29 \pmod 5,$$

is not solvable. Thus, we have $[29, 5]_4 = -1$.

We recall a method we use to find the 8-rank of the Class Group in the strict sense. The 8-rank is the dimension over $\mathbb{F}_2$ of the kernel of the following Redei map

$$R_2 : C_+[\sigma - 1] \cap C_+^{\sigma-1} \longrightarrow C_+^{\sigma-1}/C_+^{(\sigma-1)^2} \cong \mathrm{Gal}(H/H^1). \tag{4.2}$$

We do know that $C_+[\sigma-1] \cap C_+^{\sigma-1}$ is of dimension 1 over $\mathbb{F}_2$ in case $\left(\frac{p_1}{p_2}\right) = 1$. Therefore the 8 rank is equal to 0 if this map is not trivial and equal to 1 otherwise.

Let $\mathfrak{p}_i$ be any prime ideals in O_{H^1} lying above p_1 and p_2 respectively. The second map is just the Artin map over the field extension H/H^1 of degree 2. Therefore, the Artin symbol associated with $\mathfrak{p}_i$ is non-trivial if and only if $\mathfrak{p}_i$ is inert and it is trivial if and only if $\mathfrak{p}_i$ splits completely. To investigate whether $\mathfrak{p}_i$ is inert or splits completely, we will make use of the generalized Lengendre symbols.

Generalized Legendre symbols

We first start with a field number field K containing a n primitive root of 1, say ζ. Let $a \in O_K$ and $\mathfrak{p}$ be a prime ideal in O_K such that $na \notin \mathfrak{p}$. Then we have the following proposition.

Proposition 4.3.7. *Let the notations be defined as above. Then*

1. $n | N(\mathfrak{p}) - 1$.

2. $a^{\frac{N(p)-1}{N}}$ *is congruent to a unique root of unity modulo* $\mathfrak{p}$.

Proof. 1. First, we note that the polynomial $f = x^n - 1$ is separable modulo $\mathfrak{p}$. This is because in $O_K/p[x]$ we have

$$\gcd(f(x), f'(x)) = \gcd(x^n - 1, nx^{n-1}) = 1.$$

In addition, we have $f(1) = f(\zeta) = \ldots = f(\zeta^{n-1}) = 0$, so $1, \zeta, \ldots, \zeta^{n-1}$ are roots of $f \pmod{\mathfrak{p}}$. They are all different because $f \pmod{\mathfrak{p}}$ is separable. Since $\{1, \zeta, \ldots, \zeta^{n-1}\}$ is a subgroup of the multiplicative group $(O_k/\mathfrak{p})^\times$ and the order of the multiplicative group $(O_K/\mathfrak{p})^\times$ is $N(\mathfrak{p}) - 1$, Lagrange theorem tells us that $n | N(\mathfrak{p}) - 1$

2. For any $a \notin \mathfrak{p}$, by Lagrange theorem, we have

$$a^{N(p)-1} \equiv 1 \pmod{\mathfrak{p}}.$$

We can rewrite this equality in the form

$$\prod_{i=1}^{n} (a^{\frac{N(p)-1}{n}} - \zeta^i) \equiv 0 \pmod{\mathfrak{p}}.$$

Since $\mathfrak{p}$ is a prime ideal, one of those factors $a^{\frac{N(p)-1}{n}} - \zeta^i$ must lie on $\mathfrak{p}$. In other words, there exists i such that

$$a^{\frac{N(p)-1}{n}} \equiv \zeta^i \pmod{\mathfrak{p}}.$$

In part a, we already showed that ζ^i are all different modulo $\mathfrak{p}$ for $i \in \{1, \ldots, n-1\}$, this guarantees the uniqueness of i.

□

With this proposition, we have the following definition.

Definition 4.3.3. We define $\left(\frac{a}{\mathfrak{p}}\right)_n$ as the unique root of unity in O_K such that

$$a^{\frac{N(p)-1}{n}} \equiv \left(\frac{a}{\mathfrak{p}}\right)_n \pmod{\mathfrak{p}}.$$

We note that when $n = 2$ we have the familiar Legendre symbol. Moreover, similar to the Legendre symbol the generalized one also has the following property.

Proposition 4.3.8. $\left(\frac{a}{\mathfrak{p}}\right) = 1$ *if and only if a is an n^{th} power modulo* $\mathfrak{p}$.

Proof. This proposition can be proved by using the fact that the multiplicative group $(O_K/\mathfrak{p})^\times$ is cyclic.

□

Our second theorem states that the Legendre symbol defined above relates to the Artin symbol of $\mathfrak{p}$ in some certain extension in a very elegant manner. More precisely, we have the following.

Theorem 4.3.10. *Let $K, n, a, \mathfrak{p}$ be defined as above and let $L = K(\sqrt[n]{a})$. Then we have the following*

1. *$\mathfrak{p}$ is unramified in L.*
2. *Let us denote by $\left(\frac{L/K}{\mathfrak{p}}\right)$ the Artin symbol of $\mathfrak{p}$ (this is defined because $\mathfrak{p}$ is unramified according to part (a)). Then*

$$\left(\frac{L/K}{\mathfrak{p}}\right) \sqrt[n]{a} = \left(\frac{a}{\mathfrak{p}}\right)_n \sqrt[n]{a}.$$

Proof. 1. First, we will show that $f(x) = x^n - a$ is separable modulo $\mathfrak{p}$. Indeed, since $na \notin \mathfrak{p}$, we have

$$\gcd(\overline{f(x)}, \overline{f'(x)}) = \gcd(\overline{x^n - a}, \overline{nx^{n-1}}) = 1,$$

where $\overline{f}, \overline{f'}$ is the reduction of f and f' modulo $\mathfrak{p}$. By theorem (1), we can conclude that $\mathfrak{p}$ is unramified.

2. For simplicity let us denote by $\sigma = \left(\frac{L/K}{\mathfrak{p}}\right)$ and by $\wp$ some prime ideal in O_L lying above $\mathfrak{p}$. Then σ is characterized by the property

$$\sigma(x) \equiv x^{N(\mathfrak{p})} \pmod{\wp O_L}, \forall x \in O_L.$$

So in particular, for $x = \sqrt[n]{a}$, we have

$$\sigma(\sqrt[n]{a}) \equiv a^{\frac{N(\mathfrak{p})-1}{n}} \sqrt[n]{a} \pmod{\wp}. \tag{4.3}$$

By definition, we have

$$a^{\frac{N(\mathfrak{p})-1}{n}} \equiv \left(\frac{a}{\mathfrak{p}}\right)_n \pmod{\mathfrak{p}}.$$

However, we do know that $\mathfrak{p} \subset \wp$ so

$$a^{\frac{N(\mathfrak{p})-1}{n}} \equiv \left(\frac{a}{\mathfrak{p}}\right)_n \pmod{\wp}.$$

So the quality (1) can be rewritten as

$$\sigma(\sqrt[n]{a}) \equiv \left(\frac{a}{\mathfrak{p}}\right)_n \sqrt[n]{a} \pmod{\wp}.$$

We know that L is the splitting field of $X^n - a$ over K so every element in $\mathrm{Gal}(L/K)$ sends $\sqrt[n]{a}$ to one of its conjugates, namely $\{\sqrt[n]{a}, \zeta\sqrt[n]{a}, \dots, \zeta^{n-1}\sqrt[n]{a}\}$. Therefore, in order to show that

$$\sigma\sqrt[n]{a} = \left(\frac{a}{\mathfrak{p}}\right)_n \sqrt[n]{a},$$

it is sufficient to prove that $\{\sqrt[n]{a}, \zeta\sqrt[n]{a}, \dots, \zeta^{n-1}\sqrt[n]{a}\}$ are all different modulo $\wp$. Equivalently, we have to show that the polynomial $X^n - a$ is separable modulo $\wp$. Suppose to the contrary that $X^n - a$ is not separable modulo $\wp$. Then we must have

$$\gcd(f, f') = \gcd(X^n - a, nX^{n-1}) = 0.$$

This happens only when $n \in \wp$. However, we do know that $\mathfrak{p} \cap \mathbb{Z}$ and $\wp \cap \mathbb{Z}$ are prime ideals in $\mathbb{Z}$ and they are non-zero. Besides, since $\mathfrak{p} \cap \mathbb{Z} \subseteq \wp \cap \mathbb{Z}$, we can conclude that $\mathfrak{p} \cap \mathbb{Z} = \wp \cap \mathbb{Z}$. This would imply that $n \in \mathfrak{p}$, which contradicts our assumption. Thus $X^n - a$ is separable modulo $\wp$ and we have the above conclusion.

□

Application of generalized Legendre symbols to our problem

We come back to our problem. First, we have the following field extensions

$$\mathbb{Q} \subset K \subset H^1 \subset H$$

where $K = \mathbb{Q}(\sqrt{p_1 p_2})$, $H^1 = \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2})$ and $H = H^1(\alpha)$.

For each $i \in \{1, 2\}$, we have the corresponding prime ideals with this extension

$$p_i \subset P_i \subset \mathfrak{p}_i \subset \wp_i.$$

$$\begin{tikzcd}
H \arrow[d, dash] & \wp_i \arrow[d, dash] \\
H^1 \arrow[d, dash] & \mathfrak{p}_i \arrow[d, dash] \\
K \arrow[d, dash] & P_i \arrow[d, dash] \\
\mathbb{Q} & p_i
\end{tikzcd}$$

More precisely, we have

$$p_iO_K = P_i^2O_K, P_iO_{H^1} = \mathfrak{p}_{1i}\,\mathfrak{p}_{2i}\,O_{H^1}.$$

Thus the prime ideal P_i splits completely (inert) in H if and only if both $\mathfrak{p}_{1i}$ and $\mathfrak{p}_{2i}$ split completely (inert) in H. Since H/H^1 is a Galois extension this condition is equivalent to $\mathfrak{p}_{1i}$ splitting completely (inert) in H_2. For simplicity we will denote $\mathfrak{p}_{1i}$ by $\mathfrak{p}_i$. We also see that H^1 contains a 2 primitive root of 1, namely -1. Therefore, one way to investigate the ramification of p_i over the extension H/H^1 is to compute the generalized Legendre symbol $\left(\frac{x+y\sqrt{p_1}}{\mathfrak{p}_1}\right)_2$ and $\left(\frac{2x+2z\sqrt{p_1}}{\mathfrak{p}_2}\right)_2$

This computation will become easier if we apply the following theorem (which is usually called **The Translation Theorem**.)

Definition 4.3.4 (**The norm map**). Let $K \subset L$ be extension of number fields. We denote by $A = O_K$ and by $B = O_L$. For any prime $\mathfrak{q}$ in B we define

$$N(A) = \mathfrak{p}^f,$$

where $\mathfrak{p}$ is the prime in B lying below $\mathfrak{q}$ and f is the residue degree $[B/\mathfrak{q} : A/\,\mathfrak{p}]$

We have the following important theorem.

Theorem 4.3.11. *Let L/K be a finite extension of number fields. Suppose further that K contains a $n-$ root of unity. Let $\alpha \in K^\times$, $\mathfrak{p}$ be a prime ideal in O_K such that $\mathfrak{p}$ is relatively prime to α and n. Let $\wp$ be some prime ideal in O_L lying above $\mathfrak{p}$. Then we have*

$$\left(\frac{\alpha}{\wp}\right)_{L,n} = \left(\frac{\alpha}{N_{L/K}(\wp)}\right)_{K,n}.$$

Proof. See [14], page $19 - 20$. □

We can apply this theorem for $L = H^1$ and $K_1 = K = \mathbb{Q}(\sqrt{p_1})$ (and $K_2 = \mathbb{Q}(\sqrt{p_2})$). Let ϱ_1 be the ideal in O_{K_1} which lies below $\mathfrak{p}_1$. We have the following diagram

$$\begin{tikzcd}
& H^1 \arrow[dl, dash] \arrow[d, dash] & & \wp_1 \arrow[dl, dash] \arrow[d, dash] \\
K_1 \arrow[dr, dash] & K \arrow[d, dash] & \varrho_1 \arrow[dr, dash] & P_1 \arrow[d, dash] \\
& \mathbb{Q} & & p_1
\end{tikzcd}$$

Looking at this diagram, we can easily see that ϱ_1 splits completely in O_{H_1}. By applying the translation theorem, we get

$$\left(\frac{x+y\sqrt{p_1}}{\mathfrak{p}_1}\right)_{H^1,2} = \left(\frac{x+y\sqrt{p_1}}{\varrho_1}\right)_{K_1,2}.$$

However, since $\sqrt{p_1} \in \varrho_1$ we have

$$\left(\frac{x+y\sqrt{p_1}}{\varrho_1}\right)_{K_1,2} = \left(\frac{x}{\varrho_1}\right)_{K_1,2}.$$

Similarly, for p_2 we have

$$\left(\frac{2x+2z\sqrt{p_2}}{\varrho_2}\right)_{K_2,2} = \left(\frac{2x}{\varrho_2}\right)_{K_2,2}.$$

We have the following claim.

Proposition 4.3.9. *With the above notations, we have*

$$\left(\frac{x}{\varrho_1}\right)_{K_1,2} = \left(\frac{x}{p_1}\right),$$

and

$$\left(\frac{2x}{\varrho_2}\right)_{K_2,2} = \left(\frac{2x}{p_2}\right),$$

where the second symbol is just the usual Legendre symbol.

Proof. We only give a proof for the first equality. The second one can be derived in the same manner.

Suppose that $\left(\frac{x}{\varrho_1}\right)_{K_1,2} = 1$. Then by definition, there exist $a, b \in \mathbb{Z}$ such that

$$\left(\frac{a+b\sqrt{p_1}}{2}\right)^2 \equiv x \pmod{\varrho_1}.$$

Since $2 \notin \varrho_1$, the above equation is equivalent to

$$(a+b\sqrt{p_1})^2 \equiv 4x \pmod{\varrho_1}.$$

Furthermore, since $\sqrt{p_1} \in \varrho_1$, this equation is equivalent to

$$a^2 \equiv 4x \pmod{\varrho_1}.$$

Since both a, x are integers, the above relation implies that

$$a^2 \equiv 4x \pmod{p_1}.$$

In other words, x must be a quadratic residue modulo p. Thus, if $\left(\frac{x}{\varrho_1}\right)_{K_1,2} = 1$ then we also have $\left(\frac{x}{\varrho_1}\right) = 1$.

Conversely, if $\left(\frac{x}{p_1}\right) = 1$ we can see that there exists $a \in \mathbb{Z}$ such that $a^2 \equiv x \pmod{p_1}$. Since $p_1 \subset \varrho_1$, we can conclude that

$$a^2 \equiv x \pmod{\varrho_1}.$$

By definition, we have

$$\left(\frac{x}{\varrho_1}\right)_{K_1,2} = 1.$$

Combining these arguments, we can conclude that

$$\left(\frac{x}{\varrho_1}\right)_{K_1,2} = \left(\frac{x}{p_1}\right),$$

□

To compute these symbols, we will use the well-known Jacobi symbol. We recall the definition of Jacobi symbol.

Definition 4.3.5. Let a, n be integers and $n > 0$. We define

$$\left(\frac{a}{n}\right) = \prod_{i=1}^{r} \left(\frac{a}{p_1}\right)^{e_i},$$

where $n = \prod_{i=1}^{r} p_i^{e_i}$ is the factorization of n and $\left(\frac{a}{p_i}\right)$ is the familiar Legendre symbol.

This symbol shares many common properties with the familiar Legendre symbol. We list here some of these properties that we will use throughout the rest of this section. Proofs can be found in any elementary number theory book.

Proposition 4.3.10. *[Properties of Jacobi Symbol]*

1. *If m, n are odd, coprime integers then*

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}.$$

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

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

Before coming to the final result that we want to discuss, we have the following important lemma. This lemma is discussed in [28].

Lemma 4.3.4. *Let x, y, z be the solution described in* 4.3.5*. Moreover, we can also assume that $y, z > 0$. Suppose that $y = 2^j u$ where u is odd. Then we have*

1. $\left(\frac{z}{p_1}\right) = \left(\frac{p_1}{z}\right) = 1$.

2. $\left(\frac{u}{p_2}\right) = \left(\frac{p_2}{u}\right) = 1$.

3. $\left(\frac{|x|}{p_1}\right) = [p_2, p_1]_4$.

4. $\left(\frac{|x|}{p_2}\right) = [p_1, p_2]_4 \left(\frac{y}{p_2}\right)$.

5. $\left(\frac{2|x|}{p_2}\right) = [p_1, p_2]_4$.

6. $\left(\frac{p_1 p_2}{|x|}\right) = \left(\frac{-1}{|x|}\right)$.

Proof.

1. For any prime divisor of z we see that
$$x^2 \equiv p_1 y^2 \pmod{p}.$$
Therefore, p_1 is a quadratic residue modulo p. By definition of Jacobi symbol, $\left(\frac{p_1}{z}\right) = 1$. In addition, by proposition 4.3.10, we have
$$\left(\frac{z}{p_1}\right) = \left(\frac{p_1}{z}\right) = 1.$$

2. Almost similar to part 1.

3. From the relation, we have
$$x^2 \equiv p_1 z^2 \pmod{p_2}.$$
This implies that
$$\left(\frac{x}{p_1}\right) = [p_2, p_1]_4 \left(\frac{z}{p_1}\right) = [p_2, p_1]_4.$$
Since -1 is a quadratic residue modulo p_1, we have
$$\left(\frac{|x|}{p_1}\right) = \left(\frac{x}{p_1}\right) = [p_2, p_1]_4.$$

4. Almost similar to part 3.

5. From part 4 and part 2, we have
$$\left(\frac{|x|}{p_2}\right) = [p_1, p_2]_4 \left(\frac{y}{p_2}\right) = [p_1, p_2]_4 \left(\frac{2}{p_2}\right)^j.$$
If $j = 1$ then we can easily see that $p_2 \equiv 5 \pmod{8}$. Otherwise if $j > 1$ then $p_2 \equiv 1 \pmod{8}$. We divide our proof into two cases.

   Case 1. $j = 1$

   Then we have
$$\left(\frac{|x|}{p_2}\right) = [p_1, p_2]_4 \left(\frac{2}{p_2}\right),$$
and therefore
$$\left(\frac{2x}{p_2}\right) = [p_1, p_2]_4.$$

   Case 2. $j \geq 2$.

   Then $p_2 \equiv 1 \pmod{8}$ and therefore
$$\left(\frac{2}{p_2}\right) = 1.$$
Using this equality, we get
$$\left(\frac{2x}{p_2}\right) = [p_1, p_2]_4.$$

6. For any prime $q||x|$,we have

$$p_1y^2 + p_2z^2 \equiv 0 \pmod q.$$

Thus $-p_1p_2$ is a quadratic residue modulo q. By the definition of Jacobi symbol, we have

$$\left(\frac{-p_1p_2}{|x|}\right) = 1.$$

By the multiplicativity of the Jacobi symbol, we have

$$\left(\frac{p_1p_2}{|x|}\right) = \left(\frac{-1}{|x|}\right).$$

□

We can now come to an important result about the 8 rank of the class group in the strict sense.

Theorem 4.3.12. *Let p_1 and p_2 be two primes of the form $4k+1$ such that $\left(\frac{p_1}{p_2}\right) = 1$. Then we have the following*

1. *If $[p_1, p_2]_4 = -1$ or $[p_2, p_1]_4 = -1$ then the 8 rank of the class group in the strict sense is 0.*
2. *If $[p_1, p_2]_4 = [p_2, p_1]_4 = 1$ then the $8-$ rank is 1.*

Proof. We divide our proof into 2 cases.

Case 1. $[p_1, p_2]_4 = [p_2, p_1]_4 = 1$. Apply lemma 4.3.4, we have

$$\left(\frac{x}{p_1}\right) = \left(\frac{2x}{p_1}\right) = 1.$$

Thus, both $\mathfrak{p}_i$ split completely over H or in other words, the Redei map defined in 4.2 is the zero map. As we pointed out the dimension over $\mathbb{F}_2$ of the kernel of R_2 is 1. Consequently, the 8-rank of the class group in the strict sense is 1.

Case 2. If $[p_1, p_2]_4 = -1$ or $[p_2, p_1]_4 = -1$ then at least one of the two symbols $\left(\frac{x}{p_1}\right)$, $\left(\frac{2x}{p_1}\right)$ must be -1. As we have pointed out, this simply implies that the Redei map is not the zero map. Thus the kernel of R_2 has dimension 0 over $\mathbb{F}_2$. In other words, the $8-$ rank is 0.

□

Thus, we have completely understood the 8-rank of the class group in the strict sense. In case this 8-rank is 0 we can say more about the signature of the fundamental unit of $K = \mathbb{Q}(\sqrt{p_1p_2})$. Indeed, we have the proposition (which has been stated in 3.3.3).

Theorem 4.3.13. *Suppose p_1, p_2 are two primes of the form $4k+1$ and $\left(\frac{p_1}{p_2}\right) = 1$. Suppose further that the 8- rank of class group in the strict sense of the number field $K = \mathbb{Q}(\sqrt{p_1p_2})$ is 0. Let H be the field defined in 4.3.9. We have the following conclusions*

1. *$H = H_2^+$.*
2. *The fundamental unit has negative norm if and only if H is totally real.*

Proof. Since the 4 and 8 rank of the class group in the strict sense is 0 and the 1 respectively, we can easily see that $S_+ \cong \mathbb{Z}/4\mathbb{Z}$. In addition, we also know that H/K is a $\mathbb{Z}/4\mathbb{Z}$ unramified extension extension. Hence, we must have $H = H_+^2$. The second statement is a direct consequence of theorem 3.3.3. □

4.3.3 When is H totally real?

We have the following theorem.

Theorem 4.3.14. *H is totally real if and only if $[p_1, p_2]_4[p_2, p_1]_4 = 1$.*

Proof. First, we observe that $H^1(\alpha) = H^1(\gamma)$ where $\gamma = x - y\sqrt{p_1}$. Thus H is totally real if and only if $\alpha > 0$ and $\beta > 0$. This is equivalent to $x > 0$. Thus, our question turns out to be: when x is positive?

From lemma 4.3.4 have

$$[p_1, p_2]_4[p_2, p_1]_4 = \left(\frac{|x|}{p_1}\right)\left(\frac{2|x|}{p_2}\right) = \left(\frac{2}{p_1}\right)\left(\frac{|x|}{p_1 p_2}\right) = \left(\frac{2}{p_1}\right)\left(\frac{-1}{|x|}\right)$$

However, we do know that if $j = 1$ then $p_1 \equiv 5 \pmod 8$ and if $j \geq 2$ then $p_1 \equiv 1 \pmod 8$. Thus, we can easily see that

$$\left(\frac{2}{p_1}\right) = (-1)^{\frac{y}{2}}.$$

We also have

$$\left(\frac{-1}{|x|}\right) = (-1)^{\frac{|x|-1}{2}}.$$

Combining these two facts, we get

$$[p_1, p_2]_4[p_2, p_1]_4 = (-1)^{\frac{|x|+y-1}{2}}.$$

Since $x + y - 1 \equiv 0 \pmod 4$, $(-1)^{\frac{|x|+y-1}{2}} = 1$ if and only if $x > 0$.

□

Together with the main result 4.3.12, we have the following theorem.

Theorem 4.3.15. *Let p_1 and p_2 be two primes of the form $4k + 1$ such that $\left(\frac{p_1}{p_2}\right) = 1$. Then we have the following claims*

1. *If $[p_1, p_2]_4 = [p_2, p_1]_4 = -1$ then the 8 rank is 0, the Hilbert Class Field is totally real, the fundamental unit has negative norm.*

2. *If $[p_1, p_2]_4 = -[p_2, p_1]_4$ then the 8 rank is 0, the Hilbert Class Field is totally complex, the fundamental unit has positive norm.*

3. *If $[p_1, p_2]_4 = [p_2, p_1]_4 = 1$ then the 8 rank is 1 and H is totally real.*

Chapter 5

Future intentions

In this chapter, we propose an approach to tackle our problem in case d is the product of two primes p_1, p_2 of the form $4k+1$ such that $[p_1, p_2]_4 = [p_2, p_1]_4 = 1$. In this case, the 8-rank of the class group in the strict sense is 1. Hence, a natural approach is to try to construct a $\mathbb{Z}/8\mathbb{Z}$, unramified extension of $K = \mathbb{Q}[\sqrt{p_1 p_2}]$.

5.1 A starting point

The starting point of this approach is the following lemma which is introduced in the paper [15].

Lemma 5.1.1. *Let K be a field of characteristic different from 2. Suppose d is an element in K which is not a square. Then for $\alpha \in K(\sqrt{d})$, the extension $K(\sqrt{d})(\sqrt{\alpha})/K$ is a $\mathbb{Z}/4\mathbb{Z}$ Galois extension containing $K(\sqrt{d})$ if and only if*

$$N_{K(\sqrt{d})/K}(\alpha) = da^2,$$

for some $a \in K$.

Proof. Let $m = N_{K(\sqrt{d})/K)}(\alpha)$. Suppose $\alpha = x + y\sqrt{d}$ where $x, y \in K$. Then the minimal polynomial of α over K is

$$X^2 - 2xX + m.$$

We can easily conclude that the minimal polynomial of $\sqrt{\alpha}$ over K is

$$X^4 - 2xX^2 + m.$$

The four roots of this polynomial are

$$\beta, -\beta, \frac{\sqrt{m}}{\beta}, -\frac{\sqrt{m}}{\beta},$$

where $\beta = \sqrt{\alpha}$. Thus, the extension $K(\sqrt{d})(\sqrt{\alpha})/K$ is normal if and only these four roots are all in $K(\sqrt{d})(\sqrt{\alpha})$. This happens only when $\sqrt{m} \in K(\sqrt{d})(\sqrt{\alpha})$.

First, suppose that $m = da^2$ for some $a \in K$. By the above argument, we know that the extension $K(\sqrt{d}, \sqrt{\alpha})$ over K is Galois. It is also easy to prove that this extension has Galois group $\mathbb{Z}/4\mathbb{Z}$.

Conversely, suppose that $K(\sqrt{d}, \sqrt{\alpha})$ is a $\mathbb{Z}/4\mathbb{Z}$ Galois extension of K. Since there is only one normal subgroup of $\mathbb{Z}/4\mathbb{Z}$ of index 2, the Galois correspondence tells us that there exists a unique quadratic extension of K contained in $K(\sqrt{d})(\sqrt{\alpha})$. From our definition, this subfield must be $K(\sqrt{d})$. Thus $\sqrt{m} \in K(\sqrt{d})$. Since $m \in K$, m must be of the form da^2 for some $a \in K$.

□

The following lemma is a direct consequence of the above lemma.

Lemma 5.1.2. *With the same notations, there exists such an α if and only if d is the sum of two squares. Furthermore, suppose $d = x^2 + y^2$, then every $\mathbb{Z}/4\mathbb{Z}$ extension L/K containing $K(\sqrt{d})$ must be of the form*

$$L_r = K(\sqrt{rd + ry\sqrt{d}}),$$

for some $r \in K$.

Proof. The proof is almost straightforward except the use the of following observation. □

Lemma 5.1.3. *Suppose $\gamma \in K(\sqrt{d})$ such that $N_{K(\sqrt{d})/K}(\gamma) = a^2$ for some $a \in K$. Then there exists $r \in K$ such that $r\gamma$ is a square in $K(\sqrt{d})$.*

Proof. Suppose $\gamma = x + y\sqrt{d}$. We need to show that there exist $r, u, v \in K$ such that

$$r(x + y\sqrt{d}) = (u + v\sqrt{d})^2.$$

This is equivalent to

$$rx = u^2 + dv^2, ry = 2uv.$$

In a more compact form, this is equivalent to the existence of $u, v \in K$ such that

$$y(u^2 + dv^2) - 2xuv.$$

If $y = 0$ then we can simply take $v = 0, u = r = x$. If $y \neq 0$, the discriminant of this quadratic form is a^2. Hence, we can take

$$u = \frac{2xv + a}{y}.$$

That means, we can always find (r, u, v) satisfying our constraints. □

Remark 5.1.1. Suppose that α, β are two elements in $K(\sqrt{d})$ such that both $K(\sqrt{d})(\sqrt{\alpha})$ and $K(\sqrt{d})(\sqrt{\beta})$ are $\mathbb{Z}/4\mathbb{Z}$ extensions of K. Then if we take $\gamma = \frac{\alpha}{\beta}$ and apply the above observation we obtain at lemma 5.1.2.

We now come back to our problem. First, we recall what we have achieved so far. We know that if (x_0, y_0, z_0) is a solution of

$$x_0^2 - p_1 y_0^2 - p_2 z_0^2 = 0,$$

such that

- x_0 is odd
- y_0 is even
- $x_0 + y_0 \equiv 1 \pmod 4$

then we have a tower of field extensions

$$\begin{tikzcd}
H \arrow[d, dash] \\
H^1 \arrow[d, dash] \\
K \arrow[d, dash] \\
Q
\end{tikzcd}$$

where $K = \mathbb{Q}[\sqrt{p_1p_2}]$, $H^1 = \mathbb{Q}[\sqrt{p_1}, \sqrt{p_2}]$ and $H = H^1[\sqrt{\epsilon_{p_1}}]$ where $\epsilon_{p_1} = x_0 + y_0\sqrt{p_1}$. Furthermore H is a $\mathbb{Z}\,/4\,\mathbb{Z}$ is an unramified extension of K.

Now if we let

$$H^1 = \mathbb{Q}[\sqrt{p_1}, \sqrt{p_2}], \epsilon_{p_1} = x_0 + y_0\sqrt{p_1}$$

take the roles of K, d in lemma 5.1.1 and 5.1.2, we may get an approach to our problem. More precisely, we know for sure that there exists a $\mathbb{Z}\,/8\,\mathbb{Z}$ extension of K and therefore a $\mathbb{Z}\,/4\,\mathbb{Z}$ extension of H^1. From lemma 5.1.1 and 5.1.2, we know that ϵ_{p_1} must be the sum of two squares in H^1. However, it turns out that ϵ_{p_1} is the sum of two squares in $\mathbb{Q}[\sqrt{p_1}]$.

Theorem 5.1.1. *ϵ_{p_1} can be written as the sum of two squares in $\mathbb{Q}[\sqrt{p_1}]$.*

In order to prove this theorem, we will make use of the Hasse principle. We first introduce some results in finite fields and local fields.

Theorem 5.1.2. *Let F be a finite field of odd order. Then every element in F is a sum of two squares.*

On F we can define a character χ as follow

$$\chi(a) = \begin{cases} 0 & \text{if a=0} \\ 1 & \text{if a is a square} \\ -1 & \text{if a is not a square.} \end{cases}$$

Let u be some element in F. In order to show that u is the sum of two squares, it is sufficient to show that for some a, $u - a^2$ is a square. Equivalently, we need to show that for some $a \in F$, $\chi(x - a^2)$ is not -1. To do show, we will use Weil's theorem.

Theorem 5.1.3 (Weil). *Let χ be a character of the finite field F_p of order s. Let $f(x)$ be a polynomial in $\mathbb{F}_p$ of degree d and can not be written in the form $c \times h(x)^s$. Then we have*

$$\left| \sum_{a \in \mathbb{F}_p} \chi(h(a)) \right| \leq (d-1)\sqrt{p}.$$

Since F has odd order, χ is not trivial and $h(x)$ is not of the form $cf(x)^2$, our example satisfies the constraints in Weil's theorem. Hence we can apply this theorem for $h(X) = u - X^2$ and χ and obtain

$$\left| \sum_{a \in \mathbb{F}_p} \chi(u - a^2) \right| \leq \sqrt{p}.$$

Therefore, if all $\chi(u - a^2) = -1$ then we must have

$$p = \left| \sum_{a \in \mathbb{F}_p} \chi(u - a^2) \right| \leq \sqrt{p},$$

which is impossible.

Remark 5.1.2. There is a more simple proof without using the Weil's theorem, but it is too long to write down. The idea is to compute the sum

$$\sum_{a \in \mathbb{F}_p} \chi(u - a^2),$$

directly.

Definition 5.1.1. A valuation $||$ on a field K is a function from K to the set $\mathbb{R}_{\geq 0}$ satisfying the following conditions

1. $|a| = 0$ if and only if $a = 0$.
2. $|ab| = |a||b|$,
3. $|a+b| \leq |a| + |b|$ for any $a, b \in K$.

When the condition 3 is replaced by a weaker condition

$$|a+b| \leq \max\{|a|, |b|\},$$

Then the valuation is called non-archimedean. From now on, every valuation is assumed to be non-archimedean.

For any valuation $||$ we can define a corresponding function from K to $R \cup \{\infty\}$ as follow

$$\nu(a) = -\log|a|, \forall a \neq 0,$$

and $v(0) = \infty$. This function has the following properties

1. $\nu(x) = \infty$ if and only if $x = 0$.
2. $\nu(xy) = \nu(x) + \nu(y)$.
3. $\nu(x+y) \geq \min\{\nu(x), \nu(y)\}$.

Conversely, if for any a function v satisfying all the above conditions, we can construct a corresponding valuation on K. For instance, let q be any real number bigger than 1. Then we define

$$|x| = q^{-v(x)}.$$

From now on, we will use the notation $||$ and ν simultaneously.

Example 5.1.1. Let $K = \mathbb{Q}$, p be any prime number and c be some real number such that $0 < c < 1$. We are going to define a valuation on $\mathbb{Q}$.

Every element a in $\mathbb{Q}$ that is not 0 can be written in the form $p^n \frac{c}{d}$ where $\gcd(c, d) = 1$. Moreover, the number n is unique. We define

$$\nu_p(a) = n, \quad |a|_{p,c} = c^{\nu_p(a)}.$$

We also define $|0| = 0$. It is easy to prove that $||_{p,c}$ is a valuation on $\mathbb{Q}$. Indeed, the most non-trivial part of the proof is to show that

$$\nu_p(x+y) \geq \min\{\nu_p(x), \nu_p(y)\}, \forall x, y \in \mathbb{Q}.$$

This can be proved directly from the definition.

Example 5.1.2. For any number field F and $\mathfrak{p}$ is a prime ideal, we can define a corresponding valuation

$$|x| = \left(\frac{1}{N\mathfrak{p}}\right)^{v_{\mathfrak{p}}(x)}.$$

Remark 5.1.3. A valuation $||$ induces a metric on K where the distance is defined by

$$d(x,y) = |x - y|.$$

The triangle inequality is deduced from condition (3).

With this remark we have the following definition.

Example 5.1.3. Two valuations on K are called equivalent if and only if they define the same topology on K.

The following theorem is standard

Theorem 5.1.4. *Two valuations $||_1$ and $||_2$ on K are equivalent if and only if there exists a real number $s > 0$ such that*

$$|a|_1 = |a|_2^s,$$

for all $a \in K$.

Proof. See [11]. □

Example 5.1.4. In example 5.1.1, each number c such that $0 < c < 1$ produces a corresponding valuation on K. By the above theorem, all these valuations are equivalent. For some technical reason (product formula), we will take $c = \frac{1}{p}$.

We have the following important definition.

Theorem 5.1.5. *Let $||$ is a valuation on a field K. Then the set*

$$\mathcal{O} = \{x \in K \mid |x| \leq 1\} = \{x \in K \mid \nu(x) \geq 0\},$$

is a ring with units

$$\mathcal{O}^\star = \{x \in K \mid |x| = 1\} = \{x \in K \mid \nu(x) = 0\},$$

and the unique maximal ideal

$$\mathfrak{p} = \{x \in K||x| < 1\} = \{x \in K \mid \nu(x) > 0\}.$$

The field $\kappa = \mathcal{O} \,/\, \mathfrak{p}$ is called the residue field of K.

Proof. The proof is straightforward by using the inequality

$$|x + y| \leq \max\{|x|, |y|\}.$$

□

A valuation v is called discrete if the set

$$G = \{\log |x| \mid x \in K, x \neq 0\} = \nu(K^\star),$$

is a discrete subgroup of R under addition. It is the same thing as there exists $s > 0$ such that

$$\nu(K^\star) = s\,\mathbb{Z}\,.$$

We can simply take $s = 1$ (since changing s does not affect the topology on K). With this assumption, we can find an element $\pi \in \mathcal{O}$ such that

$$\nu(\pi) = 1.$$

Definition 5.1.2. The element π is called a uniformizer of K.

We have the following important proposition.

Proposition 5.1.1. *Every element $x \in K^\star$ admits a unique representation in the form*

$$x = u\pi^m,$$

where $u \in \mathcal{O}^\star$.

Proof. Let $m = v(x)$ then $v(x\pi^{-m}) = 0$. By definition, $x\pi^{-m}$ is a unit. Thus there exits $u \in \mathcal{O}^\star$ such that

$$x = u\pi^m.$$

The uniqueness of this type of representation is obvious. □

Let K be a field with a valuation $||$. We say that K is complete if the metric on K induced by $||$ is complete. In other words, every Cauchy sequence in K converges to an element in K. Not all valuation fields are complete. The most trivial example is the field $\mathbb{Q}$ with the $p-$ adic valuation introduced in 5.1.1. However, we can always embed K into a complete valuation field. The idea is similar to the completion of a metric space. More precisely, let K_v be the set of all equivalent classes of Cauchy sequences. Let $(a) = (a_1, a_2, \dots,)$ be a representative of a. We define

$$|a| = \lim_{n \longrightarrow \infty} |a_n|.$$

By definition, it is easy to verify that $||$ is valuation on K_v. Moreover, there exists a natural embedding of K into K_v by sending each element to a constant sequence. Thus K is embedded in K_v. We sum up these arguments in the following theorem.

Theorem 5.1.6. *For any valuation field $(K, ||)$ there exists a field K_ν containing K together with a valuation extending the original valuation in a way that K is dense in K_ν. Furthermore, K_ν is unique up to isomorphism fixing K.*

In case ν is discrete we can observe that

$$\nu(K) = \nu(K_\nu) = \mathbb{Z}.$$

Proof. See [11]. □

We also define $\hat{\mathcal{O}}, \hat{\mathcal{O}}^\star, \hat{\mathfrak{p}}, \hat{R}$ in the spirit of theorem 5.1.5. With this notation, we have the following theorem

Theorem 5.1.7. *If ν is a discrete valuation then*

$$\mathcal{O}/\,\mathfrak{p} \cong \hat{\mathcal{O}}/\hat{\mathfrak{p}}.$$

More over for any $n \geq 1$

$$\mathcal{O}/\mathfrak{p}^n \cong \hat{\mathcal{O}}/\hat{\mathfrak{p}}^n.$$

Proof. We will present a proof for the case $n = 1$. The general case can be done with the same argument. First of all, we have an injective map ϕ from $\mathcal{O}/\,\mathfrak{p}$ to $\hat{\mathcal{O}}/\hat{\mathfrak{p}}$ defined by

$$a + \mathfrak{p} \mapsto (a, a, \dots) + \hat{\mathfrak{p}}.$$

We need to show that ϕ is surjective. Let $(a_1, a_2, \dots,)$ be a representative of some element $a \in \hat{\mathcal{O}}$. Then by definition, there exists a number $N > 0$ such that

$$\nu(a_i - a_N) > 0, \forall i \geq N.$$

In other words, $a_i - a_N \in \mathfrak{p}$ for any $i \geq N$. Thus, we have $\phi(a_N) = (a_1, a_2, \dots)$.

□

With this theorem, we have the following proposition.

Proposition 5.1.2. *Let $R \subset \mathcal{O}$ be a system of representatives for $\kappa = \mathcal{O}/\mathfrak{p}$ such that $0 \in R$ and π be a uniformizer. Then every non-zero element in K_v can be written uniquely in the form*

$$x = \pi^m(a_0 + a_1\pi + a_2\pi^2 + \ldots),$$

where $a_i \in R$, $a_0 \neq 0$ and $m \in \mathbb{Z}$.

This representation provides us another way of viewing the valuation ring. To be more precise, we have the following theorem.

Theorem 5.1.8. *Let v be a discrete, complete valuation on a field K. Then we have a canonical isomorphism*

$$\mathcal{O} \cong \varprojlim_n \mathcal{O}/\mathfrak{p}^n.$$

We have the following important corollary.

Corollary 5.1.1. *Let L/K be an extension of number field. Suppose $\mathfrak{p}$ be a prime in K and $\wp$ is some prime lying above $\mathfrak{p}$. Suppose further that $f(\wp|\mathfrak{p}) = 1$. Then we have a canonical isomorphism*

$$K_{\mathfrak{p}} \cong L_{\wp}.$$

Fixed a number field K. We will make use of the following notations.

1. $\mathcal{O}_{\mathfrak{p}} = \{x \in K | \nu_{\mathfrak{p}}(x) \geq 0\}$.
   (Another way of understanding $\mathcal{O}_{\mathfrak{p}}$ is that it is the localization of K at $\mathfrak{p}$)
2. $m_{\mathfrak{p}} = \{x \in K | \nu_{\mathfrak{p}}(x) > 0.\}$.
   (It is the maximal ideal of the local ring $O_{\mathfrak{p}}$).
3. O_K is the ring of algebraic integers in K.

Then we have inclusions $O_K \hookrightarrow \mathcal{O}_{\mathfrak{p}}$ and $\mathfrak{p} \hookrightarrow m_{\mathfrak{p}}$. Hence, we have a natural homomorphism

$$\phi : O_K/\mathfrak{p} \longrightarrow \mathcal{O}_{\mathfrak{p}}/m_{\mathfrak{p}}.$$

It turns out that ϕ is an isomorphism. The injectivity of ϕ is obvious, therefore, we only need to verify that ϕ is surjective. It is sufficient to show that if $u \in \mathcal{O}_{\mathfrak{p}}$ such that $\nu_{\mathfrak{p}}(u) = 0$, there exists $a \in O_K$ satisfying

$$\phi(a + \mathfrak{p}) = u + m_{\mathfrak{p}}.$$

Indeed, we can find $c, d \in O_K$ such that $u = \frac{c}{d}$ and $\nu_{\mathfrak{p}}(d) = \nu_{\mathfrak{p}}(c) = 0$. Since $O_K/\mathfrak{p}$ is a field, the element $d + \mathfrak{p}$ has an inverse, say e. Namely, we have $de \equiv 1 \pmod{\mathfrak{p}}$. It is then straightforward that

$$c \equiv ecd \pmod{\mathfrak{p}}.$$

Hence $\nu_{\mathfrak{p}}(\frac{c}{d} - ce) > 0$. By definition, $\phi(ce + \mathfrak{p}) = u + m_{\mathfrak{p}}$. This shows that ϕ is surjective.

Remark 5.1.4. There is another proof using the following fact in Commutative Algebra. If R is a commutative ring and $\mathfrak{p}$ is a prime ideal of R. Then we have a natural isomorphism between $R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}$ and $k(P) = Fr(R/\mathfrak{p})$ where $Fr(R/\mathfrak{p})$ is the quotient field of the integral domain $R/\mathfrak{p}$. In our case, since O_K is a Dedekind domain, $O_K/\mathfrak{p}$ is a field and hence is equal to its field of fraction.

With a similar argument, we can also prove that for any $n \geq 1$ we also have a natural isomorphism

$$\phi_n : O_K/\,\mathfrak{p}^n \cong \mathcal{O}_{\mathfrak{p}}/m_{\mathfrak{p}}^n.$$

Furthermore, it is also easy to see that for all $m > n$ the following diagram is commutative

$$\begin{tikzcd}
O_K/\,\mathfrak{p}^m \arrow[r, "\lambda_{m,n}"] \arrow[d, "\phi_m"'] & O_K/\,\mathfrak{p}^n \arrow[d, "\phi_n"] \\
\mathcal{O}_{\mathfrak{p}}/\,\mathfrak{p}^m \arrow[r, "\lambda_{m,n}"'] & \mathcal{O}_{\mathfrak{p}}/\,\mathfrak{p}^n
\end{tikzcd}$$

Thus we have a natural isomorphism

$$\varprojlim_n O_K/\,\mathfrak{p}^n \cong \varprojlim_n O_{\mathfrak{p}}/m_{\mathfrak{p}}^n.$$

Finally, theorems 5.1.7 and 5.1.8 tell us that

$$\hat{\mathcal{O}} \cong \varprojlim_n \hat{\mathcal{O}}/\hat{m}_{\mathfrak{p}}{}^n,$$

and

$$\mathcal{O}/m_{\mathfrak{p}}{}^n \cong \hat{\mathcal{O}}/\hat{m}_{\mathfrak{p}}{}^n.$$

So we have a natural isomorphism

$$\hat{\mathcal{O}} = \varprojlim_n O_K/\,\mathfrak{p}^n\,.$$

Now, suppose $\wp$ is some prime ideal of L lying above $\mathfrak{p}$ such that $f(q|p) = 1$. It is the same thing as to say that the homomorphism

$$O_K/\,\mathfrak{p} \longrightarrow O_L/\,\wp,$$

is an isomorphism. From this isomorphism, we can conclude that for any $n \geq 1$ we have

$$O_K/\,\mathfrak{p}^n \longrightarrow O_L/\,\wp^n.$$

Combining the above arguments, we have proved that

$$K_{\mathfrak{p}} \cong L_{\wp}.$$

Theorem 5.1.9. *Let $(K, ||)$ be a complete discrete valuation field and $f(x)$ be a polynomial with coefficient in $\mathcal{O}$. Suppose there exists $x_0 \in \mathcal{O}$ such that $v(f(x_0)) > 0$ but $v(f'(x_0)) = 0$. Then f has a root in $\mathcal{O}$.*

Proof. See [11]. □

We will discuss some applications of the Hensel's lemma.

Theorem 5.1.10. *Let K be a number field and $\mathfrak{p}$ be a prime ideal of O_K not lying above 2. The unit ϵ*

$$\epsilon = a_0 + a_1\pi + a_2\pi^2 + \ldots,$$

with $a_i \in R$ being a set of representatives for $O_K/\,\mathfrak{p}$, is a square in $\hat{\mathcal{O}}$ if and only if a_0 is a square in $O_K/\,\mathfrak{p}$.

Proof. Suppose $\epsilon = \eta^2$ and

$$\eta = b_0 + b_1\pi + b_2\pi^2 + \dots,$$

Then one must have

$$a_0 \equiv b_0^2 \pmod{\mathfrak{p}}.$$

In other words, a_0 is a square in $O_K/\ \mathfrak{p}$.

Conversely, suppose a_0 is a square in O_K/β. Then there exists $b \in O_K$ such that

$$b^2 \equiv a_0 \pmod{\mathfrak{p}}.$$

Consider the polynomial $X^2 - \epsilon$. Then $f'(x) = 2X$. We then know that $\nu_{\mathfrak{p}}(f(b)) > 0$ but $\nu_{\mathfrak{p}}(f'(b)) = 0$. Hence, by Hensel's lemma, the polynomial $X^2 - \epsilon$ has a root in $\hat{\mathcal{O}}_{\mathfrak{p}}$. In other words ϵ is a square in $\hat{\mathcal{O}}_{\mathfrak{p}}$. □

Corollary 5.1.2. *Let $\mathfrak{p}$ be a prime not dividing 2. Then every unit in $\hat{\mathcal{O}}_{\mathfrak{p}}$ which is congruent to 1 modulo $\hat{m}_{\mathfrak{p}}$ is a square.*

A direct corollary of the above statement is the following

Corollary 5.1.3. *Let $\mathfrak{p}$ be a prime not dividing 2. Then every unit in $\hat{\mathcal{O}}_{\mathfrak{p}}$ is a sum of two square.*

Proof. Let

$$\epsilon = a_0 + a_1\pi + a_2\pi^2 + \dots.$$

Then since ϵ is a unit, we have $a_0 \notin \mathfrak{p}$. By the theorem on finite fields at the beginning, there exist $c, d \in O_K$ such that

$$a_0 - c^2 - d^2 \equiv 0 \pmod{\mathfrak{p}}.$$

So in particular, $\nu_{\mathfrak{p}}(c^2 + d^2) = 0$ since $a_0 \notin \mathfrak{p}$. Therefore, the element $\eta = \dfrac{\epsilon}{c^2 + d^2}$ is also a unit in $\hat{\mathcal{O}}_{\mathfrak{p}}$. Furthermore, we have $\eta \equiv 1 \pmod{m_{\mathfrak{p}}}$. Hence, η is a square in $\hat{\mathcal{O}}_{\mathfrak{p}}$. It is then easy to see that ϵ is the sum of two squares. □

In case $p = 2$, the situation is a little bit different. We will state without proof the following theorem.

Theorem 5.1.11. *A unit ϵ in $\mathbb{Q}_2$ is a square if only if $\epsilon \equiv 1 \pmod{8}$.*

5.2 Our problem

The main theorem of this section is the following theorem.

Theorem 5.2.1. *Let p_1, p_2 be two prime numbers of the form $8k + 1$ such that $[p_1, p_2]_4[p_2, p_1]_4 = 1$. Let (x, y, z) be a solution of the quadratic form*

$$X^2 - p_1Y^2 - p_2Z^2 = 0,$$

satisfying

1. *x, z are odd and y is even.*
2. *$x + y \equiv 1 \pmod{4}$.*

Then $\epsilon_{p_1} = x + y\sqrt{p_1}$ is the sum of two squares in $Q[\sqrt{p_1}]$.

We recall some properties of x, y, z that we have already known.

- $[p_1, p_2]_4[p_2, p_1]_4 = 1$ if and only if $x > 0$.

- $\left(\frac{2|x|}{p_2}\right) = [p_1, p_2]_4$.

Hence the condition $[p_1, p_2]_4[p_2, p_1]_4 = 1$ is equivalent to

- $x > 0$.

We will show that this condition will guarantee that ϵ_{p_1} is the sum of two squares in $L = \mathbb{Q}[\sqrt{p_1}]$. To do show, we will show that $x + y\sqrt{p_1}$ is the sum of two squares in every completion of $\mathbb{Q}[\sqrt{p_1}]$. We also have the observation that

$$(x + y\sqrt{p_1})(x - y\sqrt{p_1}) = p_2 z^2,$$

is the sum of two squares since p_2 can be written as the sum of squares of two integers. Hence, $x + y\sqrt{p_1}$ is the sum of two squares in some completion of L if and only if $x - y\sqrt{p_1}$ is.

Let $\wp$ be any prime in O_L. We consider the following cases.

. Case 1: $\wp = \infty$. Since $x > 0$, we can conclude that $\epsilon_{p_1} > 0$. Hence, ϵ_{p_1} is the sum of two squares in the completion of L at infinite primes.

Let $\wp$ be a prime of O_L. We will denote by p the prime ideal in $\mathbb{Z}$ lying below $\wp$. We consider the following cases.

. Case 2: $p \nmid p_2 z^2$.

Then ϵ_{p_1} is a unit in $\hat{\mathcal{O}}_\wp$ since $\epsilon_{p_1} \notin \wp$. Hence ϵ_{p_1} is the sum of two squares in the completion $L_\wp$.

Let $z = p_2^m w$ where $\gcd(w, p_2) = 1$. We consider the following cases.

. Case 3: $p = p_2$.

In this case p_2 splits completely, i.e, $p_2 = \wp\overline{\wp}$. Since $\epsilon\overline{\epsilon} = p_2 z^2$, one of the element ϵ_{p_1} and $\overline{\epsilon_{p_1}}$ must belong to $\wp$. Without loss of generality, we can assume that $\epsilon_{p_1} \in \wp$. Moreover, $\overline{\epsilon_{p_1}}$ does not belong to $\wp$. Suppose to the contrary that $\overline{\epsilon_{p_1}} = x - y\sqrt{p_1}$ is in $\wp$. Then $2x$ and $p_2 z^2$ is in $\wp$. This is impossible since $\gcd(2x, p_2 z^2) = 1$. Hence, $\overline{\epsilon_{p_1}}$ is not in $\wp$. We have

$$\nu_\wp(\epsilon_{p_1}) = \nu_\wp(\epsilon_{p_1}\overline{\epsilon_{p_1}}) = \nu_\wp(p_2 z^2) = \nu_p(p_2 z^2) = 2m + 1.$$

The last equality comes from the fact that $e(\wp|p) = 1$. By definition, $\frac{\epsilon_{p_1}}{p^{2m+1}}$ is a unit in $\mathcal{O}_\wp$. Hence, $\frac{\epsilon_{p_1}}{p^{2m+1}}$ is the sum of two squares in $\hat{\mathcal{O}}_\wp$. In addition to the fact that p^{2m+1} is the sum of two squares in $\mathbb{Z}$, we conclude that ϵ_{p_1} is the sum of two squares in $\hat{\mathcal{O}}_\wp$.

. Case 4: p is a divisor of w.

Let $n = \nu_p(w)$. By the same argument in case 3, we can conclude that $\frac{\epsilon_{p_1}}{p^{2n}}$ is a unit in $\hat{\mathcal{O}}_\wp$ and hence is the sum of two squares. Thus, ϵ_{p_1} is also the sum of two squares in $\hat{\mathcal{O}}_\wp$

. Case 5: $p = 2$

This is the most lengthy case to check. First, 2 splits completely in $\mathbb{Q}[\sqrt{p_1}]$ since p_1 is of the form $8k + 1$. Hence, we know that $L_\wp \cong Q_2$. As a result, in order to show that ϵ_{p_1} is the sum of two squares, it is sufficient to show that there exists $a, b \in \mathbb{Z}$ such that

$$\epsilon_{p_1} \equiv a^2 + b^2 \pmod{\wp^3}.$$

Since x is odd, y is even and $x + y \equiv 1 \pmod 4$, we consider the following cases.

. Case 5.1: $y \equiv 0 \pmod 8$.

Then $x \pmod 8$ is either 1 or 5. In both case 1 and 5 are the sum of two squares. Hence, we can always find $a, b \in \mathbb{Z}$ such that

$$\epsilon_{p_1} \equiv a^2 + b^2 \pmod{\wp^3}.$$

. Case 5.2: $y \equiv 4 \pmod 8$.

If $x \equiv 1 \pmod 8$ then

$$\epsilon_{p_1} \equiv 5 \pmod{\wp^3},$$

which in turn shows that ϵ_{p_1} is the sum of two square in $L_\wp$.

The remaining case is $x \equiv 5 \pmod 8$. In this case, $\epsilon_{p_1} \equiv 1 \pmod{\wp^3}$. Thus, we have the same conclusion as above.

5.3 Intentions for the next step

From the last section, we know that ϵ_{p_1} is the sum of two squares. Hence, the equation

$$w^2 - \epsilon_{p_1} u^2 - \epsilon_{p_1} v^2 = 0,$$

is solvable in $\mathbb{Z}[\sqrt{p_1}]$. From the last report, we know that all $\mathbb{Z}/4\mathbb{Z}$ extension of $H^1 = \mathbb{Q}[\sqrt{p_1}, \sqrt{p_2}]$ is of the form

$$H_3^r = H\left[\sqrt{r(w + u\sqrt{\epsilon_{p_1}})}\right],$$

where $H = H^1[\sqrt{\epsilon_{p_1}}]$. So, now some natural questions are

1. For which r the extension will be $\mathbb{Z}/8\mathbb{Z}$ over $K = \mathbb{Q}[\sqrt{p_1 p_2}]$.
2. For which r the extension will be unramified over K.

There should be some difficulties with these questions. One clear reason is that we do not use the full hypothesis that $[p_1, p_2]_4 = [p_2, p_1]_4 = 1$ in theorem 5.2.1.

Conclusion

This thesis has given some answer for the question about the norm of the fundamental unit in real quadratic number fields. For example, I showed that if d is a prime number of the form $4k+1$ then the fundamental unit has negative norm. I list here some important results that I was able to produce my own proof in this thesis.

- I showed in [2.2.5] that the fundamental unit has negative norm if and only if the negative Pell's equation has integer solution.
- I showed in [2.4.1] that the fundamental unit of the quadratic field $\mathbb{Q}[\sqrt{p}]$ where p is a prime number has negative norm if $p = 2$ or p is of the form $4k+1$. Otherwise, it has positive norm.
- Based on my advisor hints, I proved theorem [3.2.2] on my own.
- I showed in [4.1.1], the fundamental unit of $\mathbb{Q}[\sqrt{p}]$ where p is some prime of the form $4k+1$ has negative norm.
- Based on my advisor hints, I showed in [4.2.1] that if p_1, p_2 are two primes of the form $4k+1$ such that $\left(\frac{p_1}{p_2}\right) = -1$ then the fundamental unit of the quadratic number field $\mathbb{Q}[\sqrt{p_1 p_2}]$ has negative norm.
- The result about the 4 rank of the class group in the strict sense in section 4.3 is introduced in [22]. I was able to produce my own proof for this result by investigating properties of the Artin symbols.
- Theorem 4.3.6 and 4.3.10 are introduced in [8] without proofs. I was able to produce my proofs for these theorems. I was also able to apply these theorems to prove proposition 4.3.9 and consequently produce a proof for theorem 4.3.15.
- I proposed in chapter 5 a promising approach to go deeper in the original problem. For instance, based on my advisor hints, I proposed and proved theorem 5.2.1.

Chapter 6

Appendix

6.1 Hasse-Minkowski principle

Theorem 6.1.1. *A quadratic form over $\mathbb{Q}$ has a non-trivial solution over $\mathbb{Q}$ if and only if it has solution over $\mathbb{R}$ and $\mathbb{Q}_p$ for any prime p.*

Proof. See [10], chapter 4, page $27 - 45$. □

6.2 Integral basis of a number field

We say that $x_1, \ldots, x_n$ is an integral basis of the ring of algebraic integers in a number field K if every element in O_K can be written uniquely as $a_1x_1 + \ldots + a_nx_n$ where $a_n \in \mathbb{Z}$.

Theorem 6.2.1. *Let K be a number field of degree n, then K possesses an integral basis. Moreover, every integral basis has exactly n elements where N is the degree of K.*

Proof. See [3], chapter 6. □

6.3 Discriminant of a number field

Let $\{x_1, \ldots, x_n\}$ be an integral basis of a number field K. Then number

$$\text{Diss}(O) = \det(\text{Tr}(x_ix_j)_{i \leq i \leq j \leq n}),$$

does not depends on the choice of $\{x_1, \ldots, x_n\}$. It is called the discriminant of K.

Theorem 6.3.1. *Let K be a number field. A prime p is ramified in O_K if and only if $p | Disc(K)$*

Proof. See [5], page $199 - 200$. □

6.4 Minkowski bound

Theorem 6.4.1. *Let K be a number field. Then any ideal class of O_K contains an integral ideal of norm at most*

$$\sqrt{d_K} \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n},$$

where n is the degree of the extension, $d_K = Disc(O_K)$ and s is the number of complex embedding.

Proof. See [3], page $75 - 76$. □

6.5 Factoring primes

In chapter 4, we give a way to factor prime (see 4.3.6) in an extension of number fields $L\ slashK$. Here is a slightly different theorem

Theorem 6.5.1. *Suppose K is a monogenic number fields, that is K possesses an integral basis of the form $\{1, \alpha, \dots, \alpha^n\}$. Let f be the minimal polynomial of α over $\mathbb{Z}$. Let*

$$\overline{f} = \prod_{i=1}^{r} \overline{f_i}^{e_i},$$

be the factorization of f in $\mathbb{F}_p[X]$. Let $\mathfrak{p}_i = \langle p, f_i(\alpha) \rangle$ where f_i is some lift of $\overline{f_i}$. Then we have

$$\mathfrak{p}\, O_K = \prod_{i=1}^{r} \mathfrak{p}_i^{e_i}.$$

Proof. See [3], page $52 - 53$. □

References

Bibliography

[1] Miles Reid: Undergraduate commutative algebra, London Mathematical Society Student Texts, 1996.

[2] J.S Milne: Field and Galois Theory, online lecture note, version 4.

[3] William Stein: Algebraic number theory, a computational approach, online lecture note, 2011.

[4] Saban Alaca and Williams: Introductory algebraic number theory, Cambridge university press, 2003.

[5] Neukirch: Algebraic Number Theory, Grundlehren der mathematischen Wissenschaften, 1999.

[6] Franz Lemmermeyer: Reciprocity Laws, Springer Monographs in Mathematics, 2000

[7] David S. Dummit, Richard M. Foote: Abstract Algebra, third edition, 2003

[8] David A. Cox: Primes of the Form $x^2 + ny^2$, Class Field Theory, and Complex Multiplication, Pure and Applied Mathematics: A Wiley Series of Texts, Monographs and Tracts, 1997.

[9] Ian Stewart, David Tall: Algebraic Number Theory and Fermat's last theorem, third version, 2001.

[10] J-P Serre: A course in Arithmetic, Graduate Texts in Mathematics Vol. 7, 1996.

[11] N.Q. Thang: Local Fields (in Vietnamese), 2009.

[12] Kenneth Ireland, Michael Rosen: A Classical Introduction to Modern Number Theory, Graduate Texts in Mathematics v. 84, 1998.

[13] Pierre Samuel: Algebraic Theory of Numbers, 2008.

[14] Daniel Vallieres: On a generalization of the rank one Rubin-Stark conjecture, Phd Dissertation, University of California, San Diego 2011.

[15] Leila Schneps: On cyclic field extensions of degree 8, Math.Scand, 1971.

[16] Matthew Baker: An introduction to class field theory, online lecture note.

[17] , S. Lang: Algebraic Number Theory, Springer, Jun 22, 1999.

[18] Nancy Childress: Class Field Theory, Universitytext, 2008.

[19] Micheal J. Jacobson, Hugh C. Williams: Solving the Pell equation, CMS Book in Mathematics.

[20] H.W Lenstra: Solving the Pell equation, Notice of AMS, Volum 49, number 2.

[21] Franz Lemmermeyer Higher descent on Pell conics, from Legendre to Selmer, online lecture.

[22] Peter Stevenhagen: Redei matrices and applications, London Mathematical Society Lecture Note Series (No. 215), pp 245-260.

[23] Peter Stevenhagen: The number of real quadratic fields having units of negative norm, Experimental Mathematics. Volume 2, Issue 2 (1993), 121-136.

[24] Tommy Bulow: Norm of units and 4 rank of class group, Phd thesis.

[25] Yoshiomi Furuta: Norm of units of quadratic fields,J. Math. Soc. Japan Volume 11, Number 2 (1959), 139-145.

[26] Hideo Yokoi: On real quadratic fields containing units with norm 1, Nagoya Math. J. Volume 33 (1968), 139-152.

[27] H.Cohn, J.C Lagarias: On the existence of fields governing the 2-invariants of the class groups $\mathbb{Q}[\sqrt{dp}]$ as p varies.

[28] Etinnen Fouvry, Jurgen Kluners: On the negative Pell equation, Annals of Mathematics, Pages 2035-2104 from Volume 172 (2010), Issue 3.