CLASS NUMBER OF QUADRATIC FIELDS

by

Ayhan CAPUTLU

May 2010

CLASS NUMBER OF QUADRATIC FIELDS

by

Ayhan CAPUTLU

A thesis submitted to
the Graduate Institute of Sciences and Engineering

of

Fatih University

In partial fulfillment of the requirements for the degree of
Master of Science

in

Mathematics

May 2010
Istanbul, Turkey

CLASS NUMBER OF QUADRATIC FIELDS

Ayhan CAPUTLU

M. S. Thesis – Mathematics

May 2010

Supervisior: Assist. Professor Bülent KÖKLÜCE

ABSTRACT

CLASS NUMBER OF QUADRATIC FIELDS

We study the quadratic number fields and the class numbers of quadratic fields with their properties. The research on the class numbers of quadratic fields has a very long history. It actually started with Gauss's study of class numbers in quadratic forms. Some of his conjectures still continue to these days. We start the thesis by introducing the basic concepts including integral domain, algebraic number fields, ideals, units, Kronecker symbol, Dedekind domain and ideal class group. The class group is an extremely important object in algebraic number theory. Class group is commutative. Having a trivial class group is equivalent to all ideals being principal.

The concept of the ideal class group has been originated from Dedekind's work in establishing the unique factorization theory for ideals in the ring of algebraic integers of a number field.

By the “class number n problem for real and complex quadratic fields”, we mean the problem of presenting a complete list of all quadratic fields with class number n. For real quadratic fields, Gauss states that there are infinitely many real quadratic fields with class number one. Dirichlet developed his class number formula when he was trying to complete his theorems on primes.

We analyze real and imaginary quadratic number fields with class numbers 1 and 2 by comparing different methods including Hurwitz constant, Dirichet’s class number Formula, and finding class number using modules. Thesis also focuses on a survey demonstrating the historical aspect of the quadratic class number problem and contribution of different mathematicians in a chronological order until today.

Key words:

Quadratic number fields. Class number, Quadratic forms, Ideals, Units, Kronecker symbol, Dedekind domain, Ideal class group, Class group, Hurwitz constant, Dirichlet’s class number formula.

KUADRATIK CISIMLERIN SINIF SAYILARI

Ayhan CAPUTLU

Yüksek Lisans Tezi – Matematik
Mayıs 2010

Tez Yöneticisi: Yrd. Doç. Dr. Bülent KÖKLÜCE

ÖZ

Tezde kuadratik sayi cisimleri ile bu cisimlerin sinif sayilari, ozellikleri ile birlikte incelenmektedir.

Kuadratik sayi cisimlerinin sinif sayilari uzerindeki arastirmalar Gauss un kuadratik formlar uzerindeki calismalarina kadar uzanan oldukca uzun bir gecmise sahiptir. Gauss un o gunlerde ortaya koydugu bazi varsayimlar bugun dahi tam olarak aciklanamamistir. Bu calismada ilk bolumlerde cebirsel sayi cisimleri, idealler, birimler, Kronecker sembolu, Dedekind tanim kumesi ve ideal sinif gruplari ve ozellikleri uzerinde durulmustur. Sinif gruplari kavrami cebirsel sayi teorisinde cok onemli bir yere sahiptir.

Ideal sinif grubu kavrami Dedekind in calismalarinda ilk kez ortaya konulmus ve sayi cisimlerinin cebirsel tamsayilari halkasininda tanimlanan ideallerin carpanlara ayrilmasi teorisinin olusumunda kullanilmistir.

Reel ve sanal kuadratik cisimlerin n sinif sayilari problemi ile kastedilen “sinif sayisi n olan kuadratik cisimlerin liste halinde yazilmasidir”. Gauss, sinif sayisi 1 olan

reel kuadratrik cisimler icin, sonsuz sayida olduklarini ongormustur.Dirichlet, asal sayilar uzerinde ilgili teoremler uzerinde calisirken sinif sayisi formulunu de gelistirdi.

Tezimde, sinif sayilari 1 ve 2 olan reel ve sanal kuadratik sayi cisimlerini bulma yontemlerinden Hurwitz sabiti, Dirichlet in sinif sayisi formulu ve moduller yardimi ile sinif sayisi bulma metotlarinin karsilastirmali analizi uzerinde durmaktayim. Tezde ayrica gecmisten gunumuze kadar degisik matematikcilerin sinif sayisi bulma problemine katkilarini kronojik olarak inceleyip, sinif sayisi probleminin tarihsel surecine de vurgu yapilmaktadir.

Anahtar Kelimeler:

Kuadratik sayi cisimleri, Sinif sayisi, Kuadratik formlar. Idealler, Birimler, Kronecker sembolu, Dedekind tanim kumesi, Ideal sinif grubu, sinif gruplari, Hurwitz sabiti, Dirichlet sinif sayisi formulu.

DEDICATION

This work is dedicated to my wife Serpil Caputlu.

She motivated me to start this master thesis.
She helped me to continue it.
She insistently contributed to it.

ACKNOWLEDGEMENT

I would like to thank Assist. Professor Bulent Kokluce, my advisor, for his advice and inspiration. He is the person who guided me throughout the research.

I also would like to thank Fatih Unlu, Ph.D from University of Illinois, Chicago for his interest in my work and valuable advice.

I would like to express my great appreciation to all the members in our institute including Prof. Dr. Mustafa Bayram for his encouragement, Assoc.Prof. Nurullah Arslan, for his guidance in the final steps of my project.

A special thanks goes to Iskender Arslan for his close interest, sincere help and patience with my endless questions on the phone while putting this master thesis together.

Finally, I would like to thank my wife, Serpil, for her support, motivation and love.

TABLE OF CONTENTS

LIST OF SYMBOLS

I	**:** Ideal
Z	**:** Set of Integers
□	**:** The field of Rational Numbers
F	**:** Field
$\mathbf{Z_p}$	**:** Finite integral domain with characteristic p
$(Z_p, \oplus, \otimes)$	**:** Finite field with characteristic p
$\square_M$	**:** Ring of coefficients of modulo M.
$K = Q\left(\sqrt{d}\right)$	**:** Quadratic Number Field
H_d	**:** Class group
h(d)	**:** Class number of a quadratic field
$\chi_K(p)$	**:** Dirichlet Character associated with a constant
d	**:** Discriminant
O_K	**:** Ring of Integers
H_K	**:** Hurwitz constant
ε_d	**:** Fundamental unit of $K = Q\left(\sqrt{d}\right)$ *such that* $\varepsilon_d > 1$
$\left(\frac{a}{n}\right)$	**:** Kronecker symbol
C_K	**:** Order of the class group
u	**:** Unit element in $Q\left(\sqrt{d}\right)$
Tr(∝)	**:** Trace of ∝

N(∝) **:** Norm of ∝

LIST OF TABLES

PAGE NO

CHAPTER 1

INTRODUCTION

The class number problems for quadratic number fields have attracted attention of number theorists for decades. Among them, the most remarkable results are the solutions of Gauss 'conjecture on the class number of imaginary quadratic fields. The main result in this direction is that the number of imaginary quadratic fields which have a given class number h is finite. The cases h=1 and h=2 were solved completely and independently. The more general case, where h is an arbitrary positive integer was also solved.

In the case of real quadratic fields, similar questions are still open. The most information on class numbers is available for quadratic fields. These are the fields $K=Q(\sqrt{d})$, where d is a square free integer.

The situations for positive d (real quadratic fields) and negative d (imaginary quadratic fields) are quite different. In this thesis, we will examine what we mean by class number .We will discuss, analyze and compare different methods in computing the class number including Minkowki's Bound, Hurwitz Constant, Dirichlet's Class Number Formula, and finding class number using modules.

The main focus of this thesis is on the problem is to give a survey of solutions of the class number problem for quadratic number fields and give reader a systematic approach on what has been solved and what part of the main problem remain unsolved since Gauss' conjecture.

This master thesis introduces the reader not only to class number of notion but also to related concepts: groups, rings, fields, modules, units, ideals, Kronecker and Jacobi symbols, quadratic residues, unique factorization, and Ideal class group. Numerous exam and applications appear throughout the thesis.

CHAPTER 2

QUADRATIC FIELDS

2.1. The Field Axioms and Integral Domain

(F, +, ×) is a field under the operations + and ×, if and only if (F, +) is a commutative group, and the non: zero elements of F forms a group under the second operation ×.

A commutative ring with unit element is a field if all non: zero elements has an inverse element with respect to the second operation.

For instance, the set of rational numbers Q forms a field under + and ×, since (Q, +) is obviously a commutative (Abelian) group, and non: zero elements of Q is also a group under multiplication. Namely, every non: zero rational number has an inverse with respect to multiplication. Below are the field axioms:

An integral domain D is a field if all non: zero elements in D has an inverse with respect to second operation.

For example, $(Z_5, \oplus, \otimes)$ is a field since all its non: zero elements in Z_5 has multiplicative inverses. Namely, for $Z_5 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$

$$\overline{1}^{-1} = \overline{1}, \qquad (\text{since } 1 \otimes 1 = 1)$$
$$\overline{2}^{-1} = \overline{3}, \qquad (\text{since } 2 \otimes 3 = 1)$$
$$\overline{3}^{-1} = \overline{2}, \qquad (\text{since } 2 \otimes 3 = 1)$$
$$\overline{4}^{-1} = \overline{4}, \qquad (\text{since } 4 \otimes 4 = 1)$$

Note that the reciprocal is just the inverse under multiplication.

The nonzero elements of a field F form a commutative group under multiplication. For instance, the set of real numbers is a field under addition and multiplication.

Definition 2.1.1.

An integral domain D is a commutative ring with unit in which there are no zero divisors; In other words, for any a,b ∈ D, ab = 0 implies that a=0 or b=0, or a=b=0. The set of integers Z is an integral domain.

Because, for any $z_1, z_2 \in Z$, if $z_1 \times z_2 = 0$, then either z_1, or z_2, or both are equal to zero.

Take the finite group $Z_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$.

Z_6 is not a an integral domain, since $\bar{2} \times \bar{3} = \bar{0}$ and both $\bar{2} \in Z_6$ and $\bar{3} \in Z_6$ are non:

zero.Note that, Z_p, p is a prime number is an integral domain, where

$Z_p = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, ..., p-1\}$ (Z_p is an integral domain with order p)

Note that an integral domain D is a group under addition. Every nonzero element has the same order as 1 because $ma = (m1)a = 0$ only when $m1 = 0$.

The order must be prime. If it could be factored as m = ab, then 1+1+...+1 (a times) and 1+1+...+1 (b times) would be two nonzero elements whose product was zero

The ring Z_p is a field if p is prime and any finite integral domain is a field.

Definition 2.1.2.

For any a, b ∈ F, b≠0, (F is a field), $\frac{a}{b} = ab^{-1}$ [1]

A subfield of a field is a subset which is a field under the same addition and multiplication operations.

2.2. Field Extensions

Definition 2.2.1.

A finite extension of Q is called a number field. Specifically, the extension of second degree is called quadratic number field. Let k be a field extension of Q. If the degree of the extension is two, namely if $[K:Q]=2$, then it is known result that

$$K=Q(\sqrt{d})$$

for some square free integer d. (reference) .

In other words, every $\alpha \in Q(\sqrt{d})$ can be written as $\alpha=a+b\sqrt{d}$, and this expression is unique.

2.3. Quadratic Fields: Real and Imaginary Quadratic Number Fields

In this section, we will focus on the quadratic fields, that is, all algebraic number fields K such that $[K:Q]=2$. It can be shown that all quadratic extensions can be written as $K=Q\left(\sqrt{d}\right)$, where d is some square free integer.

Definition 2.3.1.

A quadratic number field is a sub field of the set of complex numbers C consisting of

the numbers of the form $a+b\sqrt{d}$, a, b, and d where a, b $\in$ Q and d with no rational square root.

If d > 0 and the set of number is of the form $a+b\sqrt{d}$, the field is a real quadratic number field,

If d < 0 and the set of number is of the form $a+b\sqrt{d}$ the field is imaginary quadratic number field.

The number $a+b\sqrt{d}$ is denoted by $Q(\sqrt{d})$ can also be called algebraic integer.

We have the following identities for the quadratic fields.

i. $(a_1+b_1\sqrt{d})\pm(a_2+b_2\sqrt{d})=(a_1+a_2)\pm(b_1+b_2)\sqrt{d}$

ii. $(a_1+b_1\sqrt{d})(a_2+b_2\sqrt{d})=(a_1a_2+b_1b_2n)+(a_1b_2+b_1a_2)\sqrt{d}$

iii. $\dfrac{(a_1+b_1\sqrt{d})}{(a_2+b_2\sqrt{d})}=\dfrac{(a_1a_2-b_1b_2d)}{a_2^2-b_2^2d}+\dfrac{(b_1a_2-a_1b_2)}{a_2^2-b_2^2d}\sqrt{d}$ [2]

Lemma 2.3.1.

Let $m\in Q(\sqrt{d})$. Then, m can be written in one and only one way in the form $m=a_1+b_1\sqrt{d}=a_2+b_2\sqrt{d}$, where a and b are rational numbers. Then, $a_1=b_1$ and $a_2=b_2$

Proof.

Assume that $a_1+b_1\sqrt{d}=a_2+b_2\sqrt{d}$. If $b_1\neq b_2$, then $d=\left(\dfrac{a_1-a_2}{b_2-b_1}\right)^2$

Then, $\dfrac{a_1-a_2}{b_2-b_1}$ is an integer and d is a perfect square, where $d\neq 1$. But, this is a contradiction since d is a square free integer. So, we conclude that $b_1=b_2 \Rightarrow a_1=a_2$.

Proposition 2.3.1. Let α_1 and α_2 be any pair of linearly independent elements of $Q(\sqrt{d})$ $\{\alpha_1,\alpha_2\}$ is a basis of $Q(\sqrt{d})$ over Q. Then, for any element α in $Q(\sqrt{d})$, there exist unique rational numbers a and b such that $\alpha=m\alpha_1+n\alpha_2$.

Exercise 2.3.1.

Determine whether the following sets are linearly independent. If not, exhibit a linear dependence relation among them.

a. $1, \sqrt{5}$ **b.** $2+\sqrt{-2}, \quad 2-3\sqrt{-2}$ **c.** $\dfrac{1}{2}, \quad \sqrt{-2}, \quad 2-3\sqrt{-2}$

Solution.

a. $m\alpha_1+n\alpha_2=0 \Leftrightarrow m=n=0$ (Criterie for linearly independent elements)

$\alpha_1=1$, and $\alpha_2=\sqrt{5}$. See that $m(1)+n(\sqrt{5})=0$, implies m=0 and n=0.

b. $\alpha_1=2+\sqrt{-2}$, and $\alpha_2=2-3\sqrt{-2}$

$m\alpha_1+n\alpha_2=0 \Leftrightarrow m=n=0$ (Criterie for linearly independent elements)

$m(2+\sqrt{-2})+n(2-3\sqrt{-2})=0$ gives $2m+\sqrt{-2}m+2n-3\sqrt{-2}n=0$

$2m+2n+(m-3n)\sqrt{-2}=0$. Therefore, $2m=0$, and $8n=0$

Consequently, $m=n=0$ and α_1 and α_2 are linearly independent.

c. $\alpha_1=\frac{1}{2}$, $\alpha_2=\sqrt{-2}$, $\alpha_3=2-3\sqrt{-2}$

$m\alpha_1+n\alpha_2+k\alpha_3=0 \Leftrightarrow m=n=k=0$ (Criteria for linearly independent elements)

$m\left(\frac{1}{2}\right)+n\left(\sqrt{-2}\right)+k\left(2-3\sqrt{-2}\right)=0$ gives $m\left(\frac{1}{2}\right)+n\left(\sqrt{-2}\right)+2k-3\sqrt{-2}k=0$

$m\left(\frac{1}{2}\right)+2k+(n-3k)\sqrt{-2}=0$.

$m=0$, $n=0$, $k=0$. Consequently, α_1,α_2 and α_3 are linearly independent.

Definition 2.3.2.

Let α be an element of $Q(\sqrt{d})$. α is an integer of $Q(\sqrt{d})$ provided that $Tr(\alpha)$ and $N(\alpha)$ are ordinary integers.

For example, $\left(\frac{1+\sqrt{5}}{2}\right)$ is an integer of $Q(\sqrt{5})$, since

$$Tr\left(\frac{1+\sqrt{5}}{2}\right)=\frac{1+\sqrt{5}}{2}+\frac{1-\sqrt{5}}{2}=1 \text{ and } N\left(\frac{1+\sqrt{5}}{2}\right)=\left(\frac{1+\sqrt{5}}{2}\right)\left(\frac{1-\sqrt{5}}{2}\right)=-1$$

Theorem 2.3.1.

Let d be a square free integer. Then the set I_d of integers of $Q(\sqrt{d})$ consists of the numbers of the form $x + yw_d$, where x and y are integers and

$$w_d=\begin{cases}\sqrt{d} & \text{if } d\equiv 2 \text{ or } 3 \pmod 4\\ \frac{1+\sqrt{d}}{2} & \text{if } d\equiv 1 \pmod 4\end{cases} \quad [3]$$

Let us now introduce Diophantine equation $x^2+y^2=t$, for any given t.

We can factor x^2+y^2 as $(x-\sqrt{-1}y)(x+\sqrt{-1}y)$. By this way, finding all solutions to the Diophantine equation can be transformed to the problem of finding all Gaussian integers of the form $x+\sqrt{-1}y$ with the norm t.

The discriminant of the binary quadratic form $ax^2+bxy+cy^2=0$ is given by the formula $D=b^2-4ac$.

Let us assume that D is any integer and consider the Pell: type Diophantine Equation

$x^2-dy^2=t$, for any t given. We can factor it as follows: $x^2-dy^2=(x+\sqrt{d}y)(x-\sqrt{d}y)$

We can consider the set of complex numbers of the form $x+y\sqrt{d}$, $x,y \in \mathbf{Z}$

If we choose $d=-1$ then the set defines the Gaussian integers.

$I_{-1}=\{x+y\sqrt{-1}:\ x \text{ and } y \in \mathbf{Z}\}$ are Gaussian integers since $-1 \equiv 3 (\mathrm{mod}\, 4)$

$I_5=\left\{x+y\frac{1+\sqrt{5}}{2}:\ x \text{ and } y \in \mathbf{Z}\right\}$ are Gaussian integers since $5 \equiv 1 (\mathrm{mod}\, 4)$

If $K=Q(\sqrt{d})$, then $O_K=I_d$, the ring of integers of this quadratic field is given by

$$I_d=\begin{cases}\left\{1, \dfrac{1+\sqrt{d}}{2}\right\} & \text{when } d \equiv 1 \pmod 4 \\ \{1, \sqrt{d}\}, & \text{when } d \equiv 2,3 \pmod 4\end{cases} \qquad [4]$$

If $d \equiv 1 (\mathrm{mod}4)$ then $d_K=\begin{vmatrix} 1 & 1 \\ \frac{1+\sqrt{d}}{2} & \frac{1-\sqrt{d}}{2}\end{vmatrix}^2=\left(\frac{1-\sqrt{d}}{2}-\frac{1+\sqrt{d}}{2}\right)^2=d$

If $d \equiv 2,3 (\mathrm{mod}4)$ then $d_K=\begin{vmatrix} 1 & 1 \\ \sqrt{d} & -\sqrt{d}\end{vmatrix}^2=(-\sqrt{d}-\sqrt{d})^2=4d$

$$\text{In summary, } d_K=\begin{cases} d, & \text{if } d \equiv 1 (\mathrm{mod}4) \\ 4d, & \text{if } d \equiv 2,3 (\mathrm{mod}4)\end{cases}$$

2.4. Algebraic Numbers:Integers:Algebraic Number Fields

Definition 2.4.1.

A number $\alpha \in C$ (complex number) is called an algebraic number if there exists a polynomial

$f(x)=a_n x^n+a_{n-1}x^{n-1}+...+a_1 x+a_0$

such that $a_0, a_1, ..., a_n$ not all zero, are in Q and $f(\alpha)=0$

If α is the root of the monic polynomial with coefficients in **Z**, we say that α is an algebraic integer.

Clearly, all algebraic integers are algebraic numbers. However, the converse is not true.

Exercise 2.4.1.

If $r \in Q$ is an algebraic integer, then $r \in \mathbf{Z}$.

Solution.

Let $r=\frac{c}{d}$, (c,d)=1 be an algebraic integer.

Then r is the root of a monic polynomial in $Z[x]$, say $f(x)=x^n+b_{n-1}x^{n-1}+...+b_0$.

Therefore, $f(r)=\left(\frac{c}{d}\right)^n+b_{n-1}\left(\frac{c}{d}\right)^{n-1}+...+b_0 \Leftrightarrow c^n+b_{n-1}c^{n-1}d+...+b_0 d^n=0$

This implies that d is a factor of c^n, which is true only if $d=\pm 1$. So, $r=\pm c \in \mathbf{Z}$.

Exercise 2.4.2.

If 4 is a factor of $(d+1)$ then $\frac{-1+\sqrt{-d}}{2}$ is an algebraic integer

Solution.

Consider the monic polynomial $x^2+x+\frac{d+1}{4} \in \mathbf{Z}[x]$ when 4 divides (d+1).

The roots of this polynomial, which by definition are algebraic integers,

are $x=\frac{-1\pm\sqrt{1-4\frac{d+1}{4}}}{2}=\frac{-1\pm\sqrt{-d}}{2}$.

Exercise 2.4.3.

Find the minimal polynomial of $\sqrt{n}$ where n is a squarefree integer.

Solution.

If n=1, the minimal polynomial is x-1.

If $n \geq 1$, then $x^2 - n$ is irredicuble and has $\sqrt{n}$ as a root. Thus, the minimal polynomial is either linear or quadratic. If it is linear, we obtain that $\sqrt{n}$ is rational, a contradiction. Therefore, $x^2 - n$ is the minimal polynomial of $\sqrt{n}$ when $n \geq 1$.

Definition 2.4.2. Let α be an element of $Q(\sqrt{d})$. We say that α is an algebraic integer of $Q(\sqrt{d})$ if Tr (α) and N (α) are ordinary integers where Tr (α) and N (α) are defined as follows: Let $\alpha = s + t\sqrt{d}$.

Then the trace of α denoted by $Tr(\alpha)$, is defined as $Tr(\alpha) = \alpha + \alpha' = 2s$.

The norm of α, denoted $N(\alpha)$, is defined as $N(\alpha) = \alpha\alpha' = s^2 - t^2 d$.

The norm will be one of the primary tools that we will use in the theory of quadratic fields. The set of algebraic integers in $Q(\sqrt{d})$ is denoted by I_d.

Lemma 2.4.1.

If K is an algebraic number field of degree n over Q, and $\alpha \in O_K$, the ring of integers, then Tr(α) and N(α) are in **Z**.

Definition 2.4.3. (Integral Basis)

Let K be an algebraic number field of degree n over Q, and O_K its ring of integers. We say that $w_1, w_2, ..., w_n$ is an integral basis for K if $w_i \in O_K$ for all i, and $O_K = \mathbf{Z}w_1 + \mathbf{Z}w_2 + ... \mathbf{Z}w_n$.

Theorem 2.4.1.

$K = Q\left(\sqrt{D}\right)$ with D square free integer. Find an integral bases for O_K

Solution:

$\mathrm{Tr}(\alpha)=2r_1$ and $N(\alpha)=\left(r_1+r_2\sqrt{D}\right)\left(r_1-r_2\sqrt{D}\right)=r_1^2-Dr_2^2$ are both integers.

We also note that since α satisfies the monic polynomial $x^2-2r_1x+r_1^2-Dr_2^2$, if $\mathrm{Tr}(\alpha)$ and $N(\alpha)$ are integers, then α is an algebraic integer.

We will discuss two cases.

Case 1. $D\equiv 1 \pmod 4$

If $D\equiv 1 \pmod 4$, and $g_1^2\equiv Dg_2^2 \pmod 4$, then g_1 and g_2 are either both even, or both odd. So, if $\alpha=r_1+r_2\sqrt{D}$ is an algebraic integer of $Q(\sqrt{D})$, then either r_1 and r_2 are both integers, or they both are fractions with denominator 2.

Case 2. $D\equiv 2,3 \pmod 4$

If $g_1^2\equiv Dg_2^2 \pmod 4$, then both g_1 and g_2 must be even.

Then a basis for Q_K is $1, \sqrt{D}$. Again, it is clear that this is an integral basis.

An arbitrary element α of K is of the form $\alpha=r_1+r_2\sqrt{D}$ with $r_1,r_2\in Q$.

If $2r_1\in \mathbf{Z}$, where $r_1\in Q$, then the denominator of r_1 can be at most 2.

We also need $r_1^2-Dr_2^2$, so the denominator of r_2 can be no more than 2.

Then let $r_1=\frac{g_1}{2}$, $r_2=\frac{g_2}{2}$, where $g_1,g_2\in \mathbf{Z}$. From the second condition, we have

$\frac{g_1^2-Dg_2^2}{4}\in \mathbf{Z}$ which means that $g_1^2-Dg_2^2\equiv 0 \pmod 4$, or $g_1^2\equiv Dg_2^2 \pmod 4$.

Theorem 2.4.2. If $D\equiv 1 \pmod 4$, show that every integer of $Q(\sqrt{D})$ can be written as $\frac{a+b\sqrt{D}}{2}$, where $a\equiv b \pmod 2$.

Solution.

An integral basis is given by $1, \frac{1+\sqrt{D}}{2}$.

Therefore, every integer is of the form $c+d\left(\frac{1+\sqrt{D}}{2}\right)=\frac{(2c+d)+d\sqrt{D}}{2}=\frac{a+b\sqrt{D}}{2}$.

Then we see that $a=2c+d$, $b=d$ satisfies $a\equiv b \pmod 2$. Conversely, if $a\equiv b \pmod 2$, writing $d=b$ and $a=2c+d$ for some c, we find

$$\frac{a+b\sqrt{D}}{2}=c+d\left(\frac{1+\sqrt{D}}{2}\right)$$ is an integer of $Q(\sqrt{D})$.

2.5. Modules

Definition2.5.1.

Let $M=\{\alpha x+\beta y\}$. M is called a module of $Q(\sqrt{d})$ and α,β [5] is called a basis of M. If α,β is any basis of M, then we write $M=\{\alpha,\beta\}$.

Let $Q(\sqrt{d})$ be a quadratic field where d is a square free integer.

Lemma 2.5.1.

Let $M=\{\alpha,\beta\}$ be a module and let a and b be two elements in M.

Then, $a\pm b$ is in M. Note that M is an additive abelian (commutative) group.

Proof.

Let $a=\alpha x_1+\beta y_1$, and $b=\alpha x_2+\beta y_2$, where x_1,x_2,y_1,y_2 are all in $\mathbf{Z}$. So,

$a\pm b=\alpha x_1+\beta y_1+\alpha x_2+\beta y_2=\alpha(x_1\pm y_1)+\beta(y_1\pm y_2)$ belongs to M.

Since M is a module, α and β are not uniquely determined by M. In other words, M may have many different bases. Assume that α,β and α_1,β_1 are bases of $Q(\sqrt{d})$.

We know that α and β belong to $\{\alpha,\beta\}$

Then, we may write $\alpha=\alpha_1x_1+\beta y_1$, and $\beta=\alpha_1z_1+\beta_1w_1$.

$$\text{Hence, } \alpha=\alpha_1x_1+\beta_1y_1=(\alpha x+\beta y)x_1+(\alpha z+\beta w)y_1=\alpha xx_1+\beta yx_1+\alpha zy_1+\beta wy_1$$
$$=\alpha(xx_1+zy_1)+\beta(yx_1+wy_1)$$
$$\beta=\alpha_1z_1+\beta_1w_1=(\alpha x+\beta y)z_1+(\alpha z+\beta w)w_1=\alpha xz_1+\beta yz_1+\alpha zw_1+\beta ww_1$$
$$=\alpha(xz_1+zw_1)+\beta(yz_1+ww_1)$$

Wit

h $xx_1+zy_1=1$, $yx_1+wy_1=0$, $xz_1+zw_1=0$, and $xz_1+zw_1=1$

When we substitute the second set of equations in the first one, by considering the fact that α and β is a basis of $Q(\sqrt{d})$, we have the following:

$$\begin{bmatrix} x_1 & y_1 \\ z_1 & w_1 \end{bmatrix}\begin{bmatrix} x & y \\ z & w \end{bmatrix}=\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Then, by calculating the determinant on both sides, we have $x_1w_1-z_1y_1=\pm1$

Proposition 2.5.1.

Let α,β and α_1,β_1 be the bases of $Q(\sqrt{d})$ and assume that $\{\alpha,\beta\}=\{\alpha_1,\beta_1\}$. Then there exists integers x_1,y_1,z_1, and w_1 such that

$$\begin{bmatrix}\alpha\\ \beta\end{bmatrix}=\begin{bmatrix}x_1 & y_1\\ z_1 & w_1\end{bmatrix}\begin{bmatrix}\alpha_1\\ \beta_1\end{bmatrix} \quad \text{and} \quad \det\begin{bmatrix}x_1 & y_1\\ z_1 & w_1\end{bmatrix}=\pm 1$$

Let α and β belong to $Q(\sqrt{d})$. The determinant $\begin{vmatrix}\alpha & \alpha'\\ \beta & \beta'\end{vmatrix}=(\alpha\beta'-\beta\alpha')$ is called the discriminant of α and β.

We know that the discriminant of the binary quadratic form $ax^2+bxy+cy^2=0$ *is* given by the formula $D=b^2-4ac$.

Exercise 2.5.1.

Find the discriminant of $x^2+4xy+5y^2$ and compute the module associated with this binary quadratic form.

Solution.

$D=b^2-4ac=16-4\cdot1\cdot5=-4$. Therefore, $s^2d \Rightarrow s=2$ and $d=-1$.

$M=\{\alpha,\beta\}$, where $\alpha=a$ and $\beta=\frac{b+s\sqrt{d}}{2}$. Substituting, $\alpha=1$ and $\beta=\frac{4+2\sqrt{-1}}{2}$

$$\det M=\begin{vmatrix}1 & 1\\ 2+\sqrt{-1} & 2-\sqrt{-1}\end{vmatrix}^2=\left(\left(2-\sqrt{-1}\right)-\left(2+\sqrt{-1}\right)\right)^2=\left(2\sqrt{-1}\right)^2=-4.$$

2.6

Quadratic Residues, Jacobi and Kronecker Symbols

i. Quadratic Residues

Definition 2.6.1.

For n>0, if the modulo equation $x^n \equiv a(\mathrm{mod}m)$ congruency has a solution, then a is called power residue mod m, n.

For n=2, it is quadratic residue, n =3, cubic residue, and so on. For example, $x^2 \equiv 3(\mathrm{mod}5)$ does not have a solution since one can easily show that $\{0,\pm1,\pm2\}$ does not satisfy the inequality. Then, 3 mod 5 is not a quadratic residue.

On the other hand, $x^2 \equiv -3(\mathrm{mod}7)$ has the solutions ±2. That means, −3 mod 7 is a quadratic residue. By the help of Euler Criteria, we can understand whether $x^n \equiv a$ has a solution in the following way: Let p be a prime number and $n \geq 2$. $x^n = a(\mathrm{mod}p)$ has a solution if and only if $a^{\frac{p-1}{2}} \equiv 1(\mathrm{mod}p)$. Let us express this theorem for n=2.

Proposition 2.6.1. (Euler Criteria)

Let p≠2 be a prime number and p is not a divisor of a. Then, $x^2 = a(\mathrm{mod}p)$ has a solution if and only if $a^{\frac{p-1}{2}} \equiv 1(\mathrm{mod}p)$ [6]

Proposition 2.6.2.

For p≠2, p prime number, $\frac{p-1}{2}$ class mod p is quadratic residue, $\frac{p-1}{2}$ (the other half), is not quadratic residue.

Proof. Mod p will take one of the values in $\{\pm1,\pm2,...\pm\frac{p-1}{2}\}$ When we take the square of each number in this set, $\{1,2^2,...(\frac{p-1}{2})^2\}$. These numbers are all different from each other, and we have $\frac{p-1}{2}$ such numbers. The remaining numbers in the are not quadratic residues.

Exercise 2.6.1.

Quadratic residues mod 11 are $\{1,2^2,3^2,4^2,5^2\}$, which can be list $\{1,3,4,5,9\}$

Definition 2.6.2.

Let p≠2 be a prime number.

$$\left(\frac{a}{p}\right)=\begin{cases}1, \text{ if } p \text{ is not a divisor of a and a is a quadratic residue } (\text{mod} p)\\ -1 \text{ if } p \text{ is not a divisor of a and a is not a quadratic residue } (\text{mod} p)\\ 0 \text{ if } p \text{ is a divisor of a}\end{cases}$$

$\left(\frac{a}{p}\right)$ is called the Legendre Symbol.

Exercise 2.6.2.

Let $p\neq 2$ be a prime number. Then, $\sum_{k=1}^{p-1}\left(\frac{k}{p}\right)=0$, for $1 \le k \le p-1$, since for half and for the other half of the numbers in $1 \le k \le p-1$, $\left(\frac{k}{p}\right)=-1$. Then, their sum will be equal to 0. The list below shows the properties of Legendre Symbol:

i. $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} (\text{mod } p)$

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

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

iv. If p is not a divisor of c then $\left(\frac{ac^2}{p}\right) = \left(\frac{a}{p}\right)$

Proof.

Using the Euler Criterion, if p is not a factor of a, then,

i. Since $\left(\frac{a}{p}\right)=1$, if and only if $a^{\frac{p-1}{2}} \equiv 1 (\text{modp})$, it follows that $\left(\frac{a}{p}\right)= a^{\frac{p-1}{2}} (\text{modp})$

If p is a factor of p, then it is obvious that $a^{\frac{p-1}{2}} \equiv 0 =\left(\frac{a}{p}\right)= (\text{modp})$

ii. From the equivalences $\left(\frac{a}{p}\right)= a^{\frac{p-1}{2}} (\text{modp})$ and $\left(\frac{b}{p}\right)= b^{\frac{p-1}{2}} (\text{modp})$, we can easily obtain $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)=\left(\frac{ab}{p}\right)$

iii. If $a \equiv b \pmod p$, then the congruency $x^2 \equiv a \pmod p$, and $x^2 \equiv b \pmod p$ are equal. Then,

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

iv. If p is not a factor of c then $x^2 \equiv c^2 \pmod p$ has a solution and $\left(\frac{c^2}{p}\right)=1$

From the properties listed above,

$$\left(\frac{ac^2}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{c^2}{p}\right)=\left(\frac{a}{p}\right) \qquad [7]$$

Exercise 2.6.3.

Using Legendre Symbol, let us calculate $\left(\frac{1001}{9907}\right)$.

$$\left(\frac{1001}{9907}\right)=\left(\frac{13}{9907}\right)\left(\frac{11}{9907}\right)\left(\frac{7}{9907}\right)$$

$$\left(\frac{13}{9907}\right)=\left(\frac{9907}{13}\right)=\left(\frac{1}{13}\right)=1. \qquad \left(\frac{11}{9907}\right)=-\left(\frac{9907}{11}\right)=-\left(\frac{7}{11}\right)=\left(\frac{11}{7}\right)=\left(\frac{4}{7}\right)=1$$

$$\left(\frac{7}{9907}\right)=-\left(\frac{9907}{7}\right)=-\left(\frac{2}{7}\right)=-1 \qquad \text{Therefore, } \left(\frac{1001}{9907}\right)=1\times(-1)\times1=-1$$

ii. Jacobi Symbol

Jacobi symbol is simply the generalization of the Legendre symbol given above. This symbol has its main use in computational number theory, and very important in cryptography.

Definition 2.6.3.

For any given integer a and any odd number n which is positive, we can define the Jacobi symbol as the product of the Legendre symbols that correspond to the prime factors of

n. $\left(\frac{a}{n}\right)=\left(\frac{a}{p_1}\right)^{\alpha_1}\left(\frac{a}{p_2}\right)^{\alpha_2}\left(\frac{a}{p_3}\right)^{\alpha_3}....\left(\frac{a}{p_k}\right)^{\alpha_k}$ where $\left(\frac{a}{p}\right)$ shows the Legendre symbol defined above.

We can list some properties of Jacobi symbol as follows.

1. If $a\equiv b\,(\mathrm{mod}\,n)$ then $\left(\frac{a}{n}\right)=\left(\frac{b}{n}\right)$
2. $\left(\frac{a}{n}\right)=\begin{cases}0 & \text{if } \gcd(a,n)\neq 1\\ \pm 1 & \text{if } \gcd(a,n)=1\end{cases}$
3. $\left(\frac{ab}{n}\right)=\left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$. Therefore, $\left(\frac{a^2}{n}\right)=1,$ or $0.$
4. $\left(\frac{a}{mn}\right)=\left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$. Therefore, $\left(\frac{a^2}{n}\right)=1,$ or $0.$

For example, $\left(\frac{8}{15}\right)=\left(\frac{8}{3}\right)\left(\frac{8}{5}\right)=\left(\frac{2}{3}\right)\left(\frac{3}{5}\right)=(-1)\times(-1)=1$

By using the Jacobean symbol, we can calculate $\left(\frac{1001}{9907}\right)$ as follows.

$$\left(\frac{1001}{9907}\right)=\left(\frac{9907}{1001}\right)=\left(\frac{898}{1001}\right)=\left(\frac{449}{1001}\right)\left(\frac{2}{1001}\right)=\left(\frac{449}{1001}\right)=\left(\frac{1001}{449}\right)=\left(\frac{103}{449}\right)=\left(\frac{449}{103}\right)=\left(\frac{37}{103}\right)$$

$$=\left(\frac{103}{37}\right)\left(\frac{29}{37}\right)=\left(\frac{37}{29}\right)=\left(\frac{8}{29}\right)=\left(\frac{2}{29}\right)\left(\frac{4}{29}\right)=-1$$

Note that Jacobi's symbol extends to Legendre symbol; if n is prime. Also note that $\left(\frac{a}{n}\right)=0$ if a and are not coprime. Assume that $n=p_1^{e_1}p_2^{e_2}...p_r^{e_r}$.

a is a quadratic residue $(\mathrm{mod}\,n)\Leftrightarrow$ it is a quadratic residue $\mathrm{mod} p_i^{e_i}$ for $i=1,....,r.$

This implies the following:

a is a quadratic residue $\mathrm{mod} p_i$ for each $i;$ and so $\left(\frac{a}{n}\right)=1.$

However, the converse is not true.

Definition 2.6.4.

p is prime and m is a residue(mod p) given. Then,

$$\left(\frac{m}{p}\right)=(-1)^{\left(\frac{p-1}{2}\right)\left(\frac{m-1}{2}\right)}\left(\frac{p}{m}\right) \qquad [8]$$

Proposition 2.6.3.

Assume that $m,n \in N$ are odd numbers. Therefore,

$$\left(\frac{m}{n}\right)=\begin{cases}\left(\frac{m}{n}\right), & \text{if } m\equiv 1(\text{mod}4) \text{ or } n\equiv 1(\text{mod}4)\\ -\left(\frac{m}{n}\right), & \text{if } m\equiv n\equiv 3(\text{mod}4).\end{cases}$$

Proof.

If m and n are coprime, then both sides are 0. Then, we may assume that GCD(m,n)=1. We need to show that

$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right)=(-1)^{\frac{m-1}{2}\frac{n-1}{2}}$. Assume that $m=p_1p_2...p_r$ and $n=q_1q_2...q_s$

So, $\left(\frac{m}{n}\right)\left(\frac{n}{m}\right)=\prod_{i,j}\left(\frac{p_i}{q_j}\right)\left(\frac{p_i}{q_j}\right)=\prod_{i,j}(-1)^{\left(\frac{p_i-1}{2}\right)\left(\frac{q_j-1}{2}\right)}$, (by Quadratic Reciprocity Theorem)

Therefore, we have to prove that $\left(\frac{m-1}{2}\right)\left(\frac{n-1}{2}\right)\equiv\sum_{i,j}\left(\frac{p_i-1}{2}\right)\left(\frac{q_j-1}{2}\right)(\text{mod}2)$

In other words, $(m-1)(n-1)\equiv\sum_{i,j}(p_i-1)(q_j-1)(\text{mod}8)$

Lemma 2.6.1.

If $a,b \in \mathbf{Z}$, are odd numbers, then $ab-1\equiv(a-1)+(b-1) \pmod 4$ [9]

Proof

Since $a,b \in Z$ are odd, then $(a-1)(b-1)\equiv 1 \pmod 4$. In other words, $ab+1\equiv a+b$.

By repeated application of the Lemma, we could see that $a_1....a_t-1\equiv\sum_i(a_i-1) \pmod 4$.

In particular, $m-1\equiv(p_1-1)+.....+(p_r-1) \pmod 4$

Since n-1 is an even number $(m-1)(n-1)\equiv(p_1-1)(n-1)+.....+(p_r-1)(n-1) \pmod 8$

Again, by the Lemma, $n-1\equiv(q_1-1)+.....+(q_s-1) \pmod 4$

Since p_i-1 is an even number,

$$(p_i-1)(n-1)\equiv(p_i-1)(q_1-1)+.....+(p_i-1)(q_s-1) \pmod 8$$

Putting these two results together, we obtain

$$(m-1)(n-1)\equiv\sum_i(p_i-1)(q_j-1) \pmod 8 \text{ as required.}$$

Exercise 2.6.4. Let us find the value of $\left(\frac{38}{165}\right)$ using the Jacobi Method.

$$\left(\frac{38}{165}\right)=\left(\frac{2}{165}\right)\left(\frac{19}{165}\right)=(-1)\left(\frac{165}{19}\right)(-1)^{\frac{165-1}{2}\cdot\frac{19-1}{2}}$$

$$=(-1)\left(\frac{165}{19}\right)=(-1)\left(\frac{13}{19}\right)=(-1)\left(\frac{19}{13}\right)(-1)^{\frac{19-1}{2}\cdot\frac{13-1}{2}}=(-1)\left(\frac{19}{13}\right)=(-1)\left(\frac{13}{19}\right)(-1)^{\frac{13-1}{2}\cdot\frac{19-1}{2}}$$

$$=(-1)\left(\frac{13}{19}\right)=(-1)\left(\frac{19}{13}\right)=(-1)\left(\frac{6}{13}\right)=(-1)\left(\frac{2}{13}\right)\left(\frac{3}{13}\right)=(-1)(-1)=1.$$

iii. Kronecker Symbol

Let a and b be two relatively prime integers. Then the Kronecker Symbol $\left(\frac{a}{n}\right)$ is defined as follows. $n=up_1^{e_1}p_2^{e_2}\ldots p_s^{e_s}$, where u is a unit.$(u=\pm1)$

Then, $$\left(\frac{a}{n}\right)=\left\{(\frac{a}{u})\prod_{i=1}^{s}(\frac{a}{p_i})^{e_i} \quad \text{where } n\geq 2\right\} \qquad [10]$$

Note that $\left(\frac{a}{1}\right)=1$ and $\left(\frac{a}{-1}\right)=\begin{cases}1 & \text{when } a^{3}0\\ -1 & \text{when } a<0\end{cases}$ and $\left(\frac{a}{2}\right)=\begin{cases}0 & \text{if } (a,2)\neq 1\\ 1 & \text{if } a\equiv\pm1(\text{mod}\,8)\\ -1 & \text{if } a\equiv\pm3(\text{mod}8)\end{cases}$

Here, $\left(\frac{a}{p_i}\right)$ is the known Legendre Symbol and $\left(\frac{a}{0}\right)=\begin{cases}1 & \text{if } a\equiv\pm1\\ 0 & \text{otherwise}\end{cases}$

Lemma 2.6.2.

Let q be an odd prime.

Exercise 2.6.5.

Compute $(5/p)$ and $(7/p)$.

Solution.

We will first compute $(5/p)$. Since $5\equiv 1\ (\text{mod}4)$, we can use part (a) of the previous Lemma. $-\left(\frac{5}{p}\right)=\left(\frac{p}{5}\right)(-1)^{\frac{5-1}{2}\cdot\frac{p-1}{2}}$

So $(5/p)=1 \Leftrightarrow p \equiv r(\text{mod}5)$, where r is a quadratic residue mod5. It is easy to determine which r are quadratic residues mod5. $1^2 \equiv 1, 2^2 \equiv 4, 3^2 \equiv 4, 4^2 \equiv 1$. So,1 and 4 are quadratic residues mod5, while 2 and 3 are not. Thus

$$\left(\frac{5}{p}\right)=\begin{cases} 1 & \text{if } p \equiv 1,4 \pmod 5 \\ -1 & \text{if } p \equiv 2,3 \pmod 5 \\ 0 & \text{if } p \equiv 5. \end{cases}$$

$1^2, 13^2, 15^2, 27^2 \equiv 1 \pmod{28}$ $3^2, 11^2, 17^2, 25^2 \equiv 9 \pmod{28}$ $5^2, 9^2, 17^2, 23^2 \equiv 25 \pmod{28}$

Thus,
$$\left(\frac{7}{p}\right)=\begin{cases} 1 & \text{if } p \equiv \pm 1, \pm 9, \pm 25 \pmod{28} \\ -1 & \text{if } p \equiv \pm 5, \pm 11, \pm 13 \pmod{28} \\ 0 & \text{if } p \equiv 7. \end{cases}$$

Exercise 2.6.6.

$x^4 \equiv 25 \pmod{1013}$ has no solution.

Solution.

First, observe that 1013 is prime. If $x^4 \equiv 25 \pmod{1013}$ had a solution x_0, then $x_0^2 \equiv \pm 5 \pmod{1013}$. However, $\left(\frac{\pm 5}{1013}\right)=\left(\frac{5}{1013}\right)=\left(\frac{1013}{5}\right)=\left(\frac{3}{5}\right)=-1$.

So the congruence has no solutions.

CHAPTER 3

ALGEBRAIC RING OF INTEGERS O_K

3.1. Ring of Integers

Definition 3.1.1.

A ring $(R,+,\times)$ is an algebraic structure consisting of a set together with two binary operations(usually called addition and multiplication) where each operation combines two elements to form a third element. The ring R is a commutative group. A ring isomorphism between the rings R and S is a one:to:one correspondence

$f: R \rightarrow S$ which preserves the ring operations:

$f(x+y) = f(x) + f(y)$ and $f(x \cdot y) = f(x) \cdot f(y)$

If a ring R has a unit, which is an identity element for multiplication, then the ring is called ring with a unit element. i.e. a number 1 such that 1a = a1 = a for every element a of the ring R. A commutative ring is a ring with commutative multiplication. The integers $\mathbf{Z}$ are a commutative ring with a unit. The even integers are a commutative ring without a unit. Note that 1 is not an element of the set of even integers.

In order to find a solution to many problems in Number Theory, the arithmetic in the set integers needs to be expanded to algebraic integers. For example, Gaussian Integer ring is defined in $Q(\sqrt{-1})$.

As an application, Diophantine Equation $x^2 + y^2 = n$, could be investigated.

Definition 3.1.2.

A Gaussian integer is a complex number of the form a + bi, where a and b are integers and $i = \sqrt{-1}$. The set of all Gaussian integers will be denoted $\mathbf{Z}[i]$

For example, 2 = 2+0i, 3+5i , 7-4i are all examples of Gaussian integers. All integers in Z are also Gaussian integers since $n = n + 0i$.

The ring of integers of this quadratic field is given by

$$I_d = \begin{cases} \left\{1, \dfrac{1+\sqrt{d}}{2}\right\} & \text{when } d \equiv 1 \pmod 4 \\ \left\{1, \sqrt{d}\right\}, & \text{when } d \equiv 2,3 \pmod 4 \end{cases}$$

$$\text{If } d \equiv 1 (\text{mod} 4) \text{ then } d_K = \begin{vmatrix} 1 & 1 \\ \dfrac{1+\sqrt{d}}{2} & \dfrac{1-\sqrt{d}}{2} \end{vmatrix}^2 = \left(\frac{1-\sqrt{d}}{2} - \frac{1+\sqrt{d}}{2}\right)^2 = d$$

$$\text{If } d \equiv 2,3 (\text{mod} 4) \text{ then } d_K = \begin{vmatrix} 1 & 1 \\ \sqrt{d} & -\sqrt{d} \end{vmatrix}^2 = (-\sqrt{d} - \sqrt{d})^2 = 4d$$

$$\text{In summary, } d_K = \begin{cases} d, & \text{if } d \equiv 1 (\text{mod} 4) \\ 4d, & \text{if } d \equiv 2,3 (\text{mod} 4) \end{cases}$$

Proposition 3.1.1.

Let a and b be Gaussian integers. a+ b, a–b, and ab are all Gaussian. The fundamental theorem of arithmetic says integers can uniquely be factorized. We will discover to where the unique factorization does not work. Here, is the problem. Factorization is meaningful only if we have a subring in a field, then we need to define ring of integers.

Exercise 3.1.1.

$Q(\sqrt{-5})$ is a ring such that $Q(\sqrt{-5}) = \left\{a+b\sqrt{-5} : a,b \in Q\right\}$

In this ring, numbers may not have the unique factorization. (Non existence of unique factorization)

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

Let a be a square: free integer which is not equal to 0 or 1. Then, the quadratic number field

$Q(\sqrt{a}) = Q + Q\sqrt{a} = \left\{x + y\sqrt{b}, \text{ where } x,y \in Q\right\}$ is the called the smallest subfield of complex numbers field C containing both Q and $\sqrt{a}$.

$m \in Q(\sqrt{a})$ is an algebraic integer if it is a zero(root) of a monic polynomial z^2+bz+c, where b and z are in $\mathbf{Z}$.

In this case, it is obvious that $Q(\sqrt{a})$ is the subring

$$\text{of } O_a = \begin{cases} Z + Zw_d & \text{whenever } d \equiv 2,3 \pmod 4 \\ Z + Zw_d & \text{whenever } d \equiv 1 \pmod 4 \end{cases}$$

O_{-1} is the ring of Gaussian integers. In Q_{-5}, unique factorization does not work.

$I_{-1}=(2+i)(2-i)=(1+2i)(1-2i)$

Exercise 3.1.2.

Determine the algebraic integers of $K=Q(\sqrt{-5})$.

Solution.

We first note that $1, \sqrt{-5}$ form a Q-basis for K.

Therefore, any $\alpha \in K$ looks like $\alpha=r_1+r_2\sqrt{-5}$, with r_1 and $r_2 \in Q$.

Since $[K:Q]=2$, we can deduce that the conjugates of α are $r_1+r_2\sqrt{-5}$ and $r_1-r_2\sqrt{-5}$.

Then $Tr(\alpha)=2r_1$ and $N(\alpha)=(r_1+r_2\sqrt{-5})(r_1-r_2\sqrt{-5})=r_1^2+5r_2^2$.

We know that if $\alpha \in Q_K$, then the trace and the norm are integers.

Also, α is a root of the monic polynomial $x^2-2r_1x+r_1^2+5r_2^2$ which is in $\mathbf{Z}[x]$ when the trace and norm are integers. We conclude that for $\alpha=r_1+r_2\sqrt{-5}$ to be in O_K, it is necessary and sufficient that $2r_1$ and $r_1^2+5r_2^2$ are integers. This implies that r_1 has a denominator at most 2, which forces the same for r_2.

Then by setting $r_1=\frac{g_1}{2}$ and $r_2=\frac{g_2}{2}$, we must have $\left(\frac{g_1^2+5g_2^2}{4}\right) \in \mathbf{Z}$

or equivalently $g_1^2+5g_2^2 \equiv 0 \pmod 4$, we conclude that g_1 and g_2 are themselves even, and thus $r_1, r_2 \in \mathbf{Z}$. We conclude that $Q_K=\mathbf{Z}+\mathbf{Z}\sqrt{-5}$.

3.2. Coefficient Ring of a Module

In this section we will concentrate on a fixed module M and rational number r. Look at the problem of finding all ζ in M such that

$N(\zeta)=r$, where N is the norm.

Assume that ε is a number of $Q(\sqrt{d})$ satisfying

$N(\varepsilon)=1$. Also, note that $N(\varepsilon\zeta)=1$.

Proposition 3.2.1.

Assume that $\zeta \in M$ and $N(\zeta)=r$.

Also, let $\varepsilon \in Q(\sqrt{d})$, satisfying $\varepsilon M \subseteq M$ and $N(\varepsilon)=1$. Then, $\varepsilon\zeta \in M$ and $N(\varepsilon\zeta)=r$.

Definition 3.2.

The set of all elements η of $Q(\sqrt{d})$ with the property $\eta M \subseteq M$ is called the ring of coefficients of M and will be denoted by Q_M

Lemma 3.2.1.

Let γ be an element of $Q(\sqrt{d})$ and let $M=(\alpha,\beta)$. Then, the following holds: γ be an element of $Q_M \Leftrightarrow \gamma\alpha$ and $\gamma\beta$ is in M. [11]

Proof.

Assume that γ is an element of Q_M.

Then, $\gamma M \subseteq M$ implies that $\alpha,\beta \in M$ and $\gamma\alpha,\gamma\beta \in M$.

Conversely, assume that $\gamma\alpha$ and $\gamma\beta$ is in M.

Then, $\gamma\alpha=\alpha x+\beta y$, for some $x,y \in Z$, and $\gamma\beta=\alpha z+\beta w$, for some $z,w \in \mathbf{Z}$.

$\mu=\alpha x+\beta y$. Multiplying each side by γ gives $\mu\gamma=\gamma(\alpha x+\beta y)=\gamma\alpha x+\gamma\beta y=(\alpha x_1+\beta y_1)x+(\alpha z_1+\beta w_1)y$
$=\alpha x_1 x+\beta y_1 x+\alpha z_1 y+\beta w_1 y=\alpha(x_1 x+z_1 y)+\beta(y_1 x+w_1 y) \in M$.
$=\alpha$ is an element of Q_M.

Lemma 3.2.2.

If $\gamma \in Q_M$, then $\gamma \in I_d$. Thus, Q_M is a subring of I_d.

Proof.

$M=\{\alpha,\beta\}$ and $\gamma \in Q_M$. Since $\gamma \in Q_M$, $\gamma\alpha=\alpha x+\beta y$, and $\gamma\beta=\alpha z+\beta w$, $x,y,z,w \in \mathbf{Z}$.

We can rewrite these two equations as $\alpha(x-\gamma)+\beta y=0$ and $\alpha w+\beta(z-\gamma)=0$

If we solve the system of equations, we can see that $(x-\gamma)(z-\gamma)-wy=0$

That means, γ satisfies the equation $\gamma^2-(x+z)\gamma+(xz-wy)=0$

By Quadratic formula, we can see that $(X-\gamma)(X-\gamma)=X^2-(x+z)X+(xz-wy)$.

Note that $Tr(\gamma)=x+z$ and $N(\lambda)=xz-wy$ are integers.

Exercise 3.2.1.

If $\gamma=3+2\sqrt{3}$, then $Tr(\gamma)=2\cdot 3=6$, $N(\gamma)=9-12=-3$.

γ is a root of the equation $x^2-6x-3=0$. Let us check if $3+2\sqrt{3}$ verifies the equation above.

$\left(3+2\sqrt{3}\right)^2-6\left(3+2\sqrt{3}\right)-3=9+12\sqrt{3}+12-18-12\sqrt{3}-3 = 9+12-18-3 = 0.$

Definition 3.2.2.

Let $Q(\sqrt{d})$ be a quadratic field and M be a fixed module.

The set of elements α of $Q(\sqrt{d})$ having the property that $\alpha M \subset M$ is called the ring of coefficients of M and will be denoted by O_M. O_M indeed is a ring. The following is standard and will be given without the proof.

Theorem 3.2.1.

There exists a positive rational integer L such that $O_M=\{1,Lw_d\}$.

The rational integer L is characterized by as the least positive rational integer such that Lw_d is in O_M. [12]

CHAPTER 4

UNITS

4.1. Introduction to Units

We can discuss the concept of divisibility for any commutative ring $\square_M$ with identity.

Definition 4.1.1.

A unit of the ring $Q(\sqrt{d})$ is an element u of $Q(\sqrt{d})$ such that u^{-1} belongs to $(\sqrt{d})$.

Proposition 4.1.1.

The units of $Q(\sqrt{d})$ are the elements of the norm one and negative one in $Q(\sqrt{d})$.

Proof.

Let us assume that $u \in Q(\sqrt{d})$ is a unit. Then,

$1 = N(1) = N(uu^{-1}) = N(u).N(u^{-1})$.

Since $N(u)$ and $N(u^{-1})Z$, we have $N(u) = N(u^{-1}) = \pm 1$

Example: Let $Q(\sqrt{-2}) = \{1, 7\sqrt{-2}\}$. Is $2+7\sqrt{-2}$ unit in $Q(\sqrt{-2})$?

$N(2+7\sqrt{-2}) = (2+7\sqrt{-2})(2-7\sqrt{-2})$

$= 4+49\square 2$

$= 102 \neq \pm 1$. Consequently, $2+7\sqrt{-2}$ is not a unit in $Q(\sqrt{-2})$

Definition 4.1.2.

We will say that a and b are associates and write $a \square b$ if there exists a unit $u \in R$. such that $a=bu$. It is easy to verify that $\square$ is an equivalence relation.

If R is an integral domain and we have a,b¹0 with a divides b,and b divides a, then a and b must be associates, for then $\exists c, d \in R$ such that $ac = b$ and $bd = a$, which implies that bdc=b.Since we are in an integral domain, dc=1, and d,c are units.

Definition 4.1.3.

$a \in R$ is irreducible if for any factorization a=bc, one of b or c is a unit.

Let R be a number field and I_d be the ring of integers in K.

Proposition 4.1.2.

Assume that $u \in R$. Then, u is a unit in R $\Leftrightarrow$ u is an integer of R with the norm ±1.

[13]

Proof.

If u is a unit of R, then N (u) and N (u^{-1}) is in Z. Then, we have, N (u) N (u^{-1}) = N ($u \cdot u^{-1}$) =1, so N (u) = ±1.

Conversely, let u be an integer of K with the norm ±1.

It has the characteristic equation of the form $u^n+a_{n-1}u^{n-1}+...+a_1u\pm1=0$, all $a_i \in Z$.

Consequently, $\pm(u^{n-1}+u_{n-1}x^{n-2}...+a_1)=u^{-1}$ and, since u^{-1} is an integer of K, u is a unit.

Unit theorem implies that there exist r, (such that $r=r_1+r_2-1$), units (u_i) of K such that any unit u of K may be uniquely expressed in the form

$u=zu_1^{n_1}....u_r^{n_r}$, with $n_i \in Z$ and z a root of unity.

The set (u_i), i=1,2,…,r, is called a fundamental system of units of K.

4.2. Units in Imaginary Quadratic Fields

Let $K = Q[\sqrt{-d}]$ be an imaginary field, where d is a square free integer.

i. If $d \equiv 1$ or 2 (mod 4), the ring of integers I_d of K is $\mathbf{Z} + \mathbf{Z}\sqrt{-d}$.

For $x = a + b\sqrt{-d}$ $(a, b \in Z)$, we have $N(x) = a^2 + db^2 \geq 0$.

If x is a unit, we should have $a^2 + db^2 = 1$.

If $d \geq 2$, this implies that b=0 and $a = \pm 1$. Then, $x = \pm 1$.

If d=1, then besides the solution $x = \pm 1$, there are other solutions

$a = 0, b = \pm 1$. In other words, $x = \pm i$.

ii. If $d \equiv 3$ (mod 4), the ring of integers I_d of K is $Z + Z\left[\frac{1+\sqrt{-d}}{2}\right]$.

$a+b\left(\frac{1+\sqrt{-d}}{2}\right)$, a and b are integers, we have $N(x)=\left(a+\frac{b}{2}\right)^2+\frac{db^2}{4}$

If x is a unit, we must have $(2a+b)^2+db^2=4$

If $m \geq 7$, then b=0, so $2a^2=4$, $a = \pm 1$, and $x=\pm 1$.

If d=3, then the relations $b=\pm 1$, and $(2a+1)^2=\pm 1$ will give us the solutions

$x=\left(\frac{\pm 1 \pm \sqrt{-3}}{2}\right)$, where the signs ± are independent.

Proposition 4.2.1.

Let K be a quadratic imaginary number field. Then, G, the group of units in K has the units +1 and −1 except the following two cases:

1. If $K=Q[i]$, where $i^2=-1$, then G has the units $i, -1, -i, 1$.
2. If $K=Q\left[\sqrt{-3}\right]$, then G has the units $\left[\frac{1+\sqrt{-3}}{2}\right]^j$, where $j=0,1,2,3,4,5$

4.3. Units in Real Quadratic Fields

Let K be a real quadratic field. The unit theorem implies that the group of units of K is isomorphic to the product of Z, where the groups of roots of unit elements are in K.

Since K is a real quadratic field, the only roots of units are ±1.

Proposition 4.3.1.

The positive units of a real quadratic field K form a multiplicative group which is isomorphic to Z.

Let $K=Q\left[\sqrt{d}\right]$, where $d \geq 2$ is a square free number.

Also, let $x=a+b\sqrt{d}$, a and b are rational numbers.

Then, the numbers $x, x^{-1}, -x, -x^{-1}$ are all units of K.

Since $N(x)=(a+b\sqrt{d})(a-b\sqrt{d})=\pm 1$, the four numbers will be of the form $\pm a \pm b\sqrt{d}$.

For $x \neq \pm 1$, only one of the four numbers $x, x^{-1}, -x, -x^{-1}$ is greater than one.

The units greater than one of K are those of the form $a+b\sqrt{d}$ where $a,b \in Z^{+}$.

Here we have some cases:

i. Assume that $d \equiv 2 \text{ or } 3 \pmod 4$. In this case the ring of integers I_d is $\mathbf{Z}+\mathbf{Z}\sqrt{d}$.

Since the units are of the form ±1, the units greater than one in K are the numbers $a+b\sqrt{d}$, with $a,b>0$, $a, b \in \mathbf{Z}$ such that $a^2-db^2=\pm 1$.

The solutions (a,b) in natural numbers of the equation (called the equation of Pell:Fermat) are obtained as follows:

Take the fundamental unit $a_1+b_1\sqrt{d}$ in K.

Put $a_n+b_n\sqrt{d}=(a_1+b_1\sqrt{d})^n$, where $n \geq 1$.

It follows from $a_n+b_n\sqrt{d}=(a_1+b_1\sqrt{d})^n$ that $b_{n+1}=a_1b_n+b_1a_n$.

Since a_1, b_1, a_n, and b_n are all positive numbers, the sequence (b_n) is strictly increasing. Then, to calculate the fundamental unit, it is enough to write down the sequence

(db^2) for $b \in N^+$ and to stop at the first number db_1^2 of this sequence.

In that case, $a_1+b_1\sqrt{d}$ is the fundamental unit in K.

For example, if d=7, then the sequence db^2 is 7, 28, $63= 64-1 = 8^2-1$.

Then, taking $b_1=3$ and $a_1=8$, we see that $8+3\sqrt{7}$ is a unit in $Q\left[\sqrt{7}\right]$.

Similarly, we can see some fundamental units as follows:

Fundamental unit for $Q\left[\sqrt{2}\right]$ is $1+\sqrt{2}$, for $Q\left[\sqrt{3}\right]$ is $2+\sqrt{3}$, for $Q\left[\sqrt{6}\right]$ is $5+\sqrt{6}$.

If the fundamental unit is of norm one, the sequence (a_n,b_n) gives solutions only for the equation $a^2-db^2=1$.

In this case, the equation $a^2-db^2=-1$ has no solution in natural numbers.

If the fundamental unit has the norm -1,

a. then the solutions of the equation $a^2-db^2=1$ gives the sequence (a_{2n},b_{2n})

b. the solutions of the equation $a^2-db^2=-1$ gives the sequence (a_{2n+1},b_{2n+1}),

The first case occurs when d=3, 6, or 7, and the second case occurs when d=2, or 10. Note that $3+\sqrt{10}$ is the fundamental unit in $Q\left[\sqrt{10}\right]$

ii. Assume now that $d \equiv 1 \pmod 4$.

The integers in $K=\left[\sqrt{d}\right]$ are the numbers $\left(\frac{a+b\sqrt{d}}{2}\right)$, with $a,b \in \mathbf{Z}$

Then, if $\frac{a+b\sqrt{d}}{2}$ is a unit in K, we must have $a^2-db^2=\pm 4$. On the other hand, if (a,b) is an integer solution to $a^2-db^2=\pm 4$. Then $\frac{a+b\sqrt{d}}{2}$ is an integer in K. Note that the trace is a and its norm is ±1. Then, $\frac{a+b\sqrt{d}}{2}$ is a unit of K.

As in (i), if we write $a_1+b_1\sqrt{d}$ for the fundamental unit of K, we can see that the solutions (a,b) of $a^2-db^2=\pm 4$ will have the values of the sequence (a_n,b_n) defined by: $a_n+b_n\sqrt{d}=2^{1-n}(a_1+b_1\sqrt{d})^n$, where $n \geq 1$.

We can find $a_1+b_1\sqrt{d}$ as in the first case (i). For example,

Fundamental unit for $Q\left[\sqrt{5}\right]$ is $\frac{1+\sqrt{5}}{2}$, for $Q\left[\sqrt{13}\right]$ is $\frac{3+\sqrt{13}}{2}$, for $Q\left[\sqrt{17}\right]$ is $4+\sqrt{17}$.

Note that all these units have norm −1. For the choice of the sign ±1 in the equation $a^2-db^2=\pm 4$, we have similar results as in the first case.

We know that $I_d=\{x+yw_d:\ x,y\in \mathbf{Z}\}$, where $w_d=\begin{cases}\frac{1+\sqrt{d}}{2}, & d\equiv 1\ (\mathrm{mod}4)\\ \sqrt{d}, & d\equiv 2,3(\mathrm{mod}4)\end{cases}$

Exercise 4.3.1.

$\frac{1+\sqrt{5}}{2}$ is the fundamental unit of I_5.

Solution.

$5\equiv 1\ (\mathrm{mod}4)$, $I_d=x+y\frac{1+\sqrt{d}}{2}$. Let $x+y\frac{1+\sqrt{5}}{2}\in I_5$. Then $,\frac{1}{2}+\frac{\sqrt{5}}{2}=x+\frac{y}{2}+\frac{y\sqrt{5}}{2}, x,y\in \mathbf{Z}$.

$x+\frac{y}{2}=\frac{1}{2}$ and $\frac{y}{2}=\frac{1}{2}$. So, x=0 and y=1. Consequently, $\varepsilon_d=\frac{1+\sqrt{5}}{2}$

Example 4.3.2.

Compute the integers of I_d where d=3.

Solution.

$d=3$, and $3 \equiv 3 \pmod 4$. $I_d=x+y\sqrt{d}$, for $2,3 \pmod 4$, $I_3=x+y\sqrt{3}$.

Example 4.3.3.

Compute the integers of I_d where d=6.

Solution.

$6 \equiv 2 \pmod 4$ $I_d=x+y\sqrt{d}$, for $2,3 \pmod 4$, $I_6=x+y\sqrt{6}$.

Example 4.3.4.

Compute the integers of I_d where d=21.

Solution.

$21 \equiv 1 \pmod 4$. $I_d=x+y\frac{1+\sqrt{d}}{2}$, for $1 \pmod 4$, $I_{21}=x+y\frac{1+\sqrt{21}}{2}$.

4.4. Continued Fractions Method in Finding Fundamental Unit

Definition 4.4.1.

A finite continued fraction is of the form

$$a_0+\cfrac{1}{a_1+\cfrac{1}{a_2+\ldots+\cfrac{1}{a_{n-1}+\cfrac{1}{a_n}}}},$$

where each $a_i \in R$ and $a_i \geq 0$ for $1 \leq i \leq n$. We use the notation $[a_0,\ldots,a_n]$ to denote the above expression.

i. $[a_0,\ldots,a_n]$ is called a simple fraction if $a_0,\ldots,a_n \in \mathbf{Z}$.

ii. The continued fraction $C_k=[a_0,\ldots,a_k]$, $0 \leq k \leq n$, is called the k^{th} convergence of $[a_0,\ldots,a_n]$.

Theorem 4.4.1.

a. Consider the continued fraction $[a_0,...,a_n]$. Define the sequences $p_0,...,p_n$ and $q_0,...,q_n$ recursively as follows:

$$p_0=a_0, \qquad q_0=1,$$
$$p_1=a_0a_1+1, \qquad q_1=a_1,$$
$$p_k=a_kp_{k-1}+p_{k-2}, \qquad q_k=a_kq_{k-1}+q_{k-2}$$

for $k \geq 2$. Show that kth convergent $C_k=p_k/q_k$

b. Let p and q be prime numbers. Then, $p_kq_{k-1}-p_{k-1}q_k=(-1)^{k-1}$, for $k \geq 1$.

c. Derive the identities

$$C_k-C_{k-1}=\frac{(-1)^{k-1}}{q_kq_{k-1}}, \quad \text{for } 1 \leq k \leq n, \text{ and } \quad C_k-C_{k-2}=\frac{a_k(-1)^k}{q_kq_{k-2}}, \quad \text{for } 2 \leq k \leq n.$$

d. $C_1>C_3>C_5>...$, and $C_0<C_2<C_4<...$, and that every odd-numbered convergent C_{2j+1}, $j \geq 0$, is greater than every even-numbered convergent C_{2k}, $k \geq 0$.

Proof. *a.* We prove this by induction on k.

only on $a_0,...,a_{k-1}$, $C_{k+1}=\left[a_0,a_1...,a_{k-1},a_k+\frac{1}{a_{k+1}}\right]$

$$= \frac{\left(a_k+\frac{1}{a_{k+1}}\right)p_{k-1}+p_{k-2}}{\left(a_k+\frac{1}{a_{k+1}}\right)q_{k-1}+q_{k-2}} = \frac{a_{k+1}(a_kp_{k-1}+p_{k-2})+p_{k-1}}{a_{k+1}(a_kq_{k-1}+q_{k-2})+q_{k-1}} = \frac{a_{k+1}p_k+p_{k-1}}{a_{k+1}q_k+q_{k-1}}=\frac{p_{k+1}}{q_{k+1}}.$$

b. Again, we apply induction on k. For k=1, $p_1q_0-p_0q_1=(a_0a_1+1)\times 1-a_0a_1=1$

For $k \geq 1$, $p_{k+1}q_k-p_kq_{k+1}=(a_{k+1}p_k+p_{k-1})q_k-p_k(a_{k+1}q_k+q_{k-1})=(p_{k-1}q_k-p_kq_{k-1})=-(-1)^{k-1}=(-1)^k$ by our induction hypothesis.

c. By (b), $(p_{k-1}q_k-p_kq_{k-1})=-(-1)^{k-1}$. Dividing both sides by q_kq_{k-1}, we obtain the first identity. Now, $C_k-C_{k-2}=\frac{p_k}{q_k}-\frac{p_{k-2}}{q_{k-2}}=\frac{p_kq_{k-2}-p_{k-2}q_k}{q_kq_{k-2}}$. However, $p_kq_{k-2}-p_{k-2}q_k$

$=(a_kp_{k-1}+p_{k-2})q_{k-2}-p_{k-2}(a_kq_{k-1}+q_{k-2})$

$=a_k(p_{k-1}q_{k-2}-p_{k-2}q_{k-1})=a_k(-1)^{k-2}$

establishing the second identity.

d. By (c), C_k

In addition, $C_{2m}-C_{2m-1}=$

Definition 4.4.2.

We define the continued fraction $[a_0,a_1,.....]$ to be the limit as $k \to \infty$ of its kth convergent C_k. $[a_0,a_1,.....]=\lim_{k\to\infty} C_k$.

Theorem 4.4.2.

Let $\alpha=\alpha_0$ be an irrational number greater than 0.

Define the sequence $\{a_i\}_{i\geq 0}$ recursively as follows: $a_k=[\alpha_k]$, $\alpha_{k+1}=\frac{1}{\alpha_k - a_k}$.

Prove that $\alpha=[a_0,a_1,.....]$ is a representation of α as a simple continued fraction.

Proof.

By induction on k, we easily see that each α_k is irrational.

Therefore, $\alpha_{k+1}>1$ which means that $a_{k+1} \geq 1$ so that $[a_0,a_1,...]$ is a continued fraction.

Also, $\alpha=\alpha_0=[\alpha_0]+(\alpha_0-[\alpha_0])=a_0+\frac{1}{\alpha_1}=[\alpha_0,\alpha_1]=[a_0,a_1,\alpha_2]=.....=[a_0,a_1,...,a_k,\alpha_{k+1}]$

for all k. By Theorem, $\alpha=\frac{a_{k+1}p_k+p_{k-1}}{a_{k+1}q_k+q_{k-1}}$ so that $|\alpha-C_k|=\left|\frac{a_{k+1}p_k+p_{k-1}}{a_{k+1}q_k+q_{k-1}}-\frac{p_k}{q_k}\right|$

$=\left|\frac{-(p_kq_{k-1}-p_{k-1}q_k)}{(\alpha_{k+1}q_k+q_{k-1})q_k}\right|=\left|\frac{1}{(\alpha_{k+1}q_k+q_{k-1})q_k}\right|<\frac{1}{q_k^2}\leq\frac{1}{(2k-3)^2}\to 0,$ as $k\to\infty$.

Thus, $\alpha=\lim_{k\to\infty} C_k=[a_0,a_1,...]$

It is evident that every real number α has an expression as a simple continued fraction. Also, representation of an irrational number as a simple continued fraction is unique.

Definition 4.4.3.

A simple continued fraction is called periodic with period k if there exists positive integers N, k such that $a_n=a_{n+K}$ for all $n \geq N$. We denote such a continued fraction by $[a_0,...a_{N-1},a_N,a_{N+1},...,a_{N+k-1}]$

Theorem 4.4.3.

Let α be a quadratic irrational. Then there are integers P_0,Q_0,d such that

$\alpha=\dfrac{P_0+\sqrt{d}}{Q_0}$, with Q_0 divides $(d-P_0^2)$. Recursively define $\alpha_k=\dfrac{P_0+\sqrt{d}}{Q_0}$,

$a_k=[a_k]$, $P_{k+1}=a_kQ_k-P_k$, $Q_{k+1}=\dfrac{d-P_{k+1}^2}{Q_k}$ for k=0,1,2,... Prove that $[a_0,a_1,a_2,....]$ is the simple continued fraction of α.

Proof.

There exist $a,b,e,f\in\mathbf{Z}$, $e,f>0$, e not a perfect square, such that

$\alpha=\dfrac{a+b\sqrt{e}}{f}=\dfrac{af+b\sqrt{eb^2f^2}}{f^2}$ and evidently, f^2 divides $a^2f^2-eb^2f^2$.

This sequence is well defined, since d is not perfect square $\Rightarrow Q_k\neq 0$, for all k.

It will be enough to show that $\alpha_{k+1}=\dfrac{1}{\alpha_k-a_k}$ for all k. $\alpha_k-a_k=\dfrac{P_k+\sqrt{d}}{Q_k}-a_k$

$$=\frac{\sqrt{d}-(a_kQ_k-P_k)}{Q_k}=\frac{\sqrt{d}-P_{k+1}}{Q_k}=\frac{\sqrt{d}-P_{k+1}^2}{Q_k\left(\sqrt{d}+P_{k+1}\right)}=\frac{Q_kQ_{k+1}}{Q_k\left(\sqrt{d}+P_{k+1}\right)}=\frac{1}{\alpha_{k+1}}$$

Theorem 4.4.4.

Let n be the period of the continued fraction of $\sqrt{d}$.

(a) All integer solutions to the equation $x^2-dy^2=\pm1$ are given by

$$x+y\sqrt{d}=\pm\left(p_{n-1}+q_{n-1}\sqrt{d}\right)^l : l\in\mathbf{Z},$$

where p_{n-1}/q_{n-1} is the $(n-1)$th convergent of the fraction of $\sqrt{d}$.

(b) $d\equiv 2,3(\text{mod}4)$, then $p_{n-1}+q_{n-1}\sqrt{d}$ is the fundamental unit of $Q(\sqrt{d})$.

(c) The equation $x^2-dy^2=-1$ has an integer solutions $\Leftrightarrow$ n is odd.

(d) If d has a prime divisor $p\equiv 3(\text{mod}4)$, then the equation $x^2-dy^2=-1$ has no solution.

Exercise: 4.4.4.

(a) Find the simple continued fractions of $\sqrt{6}$, $\sqrt{23}$

(b) Compute the fundamental unit in both $Q(\sqrt{6})$ and $Q(\sqrt{23})$. [14]

Solution.

(a) Using notation of previous theorems, setting $\alpha=\alpha_0=\sqrt{6}$, we have

$P_0=0,$ $P_1=2,$ $P_2=2,$

$Q_0=0,$ $Q_1=2,$ $Q_2=1,$

$\alpha_0=\sqrt{6},$ $\alpha_1=\frac{2+\sqrt{6}}{2},$ $\alpha_2=2+\sqrt{6},$

$a_0=2,$ $a_1=2,$ $a_2=4.$

Thus, the period of the continued fraction of α is $2Þ\sqrt{6}=[a_0,a_1,a_2]=[2,2,4]$

Applying the same procedure, we find $\sqrt{23}=[4,1,3,1,8]$.

(b) For $\sqrt{6}$, $C_1=p_1/q_1=[a_0,a_1]=a_0+1/a_1=2+1/2=5/2$.

Thus, the fundamental unit in $Q\left(\sqrt{6}\right)$ is $5+2\sqrt{6}$. For $\sqrt{23}$, $C_3=[4,1,3,1]=24/5$.

Therefore, the fundamental unit in $Q\left(\sqrt{23}\right)$ is $24+5\sqrt{23}$.

Theorem 4.4.5.

(a) $[d,2d]$ is the continued fraction of $\sqrt{d^2+1}$.

(b) Conclude that, if d^2+1 is squarefree, $d\equiv 1,3 \pmod 4$ then the fundamental unit of $Q\left(\sqrt{d^2+1}\right)$ is $d+\sqrt{d^2+1}$. Compute the fundamental unit of $Q(\sqrt{2})$, $Q(\sqrt{10})$, $Q(\sqrt{26})$

(c) The continued fraction of $\sqrt{d^2+2}$ is $[d,d,2d]$

(d) Conclude that, if d^2+2 is squarefree, then the fundamental unit of $Q(\sqrt{d^2+2})$ is $d^2+1+d\sqrt{d^2+2}$. Compute the fundamental units in $Q(\sqrt{3})$, $Q(\sqrt{11})$, $Q(\sqrt{51})$, $Q(\sqrt{66})$ **Proof.**

(a) Observing that $d^2<d^2+1<(d+1)^2$ for all $d>0$, we see that $\left[\sqrt{d^2+1}\right]=d$

and setting $\alpha=\alpha_0=\sqrt{d^2+1}$, we have

$P_0=0,$ $P_1=d,$

$Q_0=1,$ $Q_1=1,$

$\alpha_0=\sqrt{d^2+1},$ $\alpha_1=d+\sqrt{d^2+1},$

$a_0=d,$ $a_1=2d,$

This implies that the period of the continued fraction of $\sqrt{d^2+1}$ is 1.

Therefore, $\sqrt{d^2+1}=[a_0,a_1]=[d,2d]$.

(b) $d\equiv 1,3 \pmod 4$ and thus $d^2+1\equiv 2 \pmod 4$.

Thus, if d^2+1 is squarefree, then the fundamental unit of $Q\left(\sqrt{d^2+1}\right)$ is $p_0+q_0\sqrt{d^2+1}=d+\sqrt{d^2+1}$.

(c) Observing that $d^2<d^2+2<(d+1)^2$ for all $d \equiv 1$, we get $\left[\sqrt{d^2+2}\right]=d$

and setting $\alpha=\alpha_0=\sqrt{d^2+2}$, we have

$P_0=0$, $P_1=d$, $P_2=d$,

$Q_0=1$, $Q_1=2$, $Q_2=1$,

$\alpha_0=\sqrt{d^2+2}$, $\alpha_1=\frac{d+\sqrt{d^2+2}}{2}$, $\alpha_2=d+\sqrt{d^2+2}$,

$a_0=d$, $a_1=d$, $a_2=2d$.

Therefore the period of the continued fraction of $\sqrt{d^2+2}$ is 2, so

$\sqrt{d^2+2}=[a_0,a_1,a_2]=[d,d,2d]$ and thus $\frac{p_1}{q_1}=d+\frac{1}{d}=\frac{d^2+1}{d}$

(d) For all d, $d^2+2 \equiv 2,3 \pmod 4$ so, if d is squarefree, the fundamental unit in $Q\left(\sqrt{d^2+2}\right)$ is $p_1+q_1\sqrt{d^2+2}=d^2+1+d\sqrt{d^2+2}$.

4.5. Characters and Dirichlet Characters

Definition 4.5.1.

Let G be a group. A function f defined on G is said to be a character of G if and only if f satisfies the following conditions:

1) $\forall a,b \in G$ $f(a\times b)=f(a)\times f(b)$, (f is comp. multiplication)
2) $\exists c \in G$: $f(c) \neq 0$

Theorem 4.5.1.

Let G be a group and f be a character on G. Then the following holds.

e is the identity of G then f(e)=1. The values f(a) are roots of 1. Moreover, if $a^n=e$, then $(f(a))^n=1$. Since f is a character on G, then

$\exists c \in G: f(c) \neq 0 \Rightarrow f(c)=f(c\cdot e)=f(c)\cdot f(e) \Rightarrow f(e)=1$. Assume that $a^n=e \Rightarrow (f(a))^n=f(e)=1 \Rightarrow$ $(f(a))^n=1$. It means that any value of f(a) is a root of unity.

Lemma 4.5.1.

If G is a finite abelian group of order n, then there exist exactly n distinct character on G.

4.6. Dirichlet Characters on Finite Abelian Groups

Let us consider the Reduced Residue System mod k as the finite abelian group G. It consists of $\phi(k)$ distinct elements $\{a_1, a_2, ..., a_{\phi(k)}\}$ such that every element in this set are relatively prime to each other and any integer which is relatively prime to k is congruent to one and only one of the numbers in this set.

Exercise 4.6.1.

R.R.S mod 10 consists of 4 elements 1,3,7,9 and R.R.S mod 11 consists of 1,2,3,….,10.

Definition 4.6.1.

Let f be a character on R.R.S mod k. Define $\chi = \chi_f$ as follows.

$$\chi_f(a)=\begin{cases} f(a), & \text{if } (a,k)=1 \\ 0, & \text{if } (a,k)>1 \end{cases}$$

Then χ_f is called a Dirichlet Character on R.R.S

Definition 4.4.6.

If G is a finite abelian group and f is the character whose values at any $a \in G$ is 1, then f is called the PRINCIPAL character. The principal Dirichlet Character is defined as follows: $\chi_f(a)=\begin{cases} 1, & \text{if } (a,k)=1 \\ 0, & \text{if } (a,k)>1 \end{cases}$

Exercise 4.6.2.

Let us consider the following Dirichlet character

$$\chi_f(a)=\begin{cases} (-1)^{\frac{n-1}{2}}, & \text{if } (n,k)=1 \Leftrightarrow n \text{ is odd} \\ 0, & \text{if } (n,4)>1 \end{cases}$$

This is a Dirichlet character on R.R.S mod4.

Theorem 4.6.1.

Dirichlet character(modk) satisfies the following two conditions.

1) $\chi(m \cdot n)=\chi(m) \cdot \chi(n)$ 2) $\chi(k+n)=\chi(n)$ for some k.

Here, k is called the period of the character.

Proof.

If $(m,k)=(n,k)=1$, then $(mn,k)=1 \Rightarrow \chi(m \cdot n)=f(m \cdot n)=f(m) \cdot f(n)$

On the other hand, $\chi(m) \cdot \chi(n)=f(m) \cdot f(n)$. Assume that at least one of m or n is not relatively prime to k.

For instance , take n:(n,k)>1. Therefore, $\chi(m\cdot n)=0$ since (n,k)>1 $\Rightarrow$ (mn,k)=1 $\chi(m)\cdot\chi(n)=f(m)\cdot 0 \Rightarrow \chi(m\cdot n)=\chi(m)\cdot\chi(n)$

If χ is defined on R.R.S modk, obviously the following holds. $k+n \equiv n(\text{mod}k)$ and (n,k)=1 $\Rightarrow$ (n+k,k)=1

As a conclusion, $\chi(k+n)=\chi(n)$ for all n in R.R.S mod k.

Exercise 4.6.3.

If $n \equiv 1(\text{mod}4)$, then $n=4k+1 \Rightarrow (-1)^{\frac{n-1}{2}}=(-1)^{\frac{4k+1-1}{2}}=(-1)^{2k}=1$

If $n \equiv 3(\text{mod}4)$, then $n=4k+3 \Rightarrow (-1)^{\frac{n-1}{2}}=(-1)^{\frac{4k+3-1}{2}}=(-1)^{2k+1}=-1$

$$\chi(n)=\left\{\begin{array}{ll} 1, & \text{when } n \equiv 1(\text{mod}4) \\ -1, & \text{when } n \equiv 3(\text{mod}4) \\ 0, & n \text{ is even} \end{array}\right\}$$

The period of this character is 4. $\chi(4+n)=\chi(n)$, for all $n \in \mathbf{Z}$.

For example, $\chi(1783)=\chi(3)=-1(\text{mod}4)$ and $\chi(-283)=\chi(1)=1 \ (\text{mod}4)$.

4.7. Dirichlet Characters of Quadratic Number Fields

Let $K=Q(\sqrt{d})$ be a quadratic number field and d_k is its discriminant. Then, The Dirichlet character associated to it is given by

$$\chi_K(p)=\begin{cases} \left(\frac{d_K}{p}\right), & \text{if p is odd prime and p is not a divisor of } d_K \\ (-1)^{\frac{d^2-1}{8}}, & \text{if } p \equiv 2 \text{ and d is odd number} \\ 0, & \text{otherwise} \end{cases} \qquad [15]$$

In summary, we know that $d_K=\begin{cases} d, & \text{if } d \equiv 1 \pmod 4 \\ 4d, & \text{if } d \equiv 2,3 \pmod 4 \end{cases}$

The Dirichlet character $\text{mod}|d_K|$ associated to $K=Q(\sqrt{d})$ can be evaluated using $\chi_K(p)$ defined above.

Exercise 4.7.1.

Find the Dirichlet character associated to the quadratic field $Q(\sqrt{11})$. We know that $11 \equiv 3(\text{mod}4) \Rightarrow d_K=4\times 11$

We need to find $\left(\frac{d_K}{n}\right)$, in this specific case, $\left(\frac{44}{n}\right)$ for each n.

$\chi_K(n)=0$, when $n=0,2,4,6,8,10,11,12,14,16,18,20,22,24,26,28,30,32,33,34,36,38,40$ The n, we need to calculate $\chi_K(n)$ for

$$1,3,5,7,9,13,15,17,21,23,25,27,29,31,35,37,39,41$$

$\left(\frac{44}{1}\right)=1$, $\left(\frac{44}{3}\right)=\left(\frac{2}{3}\right)=-1$, $\left(\frac{44}{5}\right)=\left(\frac{4}{5}\right)=1$, $\left(\frac{44}{7}\right)=\left(\frac{2}{7}\right)=1$,

$\left(\frac{44}{9}\right)=\left(\frac{8}{9}\right)=1$, $\left(\frac{44}{13}\right)=\left(\frac{5}{13}\right)=-1$, $\left(\frac{44}{15}\right)=\left(\frac{-1}{15}\right)=\left(\frac{-1}{3}\right)\left(\frac{-1}{5}\right)=(-1)(1)=1$

$$\chi_K(n)=\begin{cases} 1, & \text{if } n\equiv 1,5,7,9,\ldots \pmod{44} \\ -1, & \text{if } n\equiv 3,13,15,\ldots \pmod{44} \\ 0, & \text{if } (n,44)\neq 1 \end{cases}$$

4.8. Dirichlet's L-Functions:

Let m be a natural number and χ a Dirichlet character mod m. That is, χ is a homomorphism $\chi:(\mathbf{Z}/m\mathbf{Z})^* \to C^*$. We extend the definition of χ to all natural numbers by setting

$$\chi(a)=\begin{cases} \chi\ (a \bmod m) & \text{if } (a,m)=1 \\ 0 & \text{otherwise} \end{cases}$$

Now, define the Dirichlet L-function: $L(s,\chi)=\sum_{n=1}^{\infty}\frac{\chi(a)}{n^s}$.

Theorem 4.8.1.

$L(s,\chi)$ converges absolutely for $Re(s)>1$.

Proof.

Since $|\chi(n)|\le 1$, we have $\left|\sum_{n=1}^{\infty}\frac{\chi(n)}{n^s}\right|\le\sum_{n=1}^{\infty}\frac{1}{n^\sigma}$, where $\sigma=Re(s)$.

The latter series converges absolutely for $Re(s)>1$.

Theorem 4.8.2.

For $Re(s)>1$, show that $L(s,\chi)=\prod_p\left(1-\frac{\chi(p)}{p^s}\right)^{-1}$.

Proof.

Since χ is completely multiplicative,

$$L(s,\chi)=\prod_p\left(1+\frac{\chi(p)}{p^s}+\frac{\chi(p^2)}{p^{2s}}+\ldots\right)=\prod_p\left(1+\frac{\chi(p)}{p^s}+\frac{\chi(p)^2}{p^s}+\ldots\right)=\prod_p\left(1-\frac{\chi(p)}{p^s}\right)^{-1}$$

Theorem 4.8.3.

$$\sum_{\chi \bmod m}\overline{\chi}(a)\chi(b)=\begin{cases}\varphi(m) & \text{if } a\equiv b\left(\bmod m\right)\\ 0 & \text{otherwise.}\end{cases} \qquad [16]$$

Proof.

If $a\equiv b(\bmod m)$, the result is clear. If a is not congruent to b(modm), let φ be a character such that $\varphi(a)\neq\varphi(b)$.

Then $\sum_{\chi \bmod m}\varphi\left(ba^{-1}\right)\chi\left(ba^{-1}\right) = \sum_{\chi \bmod m}(\varphi\chi)\left(ba^{-1}\right) = \sum_{\chi \bmod m}\chi\left(ba^{-1}\right)$

because as χ ranges over characters mod m, so does $\varphi\chi$.

But $\left(1-\varphi\left(ba^{-1}\right)\right)\sum_{\chi \bmod m}\chi\left(ba^{-1}\right)=0$, so the result follows.

CHAPTER 5

FACTORIZATION and IDEAL THEORY

5.1. Unique factorization in algebraic number fields

We know that if F is such a field, the subset of F consisting of algebraic integers forms a ring I_d, called the ring of algebraic integers in F. An algebraic number field consists of algebraic numbers. Let Φ be the set of all algebraic integers. Then Φ is a ring.

Since $I_d = \phi \cap F$, I_d is also a ring. We will often refer to I_d simply as the ring of integers in F. I_d is not a unique factorization domain. However I_d does have a very important property. Every nonzero ideal can be written uniquely as a product of prime ideals.

Remember that algebraic integers are not necessarily factorized in a unique way. That is, unique factorization theorem does not hold. For instance,

$$58 = 2 \times 29 = (2+3\sqrt{-6})(2-3\sqrt{-6})$$

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

To see that all the factors of 6 given are irreducible, and no two are associates, we need to use the norm map

$$\text{Nm: } Q\left[\sqrt{-5}\right] \to Q, \quad a+b\sqrt{-5} \to a^2+5b^2$$

For $\alpha \in Oa$, we have $Nm(\alpha)=1 \Leftrightarrow \alpha\bar{\alpha}=1 \Leftrightarrow \alpha$ is a unit. If $1+\sqrt{-5}=\alpha\beta$, then

$\mathrm{Nm}(1+\sqrt{-5})=6$. Then, Nm (α) = 1, 2, 3, or 6. In our first case, α is a unit, second and third cases will not occur here as $a^2+5b^2=2$ or 3 does not have a solution in I_{-5}. That means, fourth case, β is a unit. Similarly, 2, 3, and $1-\sqrt{-5}$ are all irreducible. Associates have the same norm.

$\frac{1+\sqrt{-5}}{2} \notin I_5 \Rightarrow$ It can not be a unit. $1+\sqrt{-5}$ and 2 are not associates. Similarly, all the 39 factors on the right hand side are not associates.

5.2. Ideals in O_K and Ideal Theory

Definition 5.2.1.

A left ideal of a ring R is a nonempty subset closed under subtraction and left multiplication by any ring element. Namely,

Let I be an left ideal for the ring R, the following holds:

i. For any $r_1, r_2 \in R$, and $a \in I$, $r_1 - r_2 \in I$

ii. For any $r \in R$, and $a \in I$, $ar \in I$.

Similarly, a right ideal of a ring R is a nonempty subset closed under subtraction and right multiplication by any ring element. Namely,

Let I be an left ideal for the ring R, the following holds:

i. For any $r_1, r_2 \in R$, and $a \in I$, $r_1 - r_2 \in I$

ii. For any $r \in R$, and $a \in I$, $ra \in I$.

An ideal is a subset of the ring R that is both a left ideal and a right ideal.

In a commutative ring R, left ideal, right ideal and the ideal itself are necessarily equal to each other. Although it is not a requirement, it is easy to show that an ideal I is also closed under addition. Let a_1 and $a_2 \in I$, then $a_1 - a_1 = 0 \in I$,

$$0 - a_2 = -a_2 \in I$$

$$a_1 - (-a_2) = a_1 + a_2 \in I$$

Proposition 5.2.1.

Assume that R is a commutative ring. Then, the set of all nilpotent elements of R is an ideal of R.

Definition 5.2.2.

Let R be a commutative ring.

The nil radical of R is the ideal $N(R) = \{ a \in R \mid a^n = 0 \text{ for some } n \in Z^+ \}$.

Definition 5.2.3.

An ideal $I \subseteq K$ is called principal if it can be generated by a single element of K. A domain K is then called a principal domain if every ideal of K is principal.

Theorem 5.2.1.

Let I be a nonzero ideal of. Then $a \cap \mathbf{Z} \neq \{0\}$

Proof.

Let α be a nonzero algebraic integer in ideal I satisfying the minimal polynomial $x^r+a_{r-1}x^{r-1}+...+a_0=0$ with $a_i \in \mathbf{Z}$ $\forall i$ *and* $a_0 \neq 0$. Then $a_0 = -(\alpha^r+...+a_1\alpha)$.

The left hand side of this equation is in **Z**, while the right side is in I.

Theorem 5.2.2.

I has an integral basis.

Solution.

Let I be an ideal of O_K, and let $w_1,w_2,.....,w_n$ be an integral basis for O_K. Note that, for any $w_i \in O_K$, $a_0w_i = -(\alpha^r+...+a_1\alpha)w_i \in I$.

Then, I has a finite index in O_K and $I \subseteq O_K = \mathbf{Z}w_1 + \mathbf{Z}w_2 + ... + \mathbf{Z}w_n$ has maximal rank. Then, since I is a submodule of O_K, there exists an integral basis for I.

Theorem 5.2.3.

If I is a nonzero ideal in O_K, then it has finite index in O_K.

Solution.

If $O_K = \mathbf{Z}w_1 + \mathbf{Z}w_2 + ... + \mathbf{Z}w_n$, then, we can pick a rational integer a such that $aO_K = a\mathbf{Z}w_1 + a\mathbf{Z}w_2 + ... + a\mathbf{Z}w_n \subset I \subset O_K$. But, it is obvious that aO_K has index a^n in O_K. Therefore, the index of I in O_K must be finite.

Theorem 5.2.4.

Every nonzero prime ideal in Q_K contains exactly one prime integer.

Proof.

If P is a prime ideal of Q_K, then it certainly contains an integer. By the definition of the prime ideal, if $ab \in P$, either $a \in P$ or $b \in P$.

So, P must contain some rational prime. Now, if P contained two distinct rational primes p,q, then it would necessarily contain their greatest common denominator which is 1. But this contradicts the assumption of nontriviality. So, every prime ideals of Q_K contains exactly one integer prime.

5.3. Unique Factorization and Ideals

Assume that F is a field, and F[x] is ring of polynomials in one variable. Since this ring is a principal ideal domain, each ideal is a multiplication of prime ideals.

However, although the ring F[x,y] of polynomials in two variables is a unique factorization domain, the ideal structure is not simple.

For example, consider the ideal $<x^2,y>$ generated by the elements x^2 and y.

In F[x,y]/<y> F[x], the only prime ideal that contains $<x^2,y>/<y>$ is $<x,y>/<y>$. Then, in F[x,y] the only prime ideal that contains $<x^2,y>$ is going to be $<x,y>$.

Since $<x,y>^2 = <x^2,xy,y^2>$, which is in $<x^2,y>$, we cannot express $<x^2,y>$ as a multiplication of prime ideals.

To have a generalization of unique factorization of ideals in polynomial rings we need to replace multiplication of ideals with intersections of ideals, and powers of prime ideals with ``primary'' ideals.

Theorem 5.3.1.

Assume that R is a commutative ring.

(a) The nil radical of R / N(R) will be zero.

(b) The nil radical of R is intersection of all prime ideals of R.

The ideal N(R) is also called the prime radical of R. This definition can also be extended to non: commutative rings. In this case we can define the prime radical of R as the intersection of all prime ideals of R.

Definition 5.3.1.

Assume that R is a commutative ring, and I is an ideal of R.

The ideal $\sqrt{I} = \{ a \in R$ such that $a^n \in I$ for some n $Z^+ \}$ is the radical of I.

Whenever I is an ideal of R, then $\sqrt{I}$ is the inverse image in R of the nil radical of R/I. This proves us that $\sqrt{I}$ is an ideal and also $\sqrt{I}$ is the intersection of all prime ideals of R that contain I.

Definition 5.3.2.

Assume that I is an ideal of the commutative ring R. Then, I is a primary ideal if for all elements a,b ∈ R we have the following: ab ∈ I implies a ∈ I or b^n ∈ I, for some n ∈ Z^+. Also,

I is an irreducible ideal if I = JK implies I=J or I=K,
for all ideals J,K of R with I $\subseteq$ J and I $\subseteq$ K.

Assume that D is a principal ideal domain, and p is an irreducible element D with $Q=p^nD$. If a,b ∈ D with ab ∈ Q, then $p^n|ab$. Then, either p|a or p|b.

If a $\notin$ I, then p is not a factor of a implies $p^n|b$, and hence b ∈ Q. This proves that Q is a primary ideal.

If both I and Q are ideals of R where I $\subseteq$ Q, then Q is a primary ideal of R if and only if Q/I is a primary ideal of R/I.

Assume that F is any field with R=F[x,y], $Q=\langle x^2,y\rangle$, and $I=\langle y\rangle$. Then we can show that $\langle x^2, y\rangle$ is a primary ideal of F[x,y]. This example shows a primary ideal that is not a power of a prime ideal.

Lemma 5.3.1.

Assume that R be a commutative ring. Whenever I is a primary ideal of R, then $\sqrt{I}$ is a prime ideal of R. [17]

5.4. Dedekind Domains

We will look at a different approach to unique factorization theorem, using ideals. First recall that an integral domain is said to be a principal ideal domain if every ideal is generated by a single element. Thus if D is a principal ideal domain, then any nonzero ideal I of D has the form I= aD for some $a \in D$, $a \neq 0$. Moreover we can write $a = p_1 p_2 \ldots p_n$ for irreducible elements $p_1, p_2, \ldots, p_n \in D$.

Then, ideal I is a product of prime ideals. This condition is at the same time our

definition of a Dedekind domain.

Definition 5.4.1.

An integral domain D is called a Dedekind domain if each proper ideal of D can be written as the multiplication of a finite number of prime ideals of D.

Dedekind domain shows some of the properties of a principal ideal domain. For instance, any nonzero prime ideal of a Dedekind domain must be maximal. This property tells us that a unique factorization domain can fail to be a Dedekind domain.

ut Dedekind domains by using the ``inverse" of an ideal. Before that, the following concepts need to be introduced.

Definition 5.4.2.

Let D be an integral domain with the quotient field F. Then, a fractional ideal of D is a nonzero D: sub module I of F such that there exists $0 \neq d \in D$ with $dI \subseteq D$.

If I is a fractional ideal of D, we can define $I^{-1} = \{ q \in F \text{ such that } qI \subseteq D\}$. That

means, I is **invertible** if $I^{-1}I = D$.

Lemma 5.4.1.

Let D be an integral domain with the quotient field F, and also let I be an ideal of D that is invertible when it is considered as a fractional ideal. In this case the following hold

a. The ideal I is finitely generated.

b. If I is a multiplication of prime ideals, then this product is unique. [17]

Theorem 5.4.1.

The following are true for any Dedekind domain D.

a. Every nonzero ideal of D is invertible.

b. Every proper ideal of D can be written uniquely as a multiplication of a finite number of prime ideals of D;

c. Every nonzero prime ideal of D is maximal.

Theorem 5.4.2.

For an integral domain D, the following are equivalent

1. D is a Dedekind domain;

2. Every nonzero ideal of D is invertible;

3. Every fractional ideal of D is invertible;

Theorem 5.4.3.

Assume that D is an integral domain with quotient field Q, and F is a finite extension field of Q. Given that D* is the set of all elements of F that are integral over D, then D* itself is a Dedekind domain.

CHAPTER 6

CLASS NUMBER

6.1. History of Class Number Problem

Finding solutions to the class number problems for quadratic number fields have caught the attention of many number theorists for many years. Among all, the most important results are the solutions of Gauss 'conjecture. In 1801, Gauss put forward several conjectures. Some of these conjectures still continue to these days and remain unsolved. His main conjecture was actually on the class number of imaginary quadratic fields. The main result in this direction is that the number of imaginary quadratic fields which have a given class number h is finite. The cases h=1 and h=2 were solved completely and independently. The more general case, where h is an arbitrary positive integer was also solved. In the case of real quadratic fields, many similar questions are still unsolved.

We know that an algebraic field is a finite extension of the rationals. Let K be an algebraic number field.

The ring of the integers of O_K consists of the elements of K which have a monic minimal polynomial. We say that two ideals I and J of O_K are equivalent if there are nonzero principal ideals A and B in O_K such that $AI=BJ$. The class group of K (or O_K) is the set of equivalence classes of ideals. In other words, it is ideals modulo principal ideals.

The class group is an extremely important object in algebraic number theory. From the definition, it is clear that class group is commutative. Having a trivial class group is equivalent to all ideals being principal. In this case, O_K is principal ideal domain and it has unique factorization.

6.2. The Ideal Class Group

45

Definition 6.2.1.

An ideal I of O_K is an additive subgroup of O_K having the following property: $(\alpha) = \{p\alpha \text{ such that } p \in O_m \text{ and } a \in I\}$

This ideal is the set of all multiples of a single element $\alpha \in O_K$ and is called a principal ideal. On the other hand, the ideal given below is non principal ideal.

$(\alpha_1,\alpha_2) = \{p_1\alpha_1 + p_2\alpha_2 \text{ , where } p_1 \text{ and } p_2 \text{ is in } O_M\}$

If (α_1,α_2) is not equal to (α_3) for any α_3 in O_m. Moreover, the product IJ of two ideals is the ideal of all finite sums of products of the form αβ where $\alpha \in I$ and $\beta \in J$.

In O_{-5}, the principal ideal (6) can be written as follows:

$(6) = (2)(3) = I_1^2 I_2 I_3 = (1+\sqrt{5})(1-\sqrt{-5}) = I_1 I_2 I_3$

Given that $I_1=(2,\ 1+\sqrt{-5})=(2,\ 1-\sqrt{-5})$, $I_2=(3,\ 1+\sqrt{-5})$, $I_3=(3,\ 1-\sqrt{-5})$.

That means, two different factorizations of the number 6 in O_{-5} is obtained by permuting I_1,I_2, and I_3 in the factorization of the ideal (6).

The two different factorizations come from different permutations of the ideals I_1,I_2 and I_3.

Let us assume that we are given $\alpha=a+b\sqrt{d} \in Q(\sqrt{d})$. Then, we can define its conjugate as $\bar{\alpha}=a-b\sqrt{d} \in Q(\sqrt{d})$, and its norm will be $N(\alpha)=\alpha\bar{\alpha}=a^2-db_2$.

Now, let us define, $\bar{I}=\{\bar{\alpha}:\ \alpha \in I\}$ and $N(I)=\gcd\{N(\alpha):\ \alpha \in I\}$

For instance, if we are given that I is the principal ideal, then

$\bar{I}=(\bar{\alpha})$, and also $N(I)=[N(\alpha)]$.

Given that I and J are two ideals, we have $N(I\cdot J)=N(I)\cdot N(J)$ Also; note that $I\cdot\bar{I}=(N(I))$ is a principal ideal. The ideal $(\alpha_1,\alpha_2)=\{m_1\alpha_1+m_2\alpha_2 \in O_M\}$ is not principal ideal if $(\alpha_1,\alpha_2) \neq (\alpha_3)$, for any given α_3 in O_K.

Definition 6.2.2.

Two ideals I and J are strictly equivalent if

$\exists\,\alpha,\beta \in Q(\sqrt{d})$ such that $(\alpha)I=(\beta)J$, with $N(\alpha\beta)>0$.

In this case, the two ideals I, J are in the same narrow ideal class.

Note that if the ring of algebraic integers O_K is a principal ideal domain then any two ideals are equivalent.

We will define H_d^+ as the finite abelian group of ideals module the relation given above. However, if we do not require $N(\alpha\beta)>0$, then we say that the two ideals I and J are in the same wide ideal class and define H_d.

In this case, H_d^+ is said to be the narrow class group and also its cardinality h_d^+ is the narrow class number.

H_d, most of the times, shows class group. The class number h_d can be obtained in terms of h_d^+ as follows:

$$h_d = \begin{cases} h_d^t & \text{if } d<0, \text{ and } N(\varepsilon)=-1 \\ \left(\frac{1}{2}\right)h_d^t, & \text{if } d>0 \text{ and } N(\varepsilon)=1 \end{cases} \qquad [18]$$

Here, ε is the fundamental unit of $(Q(\sqrt{d})$. The concept of the ideal class group has been originated from Dedekind's work in establishing the unique factorization theory for ideals in the ring of algebraic integers of a number field.

The ring Q_K is Euclidean if given $\alpha \in K$, $\exists \beta \in Q_K$ such that $|N(\alpha - \beta| < 1$.
In general, Q_K is not Euclidean, but the following result always hold:

Lemma 6.2.1.

There is a constant H_K such that given $\alpha \in K$, $\exists \beta \in O_K$, and a non-zero integer t, with $|t| \le H_K$, such that $|N(t\alpha-\beta|<1$. We will call H_K as the Hurwitz constant. In this section, we will prove that the ideal class group is finite. We need to start by introducing an equivalence relation on ideals.

Any fractional ideal A can be written uniquely in the form

$A=\frac{\rho_{1...}\rho_s}{\rho'_{1...}\rho'_r}$, where ρ_i, ρ'_i are primes in the ring of algebraic field Q_K in K, and no ρ_i is a ρ'_j.

In particular, we can always write an fractional ideal A in the form $A = \frac{b}{c} = bc^{-1}$ where b, c are two integral ideals. Note that we can write $\rho^{-1}=\frac{1}{\rho}$

Two fractional ideals A and B in K are said to be equivalent if there exists $\alpha,\beta \in Q_K$ such that $(\alpha)A=(\beta)B$. In this case we write A:B. Notice that if Q_K is a principal ideal **Ex** domain then any two ideals are equivalent.

ercise 6.2.1.

The relation ⊔ defined above is an equivalence relation.

Solution.

i. It is trivial that $A \sim A$, and

ii. if $A \sim B$ then $B \sim A$, for any ideals A and B.

iii. Suppose now that $A \sim B$ and $B \sim C$. That is, there exist $\alpha,\beta,\gamma,\theta \in Q_K$ such that $(\alpha)A=(\beta)B$, and $(\gamma)B=(\theta)C$.

We can easily see that $(\alpha\gamma)A=(\beta\theta)C$. Therefore, $A \sim B$ and $B \sim C$ imply $A \sim C$.

Hence, $\sim$ is an equivalence relation.

Theorem 6.2.1.

There exists a constant C_K such that every ideal $a \subseteq Q_K$, is equivalent to an ideal $b \subseteq Q_K$ with $N(b) \leq C_K$.

Proof.

Suppose a is an ideal of Q_K. Let $\beta \in a$ be non-zero element such that $|N(\beta)|$ is minimal. For each $\alpha \in a$, by exercise(equivalence relation), we can find $t \in \mathbf{Z}$, $|t| \leq H_K$, and $w \in Q_K$ such that $|N(t\alpha-w\beta| < |N(\beta)|$. Moreover, since $\alpha,\beta \in$ ideal a, so $t\alpha-w\beta \in$ ideal a. Therefore, by the minimality of $|N(\beta)|$, we must have $t\alpha=w\beta$. Thus, we have shown that $\forall \alpha \in$ ideal $a, \exists t \in \mathbf{Z}$, $|t| \leq H_K$, and $w \in Q_K$ such that $t\alpha=w\beta$.

Let $M = \prod_{|t| \leq H_K} t$, and we have $Ma \subseteq (\beta)$. This means that (β) divides $(M)a$, and so $(M)a=(\beta)b$, for some ideal $b \subseteq Q_K$. Observe that $\beta \in$ ideal a, so $(M)\beta \in (\beta)b$, and hence $(M) \subseteq$ ideal b. This implies $|N(b)| \leq N((M))=C_K$. Hence, $a \sim b$, and $C_K=N((M))$ satisfies requirement.

Theorem 6.2.2.

Each equivalence class of ideals has an integral ideal representative.

Proof.

Suppose A is a fractional ideal in K. Let $A=b/c$ with $b,c \subseteq Q_K$. We know that $c \cap \mathbf{Z} \neq \{0\}$, so there exists $0 \neq t \in \mathbf{Z}$ such that $t \in c$. (c is ideal)

Therefore, $(t)=tO_K \subseteq c$, and so c divides (t). This implies that there exists an integral ideal $e \subseteq Q_K$ such that $ce=(t)$. We now have $(t)=(t)\frac{b}{c} = \frac{ceb}{c}=eb \subseteq O_K$. Thus, $be \subseteq O_K$, and the result is proved.

Theorem

6.2.3.

For any integer x>0, the number of integral ideals $a \subseteq O_K$ for which $N(a) \le x$ is finite. **Proof.**

Since the norm is multiplicative and takes values bigger than 1 on prime ideals, and since integral ideals have unique factorization, it is sufficient to prove that there are only a finite number of prime ideals $\mathfrak{J}$ with $N(J) \le x$.

Now, any prime $\mathfrak{J}$ contains exactly one prime $p \in \mathbf{Z}$. Thus, $\mathfrak{J}$ occurs in the factorization of $(p) \subseteq Q_K$ into prime ideals. Since $N(\mathfrak{J}) \ge 2$, we have $N(\mathfrak{J}) = p^t$, for some $t \ge 1$. This implies there are at most n possibilities for such $\mathfrak{J}$, since the factorization

$(p) = \prod_{i=1}^{s} \mathfrak{J}_i^{a_i}$ implies that $p^n = N((p)) = \prod_{i=1}^{s} N(\mathfrak{J}_i)^{a_i}$ leading to $s \le n$.

Moreover, $p \le N(\mathfrak{J}) \le x$. This proves the theorem.

Theorem 6.2.4.

The number of equivalence classes of ideals is finite.

Proof.

By Theorem 6.2.2, each equivalence class of ideals can be represented by an integral ideal. This integral ideal, by Theorem 6.2.1 is equivalent to another integral ideal with norm less than 1, or equal to a given constant C_K. Apply Theorem 6.2.3 and we are done.

As we did in the proof of Theorem 6.2.2, it is sufficient to consider only integral representatives when dealing with the equivalence classes of ideals. Let H be the set of all equivalence classes of ideals K. Given C_1 and C_2 in H, we define the product of C_1 and C_2 to be the equivalence class of AB, where A and B are two representatives of C_1 and C_2 respectively.

Exercise

6.2.4.

The product defined above is well defined, and that H together with this product forms a group, of which the equivalence class containing the principal ideals is the identity element. **Solution.**

To prove the product defined above is well defined, we only need to show $A_1 \sim B_1$

and $A_2 \sim B_2$, then $A_1A_2 \sim B_1B_2$. Indeed, by definition, there exist $\alpha_1, \alpha_2, \beta_1, \beta_2 \in Q_K$ such that $(\alpha_1)A_1 = (\beta_1)B_1$ and $(\alpha_2)A_2 = (\beta_2)B_2$. Therefore, $(\alpha_1\alpha_2)A_1A_2 = (\beta_1\beta_2)B_1B_2$ Thus, $A_1A_2 \sim B_1B_2$. Now, it is easy to check that H with the product above is closed, associative, commutative, and has the class of principals as the identity element. To finish the exercise, we need to show that each element in H has an inverse. Suppose C is an arbitrary element of H.

Let $a \subseteq Q_K$ be a representative of C. Here, we can conclude that there exists an integral ideal b such that ab is principal.It then follows immediately that the class containing b is the inverse of C.

6.3. Exponents of Ideal Class Groups

The concept of the ideal class group arose from Dedekind's work in establishing the unique factorization theory for ideals in the ring of algebraic integers of a number field. Ideal class group is finite. From there, we go to the definition of class number.

Definition 6.3.1.

Given an algebraic number field K, we denote by $h(K)$ the cardinality of the group equivalence classes' ideals $(h(d)) = |H|$, and call it the **class number** of the field K.

The group of equivalence classes of ideals is called the ideal class group. The constant C_K could be taken to be the greatest integer less than or equal to H_K, the Hurwitz constant. The improvement on the bound enables us to determine the class number of many algebraic fields. We demonstrate this by looking at the following example:

Exercise 6.3.1.

The class number of $K=Q(\sqrt{-5})$ is 2.

Solution.

We proved that the integers in K are $Z\left[\sqrt{-5}\right]$

so that $w_1^{(1)}=1, \quad w_2^{(1)}=\sqrt{-5}$

$w_1^{(2)}=1, \quad w_2^{(2)}=\sqrt{-5}$

and the Hurwitz constant is $\left(1+\sqrt{5}\right)^2 = 10.45...$ Thus, $C_K = 10$.

This implies that every equivalence class of ideals $C \in H$ has an integral representative a such that $N(a) \le 10$. a has a factorization into product of primes,say $a=\rho_1\rho_2...\rho_m$,

where ρ_i is prime in Q_K for all i=1,...,m. Consider ρ_1. There exists a unique prime number $p \in \mathbf{Z}$ such that $p \in \rho_1$.

This implies that ρ_1 is in the factorization of (p) into product of primes in O_K.

Thus, $N(\rho_1)$ is a power of p.

For p=2,3,5 and 7, (p) factors in $\mathbf{Z}\left(\sqrt{-5}\right)$ as follows:

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

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

$(7) = (7, 3+\sqrt{-5})(7, 3-\sqrt{-5})$, and

$(5) = \left(\sqrt{-5}\right)^2$.

Thus, ρ_1 can only be $(2, 1+\sqrt{-5})$, $(2, 1+\sqrt{-5})$, $(3, 1+\sqrt{-5})$, $(3, 1+\sqrt{-5})$, $(7, 3+\sqrt{-5})$, $(7, 3+\sqrt{-5})$, or $\left(\sqrt{-5}\right)$.

The same conclusion holds for any ρ_i for i=2,...,m. Moreover, it can be seen that $\left(\sqrt{-5}\right)$ principal, and the others are not principal (by taking the norms), but are pairwise equivalent by the following relations:

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

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

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

$$(7, 3+\sqrt{-5})(3-\sqrt{-5}) = (7)(2, 1-\sqrt{-5})$$

$$(7, 3-\sqrt{-5})(3+\sqrt{-5}) = (7)(2, 1+\sqrt{-5})$$

Therefore, a is equivalent to either the class of principal ideals or the class of those primes listed above. Hence, the class number of $K=Q(\sqrt{-5})$ is 2.

Bythe “class number n problem for real and complex quadratic fields”, we mean the problem of presenting a complete list of all quadratic fields with class number n.

For real quadratic fields, Gauss states that there are infinitely many real quadratic fields with class number one.

The class number $h(d)$ of an order of a quadratic field with negative discriminant is equal to the number of reduced binary quadratic forms.

6.4. Concept of Class Number

Let p be a prime number different from 2. The probability that p divides the order of the class group of an imaginary quadratic field is $1-\prod_{i=1}^{\infty}\left(1-\frac{1}{p^i}\right)$. This conjecture suggests that it will be better if we investigate the exponents of class groups of imaginary quadratic fields. A similar analysis for the real quadratic fields will also be studied later in the thesis.

Theorem 6.4.1.

Suppose that n is odd, n>1 and $n^g-1=d$ is squarefree, where g is a fixed positive integer. Then the ideal class group of $Q\left(\sqrt{-d}\right)$ has an element of order g.

Proof.

Since d is even and squarefree, $d \equiv 2 \pmod 4$.

The ring of integers of $Q\left(\sqrt{-d}\right)$ is $\mathbf{Z}[-d]$. We have the ideal factorization:

$(n)^g=\left(n^g\right)=(1+d)=\left(1+\sqrt{-d}\right)\left(1-\sqrt{-d}\right)$

The ideals $\left(1+\sqrt{-d}\right)$ and $\left(1-\sqrt{-d}\right)$ are coprime since n is odd. Thus, by Theorem 5.3.13, (Chinese Remainder Theorem) each of the ideals $\left(1+\sqrt{-d}\right)$, $\left(1-\sqrt{-d}\right)$ must be gth powers. Thus, $a^g=\left(1+\sqrt{-d}\right)$ and $\left(a'\right)^g=\left(1-\sqrt{-d}\right)$ with $\left(aa'\right)=(n)$. Hence a has order dividing g in the class group. Suppose $a^m=\left(u+v\sqrt{-d}\right)$ for some $u,v \in \mathbf{Z}$. Note that v cannot be zero for otherwise $a^m=(u)$ implies that $\left(a'\right)^m=(u)$ so that $(u)=\mathrm{GCD}\left(a^m,\left(a'\right)^m\right)$, contrary to $\gcd\left(a,a'\right)=1$. Therefore, $v \neq 0$.

Now take norms of the equation $a^m=\left(u+v\sqrt{-d}\right)$ to obtain $n^m=u^2+v^2d \geq d=n^g-1$. If $m \leq g-1$, we get $n^{g-1} \geq n^g-1$ which implies that $1 \geq n^{g-1}(n-1) \geq 2$, a contradiction. Therefore, $a^g=\left(1+\sqrt{-d}\right)$ and a^m is not principal for any $m<g$. Thus there is an element of order g in the ideal class group of $Q\left(\sqrt{-d}\right)$

Exercise 6.4.2.

Let g be odd greater than 1. If $d=3^g-x^2$ is a squarefree with x odd and satisfying $x^2<3^g/2$, show that $Q\left(\sqrt{-d}\right)$ has an element of order g in the class group.

Solution.

See that $d \equiv 2 (\text{mod} 4)$ so the ring of integers of $Q\left(\sqrt{-d}\right)$ is $Z\left[\sqrt{-d}\right]$. The factorization $3^g = \left(x+\sqrt{-d}\right)\left(x-\sqrt{-d}\right)$ shows that 3 splits in $Q\left(\sqrt{-d}\right)$, as the ideals $\left(x+\sqrt{-d}\right)$ and $\left(x-\sqrt{-d}\right)$ are coprime. Thus, $(3)=\rho_1\rho_1'$. We must have $\left(x+\sqrt{-d}\right)=\rho_1^g$. Therefore, the order of ρ_1 in the ideal class group is a divisor of g. If $\rho_1^m = \left(u+v\sqrt{-d}\right)$, then $3^m = u^2+v^2 d$. If $v \neq 0$, we deduce that $3^m \geq d > 3^g/2$ which is a contradiction if $m \leq g-1$. Either ρ_1 has order g or v=0. In the second case, we get $u^2=3^m$, a contradiction since m is odd.

Exercise 6.4.3.

The class number of $K=Q\left(\sqrt{-19}\right)$ is 1.

Solution.

We know that 1, $\left(1+\sqrt{-19}\right)/2$ forms an integral basis. We then write

$$w_1^{(1)}=1, \qquad w_2^{(1)}=\frac{1+\sqrt{-19}}{2}$$

$$w_1^{(2)}=1 \qquad w_2^{(2)}=\frac{1-\sqrt{-19}}{2}$$

and use this to find the Hurwitz constant $H_K=\prod_{j=1}^{2}\left(\sum_{i=1}^{2}\left|w_i^{(j)}\right|\right)$

$$=\left(1+\left|\frac{1+\sqrt{-19}}{2}\right|\right)\left(1+\left|\frac{1-\sqrt{-19}}{2}\right|\right)=13.53.... .$$

Therefore, we need to examine all the primes $p \leq 13$ to determine the prime ideals with $N(\rho) \leq 13$. This primes in question are 2,3,5,7,11 and 13

They factor in $Z\left[\left(1+\sqrt{-19}\right)/2\right]$ as follows: 2,3 and 13 stay prime, and

$$5=\left(\frac{1+\sqrt{-19}}{2}\right)\left(\frac{1-\sqrt{-19}}{2}\right),\ 7=\left(\frac{3+\sqrt{-19}}{2}\right)\left(\frac{3-\sqrt{-19}}{2}\right),\ 11=\left(\frac{5+\sqrt{-19}}{2}\right)\left(\frac{5-\sqrt{-19}}{2}\right)$$

These are all principal ideals and thus are all equivalent. This shows that the class number of $K=Q\left(\sqrt{-19}\right)$ is 1.

6.5. Minkowski's Bound for Finding Class Number

Let K be an algebraic number field of degree n over Q. Therefore, each ideal class containing an ideal a satisfying $Na \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2}\left|d_K\right|^{1/2}$ where r_2 is the number of pairs of complex embeddings of K, and d_K is the discriminant.

In the case of quadratic field, n=2.

Therefore, the formula becomes $Na \le \frac{2!}{2^2}\left(\frac{4}{\pi}\right)^{r_2}\left|d_K\right|^{1/2} = \frac{1}{2}\left(\frac{4}{\pi}\right)^{r_2}\left|d_K\right|^{1/2}$

Exercise 6.5.1.

Using Minkowski's bound,

i. Show that $Q\left(\sqrt{5}\right)$ has a class number 1.

ii. Show that $Q\left(\sqrt{-5}\right)$ has a class number 2.

Solution.

i. The dicriminant of $Q\left(\sqrt{5}\right)$ is 5 and the Minkowski bound is $\frac{2!}{2^2}\sqrt{5} = \frac{\sqrt{5}}{2} = 1.11\ldots$.

The only ideal of norm less than $\sqrt{5}/2$ is the trivial ideal which is principal. There class number is equal to 1.

ii. Discriminant of $Q\left(\sqrt{-5}\right)$ is -20 and Minkowski bound is $\frac{2}{\pi}\sqrt{20} = \frac{4}{\pi}(2.236\ldots) =$ 2.84.... .

We need to look at the ideals of norm 2. There is only one ideal of norm 2 know that $\mathbf{Z}\left[\sqrt{-5}\right]$ is not principal ideal domain. Hence the class number must be 2.

Exercise 6.5.2.

Compute class numbers of the fields $Q\left(\sqrt{2}\right), Q\left(\sqrt{3}\right)$ and $Q\left(\sqrt{13}\right)$.

Solution.

The discriminants of these fields are 8,12, and 13 respectively.

The Minkowski bound is $\frac{1}{2}\sqrt{d_K} < \frac{1}{2}\sqrt{13} = 1.802\ldots$ The only ideal of the norm less than 1.8 is the trivial ideal, which is principal. So, the class number is 1.

ps: The ring of integers of $Q\left(\sqrt{2}\right)$ and $Q\left(\sqrt{3}\right)$ are Euclidean and hence PIDs.

So that the class number is 1 was already known to us.

Exercise 6.5.3.

Compute the class number of

i. $Q\left(\sqrt{6}\right)$ ii. $Q\left(\sqrt{17}\right)$

Solution.

i. For $Q\left(\sqrt{6}\right)$, d=24 and Minkowski's bound is $\frac{1}{2}\sqrt{24} = \sqrt{6} = 2.44\ldots$, 2 ramifies

in $Q(\sqrt{6})$. Moreover, $-2=(2-\sqrt{6})(2+\sqrt{6})$ so that the ideal $(2-\sqrt{6})$ is the only one of the norm 2 since $\frac{(2+\sqrt{6})}{(2-\sqrt{6})}$ is a unit. Thus, the class number is 1.

ii. For $Q(\sqrt{17})$, the discriminant is 17 and the Minkowski's bound is $\frac{1}{2}\sqrt{17}=2.06...$.

We need to consider ideals of norm 2. Since $-2=\frac{9-17}{4}=\frac{3-\sqrt{17}}{2}\cdot\frac{3+\sqrt{17}}{2}$, 2 splits and the principal ideals $\left((3+\sqrt{17})/2\right)$ and $\left((3-\sqrt{17})/2\right)$ are the only ones of norm 2. Therefore, the class number is 1.

Exercise 6.5.4.

$Q(\sqrt{-15})$ has class number 2.

Solution.

The field has discriminant -15 and Minkowski's bound is $\frac{2}{\pi}\sqrt{15}=2.26...$. Since $-15 \equiv 1 \pmod 8$, by Theorem 7.4.5, 2 splits as a product of two ideals ρ,ρ' each of norm 2. If ρ were principal, then $\rho=\left(\frac{u+v\sqrt{-15}}{2}\right)$ for integers u,v. However, $8=u^2+15v^2$ has no solution. Thus, p is not principal and class number is 2.

Exercise 6.5.6.

The fields $Q(\sqrt{-1}), Q(\sqrt{-2}), Q(\sqrt{-3}), Q(\sqrt{-7})$ have class number 1.

Solution.

The Minkowski bound for an imaginary quadratic field K is $\frac{2}{\pi}\sqrt{|d_K|}$. The given fields have discriminants equal to -4,-8,-3,-7, respectively. Since $\frac{2}{\pi}\sqrt{8}=\frac{4\sqrt{2}}{\pi}=1.80...$, we deduce that every ideal is principal.

6.6. Dirichlet's Class Number Formula

Dirichlet developed his class number formula when he was trying to finish his theorems on prime progression. Although he did not about Kronecker symbol then, Dirichlet found out that every primitive real character corresponds to a quadratic field.

Suppose that K is a quadratic field with discriminant d_k.

$$\sum_{n=1}^{\infty}\left(\frac{d_k}{n}\right)\frac{1}{n}=\begin{cases}\dfrac{2\pi h}{w\sqrt{|d_k|}}, & \text{if } d_k<0,\\ \dfrac{2h\log\varepsilon}{\sqrt{|d_k|}}, & \text{if } d_k\end{cases}$$

where h denotes the class number of K.

6.7. Class Number Problem using Modules

Definition 6.7.1.

Let M_1 and M_2 be modules. We say that M_1 and M_2 belong to the same class if there exists a non zero α in $Q(\sqrt{d})$ such that $M_1 = \alpha M_2$. It is obvious that this is an equivalence relation.

Let M be a submodule of I_d. The class of M is called the similarity class determined by M. The number of distinct similarity classes is called the class number of $Q\left(\sqrt{d}\right)$. This will be denoted by h_d.

By using Mathematica function NumberFieldClassNumber$\left[\text{sqrt}\left[d\right]\right]$, we can find the $h(d)$:class number where d is the discriminant.

The class number $h(d)$ of an order of a quadratic field where discriminant d<0 equals the number of reduced binary quadratic forms of discriminant d.

Let us give an example. The class number $h(-23)$ of the ring of integers $\mathbf{Z}\left(\frac{1+\sqrt{-23}}{2}\right)$ of the number field is 3. Because there are three reduced binary quadratic forms of discriminant.

-23 are: $(1, 1, 6)$, $(2, 1, 3)$ and $(2, -1, 3)$. In order to compute the class number $h(d)$ of the order of the quadratic number field $Q\sqrt{d}$ where discriminant is d<0, we need to count the number of reduced binary quadratic forms with discriminant d.

Lemma 6.7.1.

Let D be a square:free of integer the form $D = 4n^2 + 1$ or $n^2 + 4$, where n is a positive integer. Then we have the following:

If the class number of real quadratic field $Q(\sqrt{D})$ is equal to one, then D is a prime which is odd and n is prime number or equal to 1.

Lemma 6.7.2.

Let p and q be two different prime numbers where p is of the form $p = 4q^2 + 1$, or $p = q^2 + 4$. Then any of the following are equivalent to each other.

i. The class number of $Q(\sqrt{p})$ is equal to 1.

ii. $\sqrt{\frac{p}{q_1}} = -1$, for any prime number $q_1 < q$.

iii. $-x^2+x+\frac{1}{4}(p-1)$ is prime number for any integer number x satisfying

$1 < x < q$

6.8. Class Number of Quadratic Fields

In this section we will study how to calculate the class number h(d) for any quadratic field, real or imaginary.

To find the class number h(d) of a quadratic number field, we will use the formula

$$\lim_{s\to 1}(s-1)\zeta_K(s) = \frac{2^{r+s}\pi^s \mathrm{reg}(K)}{w_K\sqrt{[\Delta_K]}}\cdot h(d), \qquad \text{where}$$

w_K: Number of roots of unity in quadratic field K.

Δ_K: Discriminant of the field.

reg(K): Regulator of quadratic field K

$\zeta_K(s)$: Zeta function on quadratic field K

r,s : Number of real and complex embeddings

When $d < 0$, $r=0$, $s=1$ and by using the Dirichlet Unit Theorem, the rank of the free abelian group part of U_K, the group of units is $r+s-1$, and the regulator is 1. When $d > 0$, with $r=2$ and $s=0$, and $w_K=2$, the roots are 1 and -1.

The discriminant is d for $4 \bmod 1 \equiv d$ and $4d$ for $4 \bmod 3,2 \equiv d$. It is never 0, because then it would not be squarefree.

Assume $D=\Delta_K$. If u generates the free part of U_K, and $u > 1$, the regulator is ln u.

$$h_K = \frac{\sqrt{D}}{2\ln u}\lim_{s\to 1}(s-1)\zeta_K(s) \quad \text{for } d > 0, \text{ and } h_K = \frac{w_K\sqrt{D}}{2\pi}\lim_{s\to 1}(s-1)\zeta_K(s) \quad \text{for } d < 0.$$

Zeta function on K is $\zeta_K(s) = \sum_U \frac{1}{N(U)^s}$. We know that norm is multiplicative. We will apply the factorization in Dirichlet series and also we will express the infinite

sum over all ideals: $\zeta_K(s)=\prod_p \frac{1}{\left(1-\frac{1}{N(p)^s}\right)}$

We can rewrite $\left(\frac{1}{(1-p^{-s})}\right)\cdot\left(\frac{1}{(1-p^{-s})}\right)$ as $\left(\frac{1}{(1-p^{-s})}\right)\cdot\left(\frac{1}{(1-\chi(p)p^{-s})}\right)$

$\chi(p)$ is periodic with period D, and is abelian. We know that $\chi(m)\chi(n)=\chi(mn)$

for all $m,n \in Z$, and $\chi(-1)=\begin{cases} 1, & \text{if } d>0 \\ -1, & \text{if } d<0 \end{cases}$

We call $\chi(p)$ the quadratic character on K.

where, $c_m(n)=\begin{cases} 1, & \text{if n is congruent to m mod D} \\ 0, & \text{otherwise} \end{cases}$

The norm of each prime ideal p is either p or the square of a prime in a quadratic field. In a summary,for the product given above for $\zeta_K(s)$, for a given prime p,

$$\begin{cases} \frac{1}{(1-p^{-2s})}, & \text{if p remains prime} \\ \left(\frac{1}{(1-p^{-2s})}\right)^2, & \text{if p splits} \\ \left(\frac{1}{(1-p^{-s})}\right), & \text{if p ramifies.} \end{cases}$$

We factor out as $\left(\frac{1}{(1-p^{-2s})}\right)=\left(\frac{1}{(1-p^{-s})}\right)\cdot\left(\frac{1}{(1-p^{-s})}\right)\cdot(1)$.

We can define $\chi(p)$ such that $\chi(p)=\begin{cases} -1, & \text{when p remains prime} \\ 1, & \text{when p splits} \\ 0 & \end{cases}$

We can write $c_m(n)=\frac{1}{D}\sum_{j=0}^{D-1}\gamma^{(m-n)j}$, and γ is the primitive D^{th} root of unity.

$$L(s,\chi)=\frac{1}{D}\sum_{j=0}^{D-1}\left(\sum_{m=0}^{D-1}\chi(m)\gamma^{mj}\right)\sum_{n=1}^{\infty}\frac{\gamma^{-nj}}{n^s}$$

Now, we will look at the complex logarithm $\log(1-z)=-\left(z+\frac{z^2}{2}+...+\frac{z^n}{n}+...\right)$

This is the Taylor series around z=0. Therefore, $L(s,\chi)=\frac{1}{D}\sum_{j=0}^{D-1}\left(\sum_{m=0}^{D-1}\chi(m)\gamma^{mj}\right)\sum_{n=1}^{\infty}\frac{\gamma^{-nj}}{n^s}$

$=-\frac{1}{D}g(\chi,\gamma)\sum_{j=0}^{D-1}\chi(j)\log\left(1-\gamma^{-j}\right)$. We will call the sum S and $g(\chi,\gamma^j)$ is the inner product and $g(\chi,\gamma^j)=\chi(j)g(\chi,\gamma)$. Here, we will not prove that $|g(\chi,\gamma)|=\sqrt{D}$.

Substitute $\gamma=e^{\frac{2\pi i}{D}}$, for $0<j<D$. Therefore, we have

$1-\gamma^{-j}=\gamma^{-\frac{j}{2}}\left(\gamma^{\frac{j}{2}}-\gamma^{-\frac{j}{2}}\right)=2i\gamma^{-\frac{j}{2}}\sin\left(\frac{\pi j}{D}\right)=2\sin\left(\frac{\pi j}{D}\right)e^{\left(\frac{\pi}{2}-\pi\frac{j}{D}\right)i}$. *So*, $\log\left(1-\gamma^{-j}\right)=\ln\left(1-\gamma^{-j}\right)+\left(\frac{\pi}{2}-\frac{\pi j}{D}\right)i$.

i. Now, consider the case for d>0 , for which $\chi(-1)=1$. We can replace j by -j in the sum S above. Every j is periodic with D, so

$$S=\sum_{j=0}^{D-1}\chi(j)\log\left(1-\gamma^{-j}\right)=\sum_{j=0}^{D-1}\chi(j)\log\left(1-\gamma^{j}\right)$$

$$=\chi(-1)\sum_{j=0}^{D-1}\chi(j)\log\left(1-\gamma^{-j}\right)=\sum_{j=0}^{D-1}\chi(j)\log\left(1-\gamma^{j}\right).$$

$2S=\sum_{j=0}^{D-1}\chi(j)\log\left(1-\gamma^{j}\right)+\log\left(1-\gamma^{-j}\right)$. These two are the complex conjugates of each other and therefore $S=\sum_{j=0}^{D-1}\chi(j)\ln\left(2\sin\frac{\pi j}{D}\right)$, where $\gamma=e^{\frac{2\pi i}{D}}$.

By pairing together j and -j terms that are equal, we can the number of terms in half and get

$$L(1,\chi)=-\frac{2}{Dg(\chi,\gamma)}\sum_{j=0}^{\frac{D}{2}}\chi(j)\ln\left(\sin\frac{\pi j}{D}\right).$$

Here, we are only dealing with positive numbers, therefore g is not important, and the sum only evaluates the values of j relatively prime to D. Solving for the class number h_K, for d>0, we find

$h_K=\frac{1}{\ln u}\sum_{j=0}^{\frac{D}{2}}\chi(j)\ln\left(\sin\frac{\pi j}{D}\right)$, the sum goes over j rel. prime to D.

ii. With similar computations, it can be shown that

$L(1,\chi)=\frac{\pi i g(\chi,\gamma)}{D^2}\sum_{j=1}^{D-1}\chi(j)j$ and class number $h_K=\frac{w_K}{D}\left|\sum_{j=1}^{D-1}\chi(j)j\right|$,

where all j's are relatively prime with D.

The most difficult part of the formula is to find the fundamental unit for d>0. Now, let us give some examples and compute class number for some cases.

Example 6.8.1.

Let us say, d=2. Find the class number.

Solution.

D=8, and the numbers relatively prime to 8 are 1,3,5, and 7. Character number for 1 and 7 is 1 since $7 \equiv 1 (\mathrm{mod} 8)$. Remember that the sum of the character numbers is 0. Therefore, the character number for 3 and 5 must be -1. We must evaluate $\ln\sin\left(\frac{\pi}{8}\right) - \ln\left(\frac{3\pi}{8}\right)$, since we only need the first half of the formula. Because $\left(\frac{\pi}{8}\right)$ and $\left(\frac{3\pi}{8}\right)$ are complements, the natural logarithm expression is

$$\left|\ln\left(\tan\frac{\pi}{8}\right)\right| = \left|\ln\frac{\sin\frac{\pi}{4}}{1+\cos\frac{\pi}{4}}\right| = \left|\ln\frac{\sqrt{2}}{1+\sqrt{2}}\right| = \left|\ln\frac{1}{1+\sqrt{2}}\right| = |-1| = 1.$$ Class number is equal to 1.

Example 6.8.2.

Let us try, d=-6. Find the class number.

Solution.

D = 24, and the numbers relatively prime to 24 are 1,5,7,11,-11,-7,-5 and -1. By checking whether -24 is a square modulo 5,7 and 11, we can find that character numbers are 1, 1, 1, 1, -1, -1, -1, and -1, respectively.

The sum, therefore is 1+5+7+11-13-17-19-23=-48. Note that there are only two roots of unity: 1 and -1. Consequently, the formula gives us $\frac{2}{2\cdot 24}\cdot|-48| = 2$. The class number is equal to 2.

6.9. Real and Imaginary Quadratic Field with Low Class Numbers

The study of the growth of class numbers of real quadratic field is more complicated than the imaginary numbers. For example, it is a classical conjecture of Gauss that there are infinitely many real quadratic fields of class number 1.

Now, we will look at the real and imaginary field numbers with low class numbers including class number 1 and class number 2 with their properties. Cohen and Lenstra formulated general conjectures about the distribution of class groups of quadratic fields.

Gauss's hypothesis is that there are infinitely many quadratic fields with class number one. This is called "class - number one problem for real quadratic fields. "This hypothesis is not proved until today. Gauss also conjectured that as $d \to -\infty$, the class number will approach $+\infty$.

Table VI.1 Negative discriminants d corresponding to imaginary quadratic fields

d	3	4	7	8	11	15	19	20	23	24	31	35	39	40	43
class number h(d)	1	1	1	1	1	2	1	2	3	2	3	2	4	2	1

Definition

6.9.1.

A discriminant is fundamental if -d is not divisible by any square number s^2 such that $h(-\frac{d}{s^2}) < h(-d)$.

Exercise

6.9.1.

Note that h(-63)=2. Here, -63 is not fundamental discriminant. See that $63=3^2\times 7$ and $h\left(-\frac{63}{3^2}\right)=h(-7)=1$. Consequently, $h\left(-\frac{63}{3^2}\right) < h(-63)$

The complete list of negative discriminants with class numbers 1 to 5 and odd 7 to 23 are known. The mathematician Buell also gives the list of the smallest and the biggest class numbers for the fundamental discriminant less than 4,000,000. He was even able to categorize them into

i. even discriminants ii. discriminants 1 (mod8) iii. discriminants 5 (mod8)

Below is the table showing the discriminants to some real quadratic fields.

Table VI.2 Positive discriminants d corresponding to imaginary quadratic fields

d	5	8	12	13	17	21	24	28	29	33	37	40	41	44	53
class number h(d)	1	1	1	1	1	1	1	1	1	1	1	2	1	1	1

Table VI.3 Negative Fundamental Discriminants d with class number $h \geq 3$.

h(d)	**d**
1	5,8,12,13,17,21,24,28,29,33,37,41,44,53,56,57,61,…
2	40,60,65,85,104,105,120,136,140,156,165,168,185,204,…
3	229,257,316,321,469,473,568,733,761,892,993,1016,1101,…
…….	……

h(d)	N	d
1	9	3,4,7,8,11,19,43,67,163
2	18	15,20,24,35,40,51,52,88,91,115,123,148,187,232,235,267,403,427
3	16	23,31,59,83,107,139,211,283,307,331,379,499,547,643,883,907

Table VI.4 Positive Fundamental Discriminants d with class number $h \geq 3$.

The largest negative discriminant with class numbers 1,2,3,… are 163,427,907,1555,… Upper bound for this list is not known

The table below has the list of first few positive fundamental discriminants with small class numbers h(d).

When you look at the first numbers under the column d, you can see that the smallest d with h(d)=1,2,3… are 5,40,229,…., and so on.

i. Quadratic Field with Class Number One

It was proved in 1966 by Baker that there are exactly nine imaginary quadratic class number one. They are $Q\left(\sqrt{-d}\right)$ with d=1, 2, 3, 7, 11, 19, 43, 67, 163. Class number of $Q\left(\sqrt{-d}\right)$ grows like $\sqrt{d}$. More precisely, $\log h(-d) \sim \frac{1}{2}\log d$ as $d \to \infty$.

Let D be a square free integer of the form $D = 4n^2 + 1$ where n is a natural number.

We can say that there are exactly 11 real quadratic fields $Q(\sqrt{d})$ of class number one:

D=5, 13, 17, 29, 37, 53, 101, 173, 197, 293, 677

The conjectures of S. Chowla and Yokoi discusses the special families of real quadratic fields of Richaud:Degert type, and prove that at least one conjecture is true.

Theorem 6.9.1.

There exists at most one $D \geq e^{16}$ with class number equal to 1.

Theorem 6.9.2.

If the class number is equal to 1 and $D < e^{16}$, then

$D = 5,13,29,53,173,293$ when $D = n^2 + 4$ and

$D = 5, 17, 37, 101, 197, 677$ for $D = 4n^2 + 1$.

This theorem gives complete characterization of quadratic fields with class number 1.

Theorem 6.9.3.

The following thirty nine fields with possible one more field of large discriminant, are the only real quadratic fields $Q(\sqrt{D})$ of R:D type which have class number one, i.e.

$$D \in \left\{ \begin{matrix} 2,3,6,7,11,14,17,21,23,29,33,37,38,47,53,62,77,83,101,141,167, \\ 173,197,213,227,237,293,398,413,437,453,573, \\ 677,717,1077,1133,1253,1293,1753 \end{matrix} \right\} \cup \{?\} \Leftrightarrow h(D) = 1$$

ii. Quadratic Field with Class Number Two

There are at most 17 real quadratic fields $Q(\sqrt{d})$ are of class number 2. Also, if we assume the generalized.Riemann Hypothesis, there are exactly 16 real quadratic fields $Q(\sqrt{d})$ of class number 2.

$D = 10,\ 26,\ 65,\ 85,\ 122,\ 362,\ 365,\ 485,\ 533,\ 629,\ 965, 1157, 1685, 1853, 2117,$ and 2813.

Recently, Byeon and Jungyu proved the following theorem on Class Number 2 problem for real quadratic fields. They actually applied Biro's method to class number 2.

Conjecture.

Let n be an odd integer and $d = n^2 + 1$ be an even positive square free integer. Then the class number, h (d) will be 2 if and only if $d = 10, 26, 122, 362$. Specifically, they proved the following theorem.

Theorem 6.9.4.

If $d = n^2 + 1$ is an even positive square free integer with $n > 3045$, then $h(d) > 2$, where h(d) denotes $Q(\sqrt{d})$.

Propositon 6.9.1.

If the class number is equal to 2, then $D=n^2 + 4 = pq$, where $p < q$ are both primes. This proposition will be given without its proof.

Theorem 6.9.5.

For $k = Q(\sqrt{D})$, where $D = n^2 + 1 = pq$, if the class number is equal to 2, then $n=t$ for D even and $n = 2t^s$ for D odd, when t is a prime number and s=1 or 2.

Proof.

Only one of the cases, where D is odd will be proven here.Let us assume that t is the smallest prime factor of $\frac{n}{2}$.

Case 1: $D \equiv 1 \pmod 8$. Then, $\frac{n}{2}$ will be an even number.(by Lemma A and B) In other words, t = 2.On the other hand, when $2^2 < \frac{n}{2}$, we have the fact $Q(\sqrt{D}) > 2$, a contradiction. As a conclusion, $2^2 \geq \frac{n}{2}$. That means, $n = 2 \times 2$ or $n = 2 \times 2^2$

Case 2: $D \equiv 5 \pmod 8$. In this case $\frac{n}{2}$ will be an odd number.

When $t^2 < \frac{n}{2}$, then (by Lemma A and B) $-1 = (\frac{D}{t}) = (\frac{n^2+1}{t}) = (\frac{1}{t}) = 1$. This is a contradiction. Note that $(\frac{D}{t})$ shows the Jacobean symbol.

6.10. Survey of the problem on Class Numbers of Quadratic Fields

Where are all the number fields with class number? As the final part of my master thesis, I would like to give a survey of solutions of the class number problem for quadratic number fields.

I. Gauss' Conjectures

Euler discovered the following.

Theorem 6.10.1. (Euler)

x^2-x+41 is prime for x=1,2,...,40

Euler's finding actually is very close and connected to Gauss' problem on class number one. Later, in 1913, Rabinovitch reached the following.

Theorem 6.10.2. (Rabinovitch)

Therefore, the following two statements are equivalent:

1. The values of the polynomial $x^2-x+\frac{1+|D|}{4}$ is prime for $x=1,2,...,\frac{|D|-3}{4}$.

2. The imaginary quadratic number field $Q\left(\sqrt{D}\right)$ is uniquely factorable.

Euler's result is equivalent to that the class number of $Q\left(\sqrt{-163}\right)$ is 1.

In 1801 Gauss, studied some very famous conjectures as follows:

1. $h_K=h(-D)\to+\infty$ as $-D\to-\infty$, where $h_K=h(-D)$ represents the class number of imaginary quadratic number fields $K=Q\left(\sqrt{-D}\right)$.

2. There exists exactly nine imaginary quadratic number fields with class number one. Gauss also discovered that these number fields are

-D = -3,-4,-7,-8,-11,-19,-43,-67, and -163.

Gauss, later obtained that there are 18 imaginary quadratic number fields with class number 2.

3. Finally, he showed that there exists infinitely many real quadratic number fields with class number 1.

II. Dirichlet's Class Number Formula

The following formula about the class number was first proposed by Jacobi[25] in 1832. Later, Dirichlet proved it completely in 1839.

Theorem 6.10.3. (Jacobi:Dirichlet)

Let D be discriminant of the quadratic number field $K=Q\left(\sqrt{D}\right)$ and $h_K=h(D)$ is the class number. Then

$$h_K=h(D)=\begin{cases}\dfrac{w_D\sqrt{|D|}L(1,\chi_D)}{2\pi}, & \text{if } D<0\\ \dfrac{\sqrt{|D|}L(1,\chi_D)}{2\log\varepsilon_D}\end{cases} \qquad \text{where } L(1,\chi_D)=\sum_{n=1}^{\infty}\frac{\chi_D(n)}{n}>0,$$

χ_D is the Kronecker symbol of the field K, $w_D=\begin{cases}6, & \text{if } D=-3\\ 4, & \text{if } D=-4\\ 2, & \text{if } D<-4\end{cases}$

and ε_D is the fundamental unit of K. $(D>0)$

III. Research Works between 1900 and 1950

The studies made by Hecke (cf. Landau,1918), Deuring (1933), Mordell[20](1934) resulted in solving the Gauss's conjecture as follows.

Theorem 6.10.4. (HeckeDeuringMordell:Heilbronn)

$h(-D) \to +\infty$ as $-D \to -\infty$

In 1934 Heilbronn and Linfoot[6] found the following.

Theorem 6.10.5. (Heilbronn:Linfoot)

Besides D = -3, -4, -7, -8, -11, -19, -43, -67 and -163 there exists at most one more imaginary quadratic number field $Q(\sqrt{D})$ with class number 1. In 1935, Siegel proved the following theorem.

Theorem 6.10.6. (Siegel)

For any given positive constant $\delta>0$, positive constant $c(\delta)$ there exists some such that $L(1,\chi_D)>c(\delta)|D|^{-\delta}$.

Remark 1.

The constant $c(\delta)$ is not effectively computable. In 1951, T.Tatuzawa[23] proved the following.

Theorem 6.10.7. (Siegel:Tatuzawa)

Let $0<\delta<\frac{1}{2}$ and $|D| \geq \max\left(e^{\delta^{-1}}, e^{11.2}\right)$.

Then, for all quadratic number fields except at most one such field, we have $L(1,\chi_D)>0.655\delta|D|^{-\delta}$. In 1928, J.E. Littelwood[8] proved the following.

Theorem 6.10.8. (Littelwood)

By Generalized Riemann Hypothesis, we have

$$\left((1+o(1))\frac{12e^{\gamma}}{\pi^2}\right)^{-1} < L(1,\chi_D) < \left((1+o(1))2e^{\gamma}\log\log|D|\right)$$ where γ is Euler's constant.

In 1979, J. Oesterle found the same result with explicit constant without using the term $1+o(1)$.

IV. Complete Determination of the Imaginary Quadratic Fields with Class Number 1 or 2

Theorem 6.10.9. (Heegner:Baker:Stark)

There exists exactly 9 imaginary quadratic number fields with class number 1, and 18 imaginary quadratic number fields with class number 2.

For class number 1, the discriminants are:-3,-4,-7,-8,-11,-19,-43,-67,-163.

For class number 2, the discriminants are:
-15,-20,-24,-35,-40,-51,-52,-88,-91,-115,-116,-123,-148,-187,-235,-267,-403,-427.

V. Final Solution for Gauss's Problem on the Class Numbers of the Imaginary Quadratic Number Fields

The studies done by D.Goldfeld$[4](1975)$,B.Gross and D.Zagier(1983)completely solved Gauss' conjecture on the class number of the imaginary quadratic number fields. They found the following result.

Theorem 6.10.10. (Goldfeld:Gross:Zagier)

For any given $\delta>0$, there exists effectively computable positive constant $c(\delta)$ such that $h(D)>c(\delta)\left(\log|D|\right)^{1-\delta}$,

where $h(D)$ is the class number of the imaginary quadratic number field $Q\left(\sqrt{D}\right)$.

Later, J.Oesterle(1984),J.Buhler,B.Gross and D.Zagier proved the following.

Theorem

6.10.11.

For the class number $h(D)$ of the imaginary quadratic number fields $Q\left(\sqrt{D}\right)$

$h(D)> \frac{1}{55}\left(\log|D|\right)\prod_{\substack{p/D \\ p\neq|D|}}\left(1-\frac{\left[2\sqrt{p}\right]}{p+1}\right)$ where p runs through the prime numbers.

In 1986, Lu Hongwen$[31]$ improved the estimate with 54 instead of 55.

VI. Gauss' Class Number Problem on the Real Quadratic Number Fields

When we use the Dirichlet's class number formulae, it can be seen that there are fundamental difficulties in both the effectiveness of the lower bound estimate of $L(1,\chi)$ and the regular $\log\varepsilon_D$. Most of the times the fundamental unit ε_D of the real quadratic number field $K=Q\left(\sqrt{D}\right)$ with discriminant $D > 0$ can be found as follows:

Let $A = \left[a, \frac{b+\sqrt{D}}{2}\right]$ be a representative of the ideal class $\{A\}$ in K. Therefore, there exist rational integers a,b such that $|b| \le a \le \frac{D-b^2}{4a}$ ÎZ, where $GCD\left(a,b,\frac{D-b^2}{4a}\right)=1$.

Expand $a=\frac{b+\sqrt{D}}{2}$ into simple continued fractions $\alpha=[a_0,a_1,...,a_k]$, where $a_1,...,a_k$ is the fundamental period. Then we have

$\varepsilon_D=p_{k-1}+\frac{-b+\sqrt{D}}{2a}q_{k-1}$ where $\frac{p_{k-1}}{q_{k-1}}=[a_0,a_1,...,a_{k-1}]$ is the k-1 th asymptotic fraction.

Let $p(\{A\}) = k$. It is obvious that $p(\{A\})$ does not change as the representative of the ideal class $\{A\}$ changes. Define $p(K)= p\left(Q\left(\sqrt{D}\right)\right)=\frac{1}{h_K}\sum_{\{A\}} p(\{A\})$ through the ideal class group of $K=Q\left(\sqrt{D}\right)$. We call $p(K)$ as the length of the field. Then we have

Theorem 6.10.12.

When D is taken over all positive fundamental discriminants, we have

$\lim_{D\to\infty}\frac{\log p\left(Q\sqrt{D}\right)}{\log\log\varepsilon_D} = 1$. This is the restatement of Lu Hongwen's work [30](1986).

From Theorem 6.10.12 follows the following.

Theorem 6.10.13.

Assume that Gauss' conjecture is valid. i.e., there exists infinitely many real quadratic number fields $K=Q\left(\sqrt{D}\right)$ with class number $h_K=1$. Therefore, we have

$\lim_{D\to\infty}\frac{\log p(\alpha_D)}{\log\log D}=\frac{1}{2}$ where D runs through the discriminants

of those real quadratic number fields

$Q\left(\sqrt{D}\right)$ with class number 1, $\alpha_D=\begin{cases}\frac{1+\sqrt{D}}{2}, & \text{if } D\equiv 1 \pmod 4\\ \frac{\sqrt{D}}{2}, & \text{if } D\equiv 2,3 \pmod 4\end{cases}$

and $p(\alpha_D)$ is the length of fundamental period in the continued fraction of α_D.

Theorem 6.10.13 is a corollary of Theorem 6.10.12, Dirichlet's class number formula, Siegel Theorem and trivial estimate $L(1,\chi_D)<\log|D|$. By the Theorem 6.10.13, we can easily see that $p(\alpha_D)$ should be quite large for the real quadratic number fields $Q(\sqrt{D})$ with class number 1 and larger discriminant D.

According to the Siegel-Tatuzawa Theorem, for smaller $p(\alpha_D)$ there exist much fewer real quadratic number fields $Q(\sqrt{D})$ with class number 1. The following example is a typical one.

S.Chowla's Conjecture

There exists exactly 6 primes $p=4N^2+1$, (N is positive integer) such that the class number of all real quadratic $Q(\sqrt{D})$ is 1. Those six primes are p=5,17,37,101,197 and 677 corresponding to N=1,2,3,5,7 and 13.
respectively are such primes. Besides, from the Siegel-Tatuzawa Theorem it follows that there exists at most one more exceptional such prime. In 1988, Lu Hongwen [33] proved that if such exceptional prime exists, it should be greater than $10^{3.8\times10^7}$.
Lu Hongwen found some conditions under which the exceptional prime exists. Among them are the following results.

Theorem 6.10.14.

[27] (1979) Let $p=4N^2+1$, (N positive integer). Then class number of real quadratic field $Q(\sqrt{p})$ is $1 \Leftrightarrow N^2+t-t^2=$prime for $2 \le t<N$.

Theorem 6.10.15.

[28] (1980) Let $p=4N^2+1$ (N is positive integer) be a prime.

Then class number of real quadratic number field $Q(\sqrt{p})$ is 1, if and only if all prime numbers $q < N$ are the quadratic non-residue of p.

Theorem 6.10.16.

[29] (1984) Let $p=4N^2+1$ (N positive integer and N>2)

If the class number of the real quadratic number field $Q(\sqrt{p})$ is 1, then the class number of the imaginary quadratic number field $Q(\sqrt{-4p})$ is

$$h(-4p)=\begin{cases}2N+4, & \text{for } N\equiv 1(\text{mod}4)\\ 2N-4, & \text{for } N\equiv 3(\text{mod}4)\end{cases}$$

Remark 2.

After 8 years since Lu Hongwen's work, A.Mollin[18](1987)and H.Yokoi refound the Theorem C and D.

Remark 3.

The method used in the proof of Theorem 6.10.14, 6.10.15 and 6.10.16 could be used. in other fields with smaller $p(\alpha_D)$ similarly.

RESULTS AND CONLUSION

This project has been an attempt to analyze different methods in computing the class number of quadratic number fields. The thesis provides the reader with numerous examples of notions he or she has seen in the algebra, numerical analysis courses: groups, rings, fields, ideals, quotient rings, quotient fields, ideal class group and of course, class number.

In the second chapter, I emphasized the concept of quadratic fields and introduced modules, quadratic residues with Jacobi and Kronecker symbols with numerous examples.

In doing so, the thesis first laid the foundation for class number concept and investigated the ring of modules, integral extension, units in real and imaginary quadratic fields. At this step, since it was very important in calculation of the class number, I emphasized the continued fraction method in finding the fundamental unit and introduced the Dirichlet Characters of Quadratic Number Fields as this would be one of my methods in the chapters to come.

Apart from Dirichlet, I also focused on Unique Factorization in algebraic number fields and ideals before I introduce the class number concept.

Later in the thesis, I briefed the history of the class number problem and studied the ideal class group concept together with Hurwitz constant. I mainly presented several methods in finding the class number of quadratic fields including Minkowski's bound, Dirichlet's class number formula and Using modules for the calculation of the class number and give an idea

to the reader which of these methods could be more effective in specific situations. Later in the chapter, I mainly focused on the low class numbers for quadratic fields, and listed the class numbers separately for real and imaginary fields.

Last part of this thesis is devoted to a study in finding the complete determination of the real and imaginary quadratic fields with class number 1 or 2, starting with Gauss' conjecture followed by Jacobi: Dirichlet formula and also obtaining the final solution to the class number problem in a chronological order and give the reader the idea of what could be the next on class number problem and what part of the problem remain unsolved until today.

REFERENCES

[1] On the Class Numbers of Imaginary Quadratic Fields by Svirsky, Janet Burstein, Ph.D. John Hopkins University, 1985, 83 pages; AAT 8510443.

[2] Class numbers and Sums of Squares in a Quadratic Field by Lofquist, George Warthen, Ph.D., Louisiana State University and Agricultural & Mechanical College, 61 pages.

[3] Computations of Class Numbers of Quadratic Fields by Srinivasan, Anitha, Ph.D., University of Georgia, 1995, 95 pages; AAT 9604077.

[4] Introduction to Number Theory, William W. Adams, Larry Joel Goldstein class number problem for the real quadratic fields of R:D type, Leu, Ming. Ph.D. John Hopkins University.

[5] The class number one problem for some real cubic number fields with negative discriminants by Stephanie R. Louboutin.

[6] Algebraic Number Theory, Milne.

[7] Class Numbers of Orders in Cubic Fields by Anton Deitmar, Department of Mathematics, University of Exeter, Exeter EX4 4QE, Devon, United Kingdom.

[8] Class Numbers with Many Prime Factors by Kalyan Chakraborty, Florian Luca, Anirban Mukhopadhyay, Constructing infinitely many number fields of any given degree whose class numbers have many prime factors.

[9] Ideal theory: Introductory Lectures on Rings and Modules: Supplement copyright 1999 by John Beachy.

[10] Problems in Algebraic Number Theory, copyright 2007 by Murthy and Esmonde.

[11] Algebraic Theory of Numbers by Pierre Samuel, copyright 2008.

[12] On the p-divisibility of class numbers of quadratic fields. Dina Haballah Khalil.

[13] A class number problem for quadratic number fields. Leu Ming Guan Ph.D., 1989.

[14] Class numbers of imaginary quadratic fields. Mark James Watkins UMI, 2002.

[15] Elliptic curves and class groups of quadratic fields. Duncan Alan Buel, Chicago, UIC, 1976.
[16] Existence of certain fundamental discriminants and class numbers class number of real quadratic fields, Dongho Byeon, Seoul National University, 2002.
[17] A note on the Divisibility of Class Number of Real Quadratic Fields, Gan Yu, University of Michigan, 2001.
[18] On the real quadratic function fields, Erwan Le Yaouanc.
[19] A.Baker, Linear forms in the logarithm of algebraic numbers, 204-206.
[20] A.Baker, Imaginary quadratic fields with class number two, 139-152.
[21] S.Chowla, Class number and quadratic residues.
[22] D.M.Goldfeld, The class number of quadratic fields, 623-663.
[23] Heilbronn, On the class number in imaginary quadratic field, 150-160.
[24] Heilbronn, On the imaginary quadratic corpora of class number 293-301.

[25] C.G. Jacobi, 189-192.
[26] J.E. Littlewood, On the class number of $P\left(\sqrt{-k}\right)$, 358-372.
[27] H.Lu, On the class number of real quadratic field, 118-130.
[28] H.Lu, On the real quadratic fields with class number 1, 133-135.
[29] H.Lu,Kronecker, Limit formula of real quadratic fields, 1233-1250.
[30] H.Lu, On the period of simple continued fractions, 433-443.
[31] H.Lu, A note on the Goldfeld theorem, pg 36.
[32] H.Lu, M.Zang, Gauss'conjectures in Quadratic number fields, 1993.
[33] H.Lu, Chowla's conjecture on a class of real quadratic fields, 1998.
[34] P. Dei, H.Lu, Modular forms of class number of quadratic fields, 1990.
[35] G.Ji, H.Lu, Class number and computers, 1991.
[36] R.A. Mollin, Class number one criteria for real quadratic fields, 162-164.
[37] R.A.Mollin, A conjecture of Chowla, 1988, 794-796.
[38] L.J.Mordell, On the Riemann Hypothesis and imaginary fields, 289-298.
[39] H.M.Stark, Complete determination of complex quadratic fields, 1-27.
[40] H.M.Stark, A transcendence theorem for class number problem, 153-173.
[41] T.Tatuzawa, On a theorem of Siegel, 163-178.
[42] H.Yokoi, Class number one problem for certain real quadratic fields, 125-137.