CLC__________ Number__________

UDC__________ Available for reference □ Yes □ No

SUSTech

Southern University
of Science and
Technology

A Dissertation for Bachelor's Degree

Thesis Title:This is a very very very very very very long title just for testing the page

Student Name: ______________________________

Student ID: ______________________________

Department: ______________________________

Program: ______________________________

Thesis Advisor: Prof. XXXX

Date: April 15, 2019

COMMITMENT OF HONESTY

1. I solemnly promise that the paper presented comes from my independent research work under my supervisor's supervision. All statistics and images are real and reliable.

2. Except for the annotated reference, the paper contents no other published work or achievement by person or group. All people making important contributions to the study of the paper have been indicated clearly in the paper.

3. I promise that I did not plagiarize other people's research achievement or forge related data in the process of designing topic and research content.

4. If there is violation of any intellectual property right, I will take legal responsibility myself.

Signature: ___________________

Date:___________________

Preface

This thesis is intended to summarize the learning outcomes and some works done by me during the undergraduate period in south university of science and technology of china (SUSTC). In this thesis, I choose two topics, one is related to algebraic number theory and the other one is something about function fields. The central idea or tool is the Galois theory, which connects the two part for this paper. For the number fields part, I have rearrange many references and books in order to give a simple and clear skeleton. For the function fields, we prove an explicit theorem, which is useful for studying the discrete (finite) subgroups of the automorphism group of a function field.

Before the main contents of the thesis, I would like to take some words for my process on studying mathematics during the time in SUSTC. Although there is no mathematics department for our newly established university, I am grateful that I have learn many mathematics, especially abstract algebra, algebraic number theory and algebraic geometry from Prof. Xianke Zhang, and Prof. Jietai Yu in the University of Hongkong etc.

As a student who loves mathematics very well, I have met so many kindly and responsible mathematicians during my 3.5-years' college life. During the first two years, as the representative of mathematics lessons in our inaugural class across all majors, I have "obligation" to get good grades on mathematics lessons in order to set a good example. I learned Calculus and Analysis from Prof. Xuefeng Wang in mathematics department of Tulane University, Prof. Jinzhong Zhang in Guangzhou University, Prof. Zhongkan Liu in SUSTC and Beihang University, who is my first supervisor. We had frequent discussions on some topics on analysis as well as many other topics like elementary geometry and ordinary differential equation etc.

After entering financial mathematics department, I also learned ordinary differential equation, probability, stochastic process, numerical methods, as well as some statistics from the professors in the department. Among of them, Prof. Anyue Chen, Prof. Jingzhi Li, Prof. Xuejun Jiang, Prof. Huaiqing Wang, Prof. Dejun Xie and Prof. Bianxia Sun gave me so many supports. Especially, Prof. Li, as my graduation designation supervisor, encouraged me a lot on studying algebra, and helped me to know some good mathematician friends of him.

Prof. Xianke Zhang, supervisor of me (after Prof. Liu) and an academic supervisor of this thesis, has guided me into the world of abstract algebra, a field which is quite abstruse for freshman. However, I found appealing thing inside the abstract definitions and complex relations one day. After that, besides the formal classes, we held several seminars on algebraic number theory and commutative algebra etc under the guidances of Prof. Zhang.

Prof. Jietai Yu who has inspired me on Galois theory and algebraic geometry, has given me many guidances on research area as well as daily life. He gave us Galois courses as well as seminar on algebraic geometry. Among that time, I had my first opportunity to give a presentation in the formal seminar. I still remember the topics for that seminar is the finite subgroups of $\mathrm{PGL}(2, \mathbb{C})$ (we will show the relevant topic in chapter **??**). What's more, Prof. Yu found more opportunities for me to learn more mathematics as well as to further my study.

During those experiences outside the campus, I have learnt more recent works on affine algebraic geometry. The happiest things for me during those academic activities are finding many good friends, like Swapnil Lokhande, Sagar Kolte, Shameek Paul, Shihong Ma, Ju Huang, Haifeng Tian etc. They really gave me so much encouragement and concern. Also, I also met many good mathematician, like Prof. Alexey Belov, Prof. Leniod Makar-Limanov, Prof. Wenhua Zhao, Prof. Fang Li, Prof. Xiankun Du and so on. They gave me some instructions on some problems and encouraged me on studying mathematics.

Last but not least, I've come to realize that the ability of self-study is the most important good properties for a university student. I have paid much time to learn something outside the courses, to find some interesting topics, to sort out learning knowledge. During these years, I wrote a personal mathematics blog to record those things.

Wenchao ZHANG
September, 2014 at SUSTC

Contents

Preface · · · · · · · · · · III

Contents · · · · · · · · · · V

摘　要 · · · · · · · · · · VII

ABSTRACT · · · · · · · · · · IX

Notations · · · · · · · · · · XI

Chapter 1　Introduction · · · · · · · · · · 1

Chapter 2　Galois Theory · · · · · · · · · · 3

2.1 Galois Extension · · · · · · · · · · 3

2.2 The fundamental theorem of Galois theory · · · · · · · · · · 4

2.3 Galois Groups of Polynomials · · · · · · · · · · 4

2.4 Dedekind's Criterion · · · · · · · · · · 5

2.5 Computing Galois Group of a Polynomial · · · · · · · · · · 6

Chapter 3　Algebraic Number Theory · · · · · · · · · · 9

3.1 Algebraic Numbers and Number Fields · · · · · · · · · · 9

3.2 Discriminants of Elements and Fields · · · · · · · · · · 9

3.3 Decomposition of Prime Numbers · · · · · · · · · · 11

3.4 Units and Ideal Classes · · · · · · · · · · 12

3.5 Character and Conductor · · · · · · · · · · 14

Chapter 4　Quadratic Fields · · · · · · · · · · 17

4.1 Discriminant, Integral Basis · · · · · · · · · · 17

4.2 Decomposition of Primes · · · · · · · · · · 17

4.3 Unit Group of Imaginary Quadratic Fields · · · · · · · · · · 18

4.4 Class number of Imaginary Quadratic Fields · · · · · · · · · · 18

4.5 Unit group of Real Quadratic Fields · · · · · · · · · · 19

4.6 Class Numbers of Real Quadratic Fields · · · · · · · · · · 20

Chapter 5　Cyclic Cubic Fields · · · · · · · · · · 21

5.1 Cubic Polynomial and Cyclic Cubic Field · · · · · · · · · · 21

5.2 Discriminant and Integral Basis · · · · · · · · · · 23

5.3 Prime Decomposition · · · · · · · · · · 25

5.4 Units and Class Number · · · · · · · · · · 26

5.5 Conductor of Cyclic Cubic Field · · · 26
5.6 Examples · · · 27
5.6.1 An Example for Prime Decomposition · · · 27
5.6.2 Some Examples for computing class group · · · 27
5.7 Some Special Cyclic Cubic Fields · · · 27
5.7.1 Cubic Trinomials · · · 27
5.7.2 Simplest Cubic Fields · · · 29
Chapter 6 Cyclic Sextic Fields · · · 31
6.1 Discriminant and Integral Basis · · · 31
6.2 Prime Decomposition · · · 33
6.3 Unit and Class Number of Real Cyclic Sextic Field · · · 34
6.4 Unit and Class Number of Complex Cyclic Sextic Fields · · · 35
Chapter 7 Examples for Cyclic Sextic Fields · · · 37
7.1 7-th Cyclotomic Field · · · 37
7.1.1 Cyclotomic Fields · · · 37
7.1.2 7-th Cyclotomic Field · · · 38
7.2 A Real Cyclic Sextic Field · · · 40
7.3 Sextic Trinomials · · · 41
Chapter 8 Galois Extensions of Function Fields · · · 43
8.1 Existence Theorem · · · 43
8.2 Explicit Form of Invariants · · · 45
Appendix A Table of Orbit-length Partition for Small Degree Polynomials · · · 51
Appendix B Resultant and Discriminant of a Polynomial · · · 53
Appendix C The Legendre-Jacobi-Kronecker Symbol · · · 55
C.1 The Legendre Symbol · · · 55
C.2 The Kronecker Symbol · · · 55
Acknowledgements · · · 57

摘　要

本文主要分为两个部分，前半部分主要研究了六次循环域的结构。首先将代数数论的一般理论、二次域和循环三次域的主要理论和近期文献中有关三次、六次循环域的结果, 进行了整理综合。在此基础上, 我们给出了一般六次循环域的整基，素分解的方法，具体给出了多个例子。例如，我们解决了最简单的复六次循环域——7 次分圆域的判别式，整基，素分解。同时，利用一般的类数和单位的理论，计算了它的类数和单位群。其次，我们给出了一个实六次循环域，在解决该例子时先利用线性预解子的方法判定出所给多项式 $f(x) = x^6 - x^5 - 6x^4 + 6x^3 + 8x^2 - 8x + 1$ 的伽罗瓦群为 C_6，即得到其对应的分裂域为六次循环域。之后，通过六次循环域的结果给出该例子的二次子域和三次循环子域，从而进一步得到它的整基、素分解，并且我们还计算了这个域的类数。

六次循环域整基和素分解的一般结果是在利用解析数论方法得到判别式的前提下，利用其子域结构得出来的。

第二部分研究的是函数域上的伽罗瓦扩张。在经典的代数和代数几何理论中，Lüroth 定理揭示了一元函数域 $K(x)$ 和基域 K 的中间域 E 是基域的单扩张（中间域不等于基域时为非代数扩张）。进一步地，本文假定 $K(x)/E$ 为伽罗瓦扩张，不利用 Lüroth 定理，证明了 $E = K(u)$, 其中 $u \in K(x)$，可以被 Gal$(K(x)/E)$ 的初等对称多项式所确定。我们在其后也给出了一个经典 Gal$(K(x)/E) = D_3$ 的例子。

关键词：　伽罗瓦理论, 六次循环域, 整基, 素分解,Lüroth 定理

ABSTRACT

We have two parts in this thesis. In the first part, we study the structure of cyclic sextic field with many details on its subfields: quadratic field and cyclic cubic field. We reorganize main theory of algebraic number theory and some recent references on cyclic cubic field and cyclic sextic field. Based on these results, we solve the integral basis of the cyclic sextic field as well as find the prime decomposition algorithm. Precisely, we give some examples applying our results. For example, we solve discriminant, integral basis, prime decomposition of 7-cyclotomic field. We also compute its unit group and class number using general theory. We also give an example for real cyclic sextic field. Using linear resolvent method, we first determine that the minimal polynomial has Galois group C_6. Then we also find the quadratic subfield and cyclic cubic subfield in order to get the integral basis and prime decomposition. We compute the class number as well.

The general results for integral basis and prime decomposition of cyclic sextic field are given by structures of its subfields based on its discriminant which is computed through analytic number theory's method.

In the second part, we discuss Galois extensions of a function field. In the classical theory of algebra and algebraic geometry, Lüroth's theorem reveals that any intermediate field E/K of $K(x)/K$ (where x is transcendental extension over K) is a simple extension. More precisely, assuming that $K(x)/E$ is Galois, without using Lüroth's theorem, we prove that $E = K(u)$, where $u \in K(x)$ can be determined by the elementary symmetric polynomials. We then give a classical example for Gal$(K(x)/E) = D_3$.

Keywords: Galois Theory,Cyclic Sextic Fields, Integral Basis, Prime Decomposition, Lüroth's Theorem

Notations

$\mathbb{Q}$	rational number field
$\mathbb{Z}$	rational integer ring
K	algebraic number field
O_K	the ring of integers of K
Aut(K/F)	Automorphism group of K which fixes F
Gal(K/F)	Galois group of K which fixes F
Res(f, g)	resultant of polynomials $f(x)$ and $g(x)$
$R_{p,f}$	resolvent polynomial of $f(x)$ with $orb(p)$
Disc(f)	discriminant of polynomial f
Disc(θ)	discriminant of minimal polynomial of θ,i.e. Disc$(1, \theta, \ldots, \theta^{n-1})$
ht(f)	height (or degree) of a rational function f
$d(K)$	discriminant of field K
N(α)	Norm of α
Tr(α)	Trace of α
C_n	cyclic group
$Cl(K)$	class group of K
$h(K)$	class number of K
$U(K)$	group of units in K
ζ_n	n^{th} root of unity

Chapter 1 Introduction

Formally, there are 2 parts and 8 chapters in this thesis. The first 4 chapters, namely chapter 2-4, mainly refer to some reviews for Galois theory and Algebraic Number theory etc. In chapter 6-8, we obtain some results on cyclic sextic fields and Galois extensions of function fields. And then, we also give some examples using our consequences.

Algebraic Number Theory and Algebraic Geometry are two central researching frontiers of pure mathematics. To find the discriminant, integral basis, class number of a algebraic number field is a classical question in algebraic number theory. More accurately, if we consider the splitting field of the polynomials over $\mathbb{Q}$, which is certainly Galois, then some restrictions from Galois extension will affect the structures of the field. Igor Shafarevich showed that every finite solvable group G is realizable over $\mathbb{Q}$, i.e. there exists a field K such that Gal$(K/\mathbb{Q}) \cong G$. This is related to a famous question, the Inverse Galois Problem. For our cases, we focus on some simple cyclic fields which have cyclic group as its Galois group over $\mathbb{Q}$.

We introduce Galois theory in chapter **??**. The Galois theory is the principal connection between the two parts of the thesis. In chapter **??**, we will first introduce some necessary preliminaries of Galois Theory for our results based on Emil Artin's book [**?**] and David A. Cox's book[**?**]. Then, we focus on computing the Galois group of a polynomial. We sort out some useful materials from A. Healy [**?**], C. Bright [**?**], and L. Soicher and J. McKay [**?**].

One will find that chapter 3-5 have almost the same content's structure, i.e. we have several common sections like the discriminant, integral basis, decomposition of prime, unit group and class number and so on. In fact, Chapter 3 is the reviews of general theory for number fields and some analytic number theory. We have paid much time on sorting out the materials from books of Prof. Xianke Zhang [**?**], Henri Cohen [**?**] and Richard Molin [**?**]. In chapter 4 and 5, we have clearly rearranged those results for quadratic field and cyclic cubic field based on Cohen and Zhang's books. Some of results has been modified for the simplicity. In chapter 5, we have posed an example for prime decomposition in cyclic cubic field and two examples for computing the class number of those fields. What's more, we have recovered the results of Seidelmann's paper [**?**] through a lemma in Cohen's book. We also give a formula (See theorem **??**) for a type of cyclic cubic field which is given risen by the ideas of F.C. Orvay's [**?**].

In chapter 6, we first refer to Sirpa Mäki's results [**?**] on discriminant and conductor of a cyclic sextic field, and then get the integral basis and prime decomposition of it. Mäki give a direct result for discriminant, we have tried to recover the result to get it using the conductor-discriminant formula. Then with this message, we complete to find the integral basis of cyclic sextic field. At section **??**, we succeed in obtaining all the cases for decomposition of prime numbers. For real cyclic cubic field, the unit group and class number has been solved for some "small" (actually is quite large) discriminants, we can find a table in Mäki's book. For complex cyclic sextic field, it's a CM-field, hence the class number and the unit group could be reduced into its cyclic cubic field. But unfortunately, we haven't got the final precise results of them.

In chapter 7, we give two examples. One of them is a complex cyclic sextic field and the other is a real cyclic sextic field. For this a complex cyclic sextic field, i.e. 7-th cyclotomic field, we use our results in chapter 6 to get its discriminant and the prime decomposition, integral basis. Then we verify those results through the theory of cyclotomic field. Since this field is quite simple, we use the general theory of class number to find its class number is 1. Then, we also given an inconspicuous example. We first verify the Galois group of the polynomial using the method in chapter 2, then we first compute the polynomial discriminant. After that, using the discriminant formula, we confirm the subfields of it, and also do other processes as we mentioned above except the unit group. We also find another example proposed by A Bremner and B Spearman[**?**] with sextic trinomial, but unfortunately, we haven't got the final results.

Although there is only one chapter for part two, i.e. the Galois extensions in a function field, this is still an important part of my thesis. We have proved two theorem for specializing Lüroth's theorem within Galois extension. More precisely, assuming that $K(x)/E$ is Galois, without using Lüroth's theorem, we prove that $E = F(u)$, where $u \in K(x)$ can be determined by the elementary symmetric polynomials. We then give a classical example for Gal$(K(x)/E) = D_3$.

Chapter 2 Galois Theory

Galois Theory, named after Évariste Galois, is a useful tool to provide a connection between field theory and group theory. From the fundamental theorem of the Galois theory, we could find that the certain problems in field theory can be reduced to group theory, which is in some sense simpler and better understand. Originally, Galois used permutation groups to describe how the various roots of a given polynomial equation are related to each other. The modern approach to Galois theory, developed by Richard Dedekind, Leopold Kronecker and Emil Artin, among others, involves studying automorphisms of field extensions. In this chapter, we will introduce some basic theory of Galois theory and an application of it.

2.1 Galois Extension

For simplicity, we skip the theory of group and some basic definition of field. A field K containing a field F is called an extension field of F. Such an K can be regarded as an F-vector space, and we write $[K : F]$ for the dimension, which we called degree of the extension.

Consider fields K/F, we say the extension K/F is **algebraic** if for any $\alpha \in K$ is algebraic over K, i.e. every element of K is a root of some non-zero polynomial with coefficients in F. The field extensions that are not algebraic are called transcendental.

we say an algebraic field extension K/F is **separable** if for every $\alpha \in K$, the minimal polynomial of α over F is a separable polynomial, i.e., has distinct roots. For F is characteristic 0, any algebraic extension is separable. Also, for any finite field, any algebraic extension of it is separable.

A **splitting field** of a polynomial $p(X)$ over a field F is a field extension K/F which p factors into linear factors and such that the roots generate K over F. We say an algebraic field extension K/F is **normal** if K is the splitting field of a family of polynomials in $F[x]$. Or equivalently, every irreducible polynomial in $F[X]$ that has one root in K, has all of its roots in K.

An F-isomorphism $K \to K$ is called an F-**automorphism** of K. The F-automorphisms of K form a group, which we denote Aut(K/F).

The normal extension K/F is also equivalent to that every embedding (i.e. injective ring homomorphism) σ of K into F^c is an automorphism of K over K.

Definition 2.1.1 (Galois Extension)**.** *A finite extension K of F is said to be Galois if K/F is both separable and normal. The F-automorphisms of K is called the **Galois group** of K over F, and it is denoted by* Gal(E/F).

An important theorem of Emil Artin [?] states that for a finite extension K/F, each of the following statements is equivalent to the statement that E/F is Galois:

Theorem 2.1.1 (Artin)**.** *For an extension K/F, the following statements are equivalent:*

1. *K is the splitting field of a separable polynomial $f \in F[x]$.*
2. *$F = K^G$ for some finite group G of automorphisms of K.*
3. *K is normal, separable and of finite degree over F.*
4. *K/F is Galois.*

2.2 The fundamental theorem of Galois theory

We then call the fundamental theorem of Galois theory which is the central theorem of Galois theory.

Theorem 2.2.1 (The fundamental theorem of Galois theory)**.** *Let K/F is Galois, and $G =$ Gal(K/F). The maps $H \mapsto K^H$ and $M \mapsto$ Gal(K/M) are inverse bijections between the set of subgroups of G and the set of intermediate fields between K and F. Moreover, we have*

1. *the correspondence is inclusion-reversing.*
2. *indexes equal degrees: $(H_1 : H_2) = [K^{H_2} : K^{H_1}]$*
3. *$\sigma H \sigma^{-1} \leftrightarrow \sigma M$*
4. *H is normal subgroup of G if, and and only if, K^H is normal over F, in which case*

$$\mathrm{Gal}(K^H/F) \cong G/H.$$

2.3 Galois Groups of Polynomials

If the polynomial $f \in F[x]$ is separable, then its splitting field F_f is Galois over F, and we call Gal(F_f/F) the Galois group G_f of f. From now on, we just consider the simplest case, i.e. $F = \mathbb{Q}$, and we denote Gal$(f) =$ Gal$(\mathbb{Q}_f/\mathbb{Q})$. Then, any splitting field $\mathbb{Q}_f$ is Galois over $\mathbb{Q}$.

A well-known theorem is that the roots of f are solvable in radical if only if Gal(f) is solvable, which provides some motivation as to why the Galois group of a polynomial is of interest.

Let f be a univariate polynomial with rational coefficients. Throughout this article we suppose that f has degree n and roots $r_1, r_2, \ldots, r_n$. The splitting field $\mathbb{Q}_f$ of f, denoted by $\mathbb{Q}(r_1, \ldots, r_n)$, is a finite extension of $\mathbb{Q}$ generated by the roots of f. Then the Galois group of f is defined to be

$$G_f = \mathrm{Gal}(f) := \mathrm{Gal}(\mathbb{Q}(r_1, \ldots, r_n)/\mathbb{Q}).$$

Observing that the splitting field $\mathbb{Q}_f$ of a monic polynomial $f(x)$ with rational coefficients can be change into a splitting field of a monic polynomial with integer coefficients.

Now we use some words to explain it. Let

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0,$$

where $a_i \in \mathbb{Q}, i = 0, \ldots, n-1$. Assume the greatest common divisor of the denominators is d, then $a_i = b_i/d$, where $b_i, d \in \mathbb{Z}, i = 0, 1, \ldots, n-1$. Hence, we have

$$f\left(\frac{x}{d}\right) = \left(\frac{x}{d}\right)^n + \frac{b_{n-1}}{d}\left(\frac{x}{d}\right)^{n-1} + \cdots + \frac{b_0}{d},$$

Whence,

$$d^n f\left(\frac{x}{d}\right) = x^n + b_{n-1}x^{n-1} + \cdots + b_0,$$

It's clear that the splitting fields of $f(x)$ and $g(x) := d^n f(\frac{x}{d})$ coincide. More precisely, we called $f(x)$ is equivalent to $g(x)$ (resp. G_f is equivalent to G_g) **up to scaling**.

If $f(x) \in K[x]$ is a separable irreducible polynomial of degree n and G_f is its Galois group over K, then the group G_f can be embedded into S_n by writing the roots of $f(x)$ as $r_1, \ldots, r_n$ and identifying each automorphism in the Galois group with the permutation it makes on the r_i's.

In S_n we have the alternating group $A_n \subset S_n$, the following result is famous to determine the Galois group of the polynomial:

Theorem 2.3.1. *Let $K = \mathbb{Q}(\theta)$ be a number field of degree n, where θ is an algebraic integer with $f(x)$ be a minimal polynomial, then $G_f \subset A_n$ if and only if* $\mathrm{Disc}(f)$ *is a square.*

2.4 Dedekind's Criterion

A theorem of Dedekind [**?**] which provides useful information about G_f over $\mathbb{Q}$.

Theorem 2.4.1 (Dedekind's criterion)**.** *Let $f(x) \in \mathbb{Z}[x]$ be a monic irreducible polynomial of degree n. Put $f_p(x) = f(x) \mod p$. Suppose $f_p(x)$ is a product of monic irreducible polynomials of degrees $n_1, n_2, \ldots, n_r$ in $\mathbb{F}_p[x]$, where $n_1 + n_2 + \cdots + n_r = n$. Then G_f is a subgroup of S_n which contains a permutation permuting the roots with cycles type $(n_1, n_2, \ldots, n_r)$.*

From the theorem, we should know first that $f(x)$ is irreducible over $\mathbb{Q}$. Irreducibility can be read off from the factorizations, since a factorization over $\mathbb{Q}$ can be scaled to be a (monic) factorization over $\mathbb{Z}$. then if we have linear factor in $\mathbb{Z}[x]$, then of course, we have linear factor in $\mathbb{Z}_p[x]$.

It is important to remember that Dedekind's theorem does not correlate any information about the permutations coming from different primes. We don't know the exact roots which permuted by the cycles.

2.5 Computing Galois Group of a Polynomial

Galois groups are not easy to compute. As Galois says in the "Discours Preliminaire" to his first memoir on Galois theory [**?**]:

> If now you give me an equation that you have chosen at will, and about which you want to know if it is or is not solvable by radicals, I cannot do any more than indicate the means for answering your question, without wanting to charge either myself or any other person with doing it. In a word, the calculations are impractical.

Even with the aid of modern computers, it is not easy to compute the Galois group of a polynomial of large degree unless the polynomial has some special structure. We will introduce some ways of computing Galois groups of arbitrary polynomials.

Throughout the method of Dedekind's criterion, one can only determine whether the Galois group of a polynomial with degree n in $\mathbb{Q}[x]$ is to be S_n or A_n or not. For more results on that, one can refer [**?**] etc.

The following Resolvent Method has developed by L. Soicher and J. Mckay etc. can be useful to compute the Galois group of the polynomial. This method was first described by Jordan[**?**] in 1870, and improved by L. Soicher etc.[**?**] who raised the linear resolvent polynomial method to computing the Galois group of a polynomial. We note two immediate consequences. First, f is a separable polynomial, i.e., it has distinct roots. Second, Gal(f) is a transitive group, i.e. for all r_i and r_j there is some $\sigma \in$ Gal(f) which sends r_i to r_j.

To using this method, we should first know some definitions. The **orbit** of a polynomial $p \in R[x_1, \ldots, x_n]$ under S_n is the set of polynomials that p can be sent to by permuting the x_i, and this is denoted by orb(p).

Note that, this definition can be thought of as measuring "how close" a polynomial is to being symmetric. For example, orbp has the smallest situation, i.e. orb$(p) = \{p\}$, then we have p fixes any permutation, hence p is symmetric polynomial.

The most important definition for the method is resolvent polynomial, here comes to our definition:

Definition 2.5.1. *The* ***resolvent polynomial*** *is defined in terms of two polynomials* $f \in \mathbb{Z}[x]$ *and* $p \in \mathbb{Z}[x_1, \ldots, x_n]$ *to be the new univariate polynomial*

$$R_{p,f}(y) := \prod_{p_i \in \text{orb}(p)} (y - p_i(r_1, \ldots, r_n))$$

In particular, a resolvent polynomial $R_{p,f}$, where $p = e_1x_1 + \cdots + e_rx_r \in \mathbb{Z}[x]$ for some $r, 1 \leq r \leq n$,and $e_1, \cdots, e_r$ nonzero integers, is called a **linear resolvent polynomial**.

Since the resolvent is defined with respect to the orbit of p it is symmetric in the r_i, i.e. permuting the r_i will permute the roots of $R_{p,f}$ but does not change $R_{p,f}$ itself. i.e. the coefficients of $R_{p,f}$ are symmetric polynomials of $r_1, \ldots, r_n$, and the by the **fundamental theorem of symmetric polynomials** can be written in terms of the elementary symmetric polynomials in $r_1, \ldots, r_n$. However, the elementary symmetric polynomials in $r_1, \ldots, r_n$ are exactly the coefficients of f, therefore integers. Hence, $R_{p,f} \in \mathbb{Z}[y]$ providing $p \in \mathbb{Z}[x_1, \ldots, x_n]$ and $f \in \mathbb{Z}[x]$.

For larger degree polynomials, it's hard to get the resolvent. However, computer becomes to our useful tool for computing coefficients of $R_{p,f}$ from above property. We can first approximate the roots of f via numerical root-finding methods, form all combinations of the roots as specified by p, and then expand the product from the definition to find approximations of the coefficients of $R_{p,f}$. Since the coefficients are integers, if the approximations are known with sufficient accuracy then the approximations may simply be rounded to the nearest integer.

The action by $\sigma \in \text{Gal}(f)$ on the roots of $R_{p,f}$ actually gives $Gal(R_{p,f})$. More precisely, let $\phi : \text{Gal}(f) \to \text{Gal}(R_{p,f})$ be defined so that $\phi(\sigma)$ is the action by σ on the roots of $R_{p,f}$. Formally, a proposition which can be found in Cohen's book [**?**] is the following:

Proposition 2.5.1. *If the roots of $R_{p,f}$ are distinct then* $\text{Gal}(f) = \phi(\text{Gal}(R_{p,f}))$.

As mentioned before, to use the above theorem we require that $R_{p,f}$ have distinct roots, however it will not always be the case. The **Tschirnhausen transformation** is an algorithm to get rid of this problem. For more information, one can refer to Cohen's book [**?**].

The linear resolvent method (together with recognizing squarefree of the discriminant of the polynomial, i.e. determined the Galois group is a subgroup of A_n or not) can be applied for polynomial up to degree 7 [**?**]. One can find a table from L. Soicher and J. McKay's work [**?**]. In additional, we repose some parts of this table in Appendix **??**, see table **??**.

Chapter 3 Algebraic Number Theory

Algebraic number theory is a major branch of number theory that studies algebraic structures related to algebraic integers. Usually, it studies algebraic properties of the algebraic integers' ring such as factorization, the behaviour of ideals, and field extensions. In this chapter, we will introduce some definitions and useful results in algebraic number theory as well as some preliminaries of analytic number theory based on [**? ? ?**].

3.1 Algebraic Numbers and Number Fields

We first give the necessary background on algebraic numbers, number fields etc. Let $\alpha \in \mathbb{C}$. Then α is called an **algebraic number** if there exists $f(x) \in \mathbb{Z}[x]/0$ such that $f(\alpha) = 0$. The number α is called an **algebraic integer** if, in addition, one can choose f to be monic.(i.e. with leading coefficient equal to 1).

More generally, we can define the integral element of a ring(See [**?**]) through similar definition.

A **number field** is a field containing $\mathbb{Q}$ which, considered as a $\mathbb{Q}$-vector space, is finite dimensional. The number $d = [K : \mathbb{Q}] = \text{dim}_{\mathbb{Q}} K$ is called the degree of the number field K.

The **signature** of a number field is the pair (r_1, r_2) where r_1 is the number of embeddings of K whose image lie in $\mathbb{R}$, and $2r_2$ is the number of non-real complex embeddings, so that $r_1 + 2r_2 = n$. If T is an irreducible polynomial defining the number field K by one of its roots, the signature of K will also be called the signature of T.

The following proposition [**?**] shows that there are only two possibilities for the signature of a Galois extensions.

Lemma 3.1.1. *Let K be a Galois extension of $\mathbb{Q}$ of degree n. Then, either K is totally real $(r_1 = n)$,or K is totally complex $(r_2 = n/2)$ which can occur only if n is even.*

3.2 Discriminants of Elements and Fields

The definition of discriminants of polynomials can be found in the Appendix **??** if need some reviews, now we will introduce the definition of discriminant of elements and fields. Let K be a number field of degree n, σ_i be the n embeddings of K into $\mathbb{C}$, and α_j be the set of n elements of K. Then we have

$$\text{Disc}(\alpha_1, \dots, \alpha_n) = \det(\sigma_i(\alpha_j))^2 = \det(\text{Tr}_{K/\mathbb{Q}}(\alpha_i \alpha_j))$$

In particular,If $K = \mathbb{Q}(\alpha)$, $f(x)$ is the minimal polynomial of α, then

$$\text{Disc}(f) = \text{Disc}(\alpha) = \text{Disc}(1, \dots, \alpha^{n-1})$$

we denote by O_K the ring of algebraic(rational) integers of K. Then we have that the ring O_K is a free $\mathbb{Z}$-module of rank $n = \deg(K)$. Hence we can define the (absolutely) integral basis as follows:

Definition 3.2.1. *A $\mathbb{Z}$-basis of the free module O_K will be called an (absolutely)**integral basis** of K. The discriminant of an integral basis is independent of the choice of that basis, and is called the **discriminant of the field** K and is denoted by $d(K)$.*

Similarly, we can define a **relatively integral basis**: Let A be a commutative integral domain with 1, $K = \text{Frac}(A)$,L/K is an extension with $[L : K] = n$, B is the integral closure of A in L. If B is a free A-module , i.e. $B = A\alpha_1 \oplus \cdots \oplus A\alpha_n$. Then we call $\alpha_1, \ldots, \alpha_n$ the A-basis of B(resp. integral basis of L/K.) Then we have

$$\text{Disc}(L/K) = (\text{Disc}(\alpha_1, \ldots, \alpha_n)),$$

which is the discriminant of L/K.

Then, we will show a important theorem [**?**] regarding the relationship of the discriminant of the minimal polynomial and the discriminant of the field.

Lemma 3.2.1. *Let T be a monic irreducible polynomial of degree n in $\mathbb{Z}[x]$, θ a root of T, and $K = \mathbb{Q}(\theta)$. If $f = [O_K : \mathbb{Z}[\theta]]$, then*

$$\text{Disc}(T) = d(K)f^2.$$

The number f is called the **index** of θ in O_K. A theorem for recognizing the integral basis of a field is important. Moreover, we have general results for relative integral basis [**?**]. The following proposition has combined these two cases.

Proposition 3.2.1. *The algebraic numbers $\alpha_1, \ldots, \alpha_n$ form an integral basis if and only if they are algebraic integers and if* $\text{Disc}(\alpha_1, \ldots, \alpha_n) = d(K)$. *More generally, if L/K has integral basis, then $\beta_1, \ldots, \beta_n \in B$ form an integral basis if and only if* $(\text{Disc}(\beta_1, \cdots, \beta_n)) = \text{Disc}(L/K)$.

The result related the structure of discriminant of a field due to Stickelberger can not be avoid when we talking about discriminant here:

Lemma 3.2.2 (Stickelberger's criterion)**.** *Let K be a number field, then*

$$d(K) \equiv 0 \textit{ or } 1 (\text{mod}\, 4)$$

The determination of an explicit integral basis and of the discriminant of a number field is not an easy problem, and is one of the main tasks of this article. However one case in which the result is trivial:

Corollary 3.2.1. *Let f be a monic irreducible(i.e. minimal) polynomial in $\mathbb{Z}[x]$, θ a root of f, and $K = \mathbb{Q}(\theta)$. Assume that the discriminant of f is squarefree or is equal to $4d$ where d is squarefree and not congruent to 1 modulo 4. Then the discriminant of K is equal to the discriminant of f, and an integral basis of K is given by $1, \theta, \ldots, \theta^{n-1}$.*

Finally, the result to determine the sign of discriminant is useful:

Lemma 3.2.3. *Let K be an algebraic number field, then*

$$d(K) = (-1)^{r_2}|d(K)|$$

3.3 Decomposition of Prime Numbers

For simplicity, we continue to work with a number field K considered as an (finite) extension of $\mathbb{Q}$, and not considered as a relative extension. Many of the results which are explained in that context are still true in the more general case, but some are not. Almost always, these generalizations fail because the ring of integers of the base field is not a PID(Dedekind). The main results concerning the decomposition of primes are as follows:

Proposition 3.3.1. *Let p be a prime number, then there exist positive integers e_i such that*

$$pO_K = \prod_{i=1}^{g} \wp_i^{e_i},$$

where $\wp_i$ are all the prime ideals above p, i.e. $\wp_i \cap \mathbb{Z} = p\mathbb{Z}$.

The integer e_i is called the **ramification index** of p at $\wp_i$ and is denoted $e(\wp_i|p)$. The degree f_i of the field extension defined by

$$f_i = [O_K/\wp_i : \mathbb{Z}/p\mathbb{Z}]$$

is called the **residue degree** of p and is denoted $f(\wp_i|p)$. g is called the **decomposition number** of p in K.

There is an important relation between these coefficients, which comes to a theorem.

Proposition 3.3.2. *Let $[K : \mathbb{Q}] = n$, then for any p, the decomposition in Theorem* **??** *satisfies*

$$\sum_{i=1}^{g} e_i f_i = n.$$

Let $pO_K = \prod_{i=1}^{g} \wp_i^{e_i}$ be the decomposition of a prime p. We will say that p is **inert** if $g = 1$ and $e_i = 1$,i.e. $pO_K = \wp_i$. We will say that p **splits completely** if $g = n$. Finally, we say that p is **ramified** if there is an e_i which is greater than or equal to 2 (in other words if pO_K is not squarefree), otherwise we say that p is **unramified**. Those prime ideals $\wp_i$ such that $e_i > 1$ are called the ramified prime ideals of O_K. In particular, if $e_1 = n$, then we say that p **ramifies totally**.

From the definitions of these ramification index and decomposition number satisfy chain rule, which is a very important message for us to decompose prime number in a compositum of fields.

In the case when $K/\mathbb{Q}$ is a Galois extension, the result is more specific: Assume $K/\mathbb{Q}$ is a Galois extension. Then for any p, the ramification indices e_i are equal, the residual degrees f_i are equal as well, hence $efg = n$. In addition, the Galois group operates **transitively** on the prime ideals above p: i.e. there exists $\sigma \in \text{Gal}(K)$, such that $\sigma(\wp_i) = \wp_j$.

The existence of ramified prime has showed by Minkowski: If K is a number field different from $\mathbb{Q}$, then $|d(K)| > 1$. In particular, there exists at least one ramified prime in K. What's more, the fundamental ramification theorem[**?**] is as follows:

Proposition 3.3.3. *Let p be a prime number, then p is ramified in K if and only if p divides the discriminant $d(K)$. In particular, there are only a finite number of ramified primes (exactly $w(d(K))$, where $w(x)$ is the number of distinct prime divisors of an integer x).*

On the contrary, for unramified prime, we have another theorem given by Stickelberger[**?**].

Proposition 3.3.4 (Stickelbeger). *If p is an unramified prime in K with $pO_K = \prod_{i=1}^{g} \wp_i$, we have*

$$\left(\frac{d(K)}{p}\right) = (-1)^{n-g},$$

for $p = 2$, $\left(\frac{d(K)}{2}\right) = (-1)^{n-g}$ is to be seen as the Jacobi-Kronecker symbol(See Appendix **??***).*

We now consider a more difficult algorithmic problem, that of determining the decomposition of prime numbers in a number field. The basic theorem on the subject, which unfortunately is not completely sufficient(but right for Dedekind domain with power integral basis, even for without essential factor), is as follows.

Proposition 3.3.5 (Kummer). *Let $K = \mathbb{Q}(\theta)$ be a number field, where θ is an algebraic integer, whose minimal polynomial is denoted $T(x)$. Let f be the index of θ, i.e. from definition $f = [O_K : \mathbb{Z}[\theta]]$. Then for any prime p not dividing f on can obtain the prime decomposition of pO_K as follows. Assume*

$$T(x) \equiv \prod_{i=1}^{g} T_i(x)^{e_i} (\operatorname{mod} p)$$

be the decomposition of T into irreducible factors in $\mathbb{F}_p[x]$, where the T_i are also monic. Then

$$pO_K = \prod_{i=1}^{g} \wp_i^{e_i},$$

where

$$\wp_i = (p, T_i(\theta)) = pO_K + T_i(\theta)O_K$$

Furthermore, the residual index f_i is equal to the degree of T_i.

3.4 Units and Ideal Classes

Let K be a number field and O_K be the ring of integers of K. We say that two (fractional) ideals* I and J of K are equivalent if there exists $\alpha \in K^*$ such that $J = \alpha I$. The set of equivalence classes is called the **class group** of O_K and is denoted $Cl(K)$.

Since fractional ideals of O_K form a group it follows that $Cl(K)$ is also a group. The main theorem concerning $Cl(K)$ is that it is finite.

*Fractional ideal I in O_K is a non-zero sub-module of K such that there exists a non-zero integer d with dI ideal of O_K.

For any number field K, the class group $Cl(K)$ is a finite Abelian group, whose cardinality, called the **class number**, is denoted $h(K)$. Note that $h(K) = 1$ if and only if O_K is a PID(UFD).

Denote by $I(K)$ the set of fractional ideals of K, and $P(K)$ the set of principal ideals. We clearly have the exact sequence:

$$1 \to P(K) \to I(K) \to Cl(K) \to 1.$$

The set of units in K form a multiplicative group which we will denote by $U(K)$. Units are algebraic integers of norm equal to ± 1. The torsion subgroup of $U(K)$, i.e. the group of roots of unity in K, will be denoted by $\mu(K)$.

It is clear that we have the exact sequence:

$$1 \to U(K) \to K^{\times} \to P(K) \to 1.$$

To sum up above two sequence, we have new exact sequence as follows:

$$1 \to U(K) \to K^{\times} \to P(K) \to I(K) \to Cl(K) \to 1.$$

The main result concerning units is the following theorem:

Proposition 3.4.1 (Dirichlet's Unit Theorem)**.** *Let (r_1, r_2) be the signature of K, then $U(K)$ is finitely generated Abelian group of rank $r_1 + r_2 - 1$. i.e. we have a group isomorphism:*

$$U(K) \cong \mu(K) \times \mathbb{Z}^{r_1+r_2-1},$$

and $\mu(K)$ is a finite cyclic group.

If we set $r = r_1 + r_2 - 1$, we see that there exist units $u_1, \dots, u_r$ such that every element x of $U(K)$ can be written in a unique way as

$$x = \zeta u_1^{n_1} \cdots u_r^{n_r},$$

where $n_i \in \mathbb{Z}$ and ζ is a root of unity in K.Such a family (u_i) is called a system of **fundamental units** of K.

A very important property is the number is finite, what's more, like we claimed before, the ideal class group for any number field is a finite Abelian group. As for the class number, we can give a certain upper bound of it. First of all, we give the definition of Minkowski bound [**?**]:

Definition 3.4.1. *If K is a number field, the quantity*

$$C_K = \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} \sqrt{|d(K)|}$$

is called the ***Minkowski's bound****, where $d(K)$ is the discriminant of K and $[K : \mathbb{Q}] = n$ with signature $\{r_1, r_2\}$.*

The following lemma [**?**] will give us a useful method to determined the class number and class field for $n = [K : \mathbb{Q}]$ is small.

Lemma 3.4.1. *Any ideal class of a number field K has an (integral) ideal I, such that*

$$\mathrm{N}(I) \leq C_K$$

From this lemma, we can also get the so-called Hermite's theorem on discriminant: There are only finitely many number fields having a given discriminant d.

In fact, we have a following method to determined the class number and class group" Firstly, we should calculated the Minkowski's bound of the number field K. From the lemma, we can find all rational primes that $p \leq C_K$. Given the prime decomposition of pO_K, then we can compute all prime ideals $\wp$ over p. Hence the class group $Cl(K)$ is generated by $A = \{[\wp] | \wp | p \leq C_K\}$, where $[\wp]$ is the ideal class which $\wp$ lies in. If A is not so big, the we can consider the multiple relationship between its elements, then we can get the class group and class number.

3.5 Character and Conductor

A **character** on a group G is a group homomorphism from G to the multiplicative group of a field(usually complex numbers field). The set $\hat{G}$ of these morphisms forms an abelian group under pointwise multiplication. Sometimes we only consider unitary characters, thus the image is in the unit circle.

Now we consider the special character we mentioned above, **Dirichlet character**, which is defined as follows:

Definition 3.5.1. *A Dirichlet character is any function χ from the integers $\mathbb{Z}$ to the complex numbers $\mathbb{C}$ such that χ has the following properties:*

1. *the function is periodic, i.e. $\exists k \in \mathbb{Z}^+$, s.t. $\chi(n) = \chi(n+k), \forall n$.*
2. *If* $\gcd(n,k) > 1$*, then $\chi(n) = 0$; if* $\gcd(n,k) = 1$*, then $\chi(n) \neq 0$*
3. *$\chi(mn) = \chi(m)\chi(n)$ for all integers m, n.*

The Dirichlet character has following properties: from the definition, we can directly get $\chi(1) = 1$, the character is periodic with period k, we say that χ is a character to the **modulus** k. i.e. we have

$$a \equiv b \mod k \Rightarrow \chi(a) = \chi(b)$$

If $\gcd(a,k) = 1$, then from Euler theorem, we have $a^{\phi(k)} \equiv 1 \mod k$, therefore we have $\chi(a^{\phi(k)}) = \chi(1) = 1$, on the other hand, $\chi(a^{\phi(k)}) = \chi(a)^{\phi(k)}$. i.e. for all a relatively prime to k, $\chi(a)$ is a $\phi(k)$-th complex root of unity.

A character χ is said to be **odd** if $\chi(-1) = -1$ and **even** if $\chi(-1) = 1$. A character is called **principal** if it assumes the value 1 for arguments coprime to its modulus and otherwise is 0. A character of the (Abelian) field can be viewed as the character of the Galois group of the field.

For example, the character of a quadratic field K is $\hat{K} = \{1, \chi\}$ (see [**?**] etc.). the character χ is the same to the Legendre-Kronecker symbol (See Appendix **??**).

Then, we will introduce the conductor. Taking as base the field of rational numbers, the Kronecker−Weber theorem **??** states that an algebraic number field K is abelian over $\mathbb{Q}$ if and only if it is a subfield of a cyclotomic field $\mathbb{Q}(\zeta_n)$. The **conductor** of K is then the smallest such n.

we can also define a conductor of character, i.e. the conductor of a character is the smallest modulus of χ, More precisely, the conductor of a Dirichlet character χ modulo k is the smallest positive integer k_0 which divides k and which has the property that $\chi(n+k_0) = \chi(n)$ for all n. For this case, the χ is called the **primitive character of conductor** (or modulus) f_χ.

The relation between the conductor of characters and Abelian number field is that, the conductor f of the field K is the least common multiple of conductor of character for Galois group of the Abelian number field, i.e.

$$f = \mathrm{lcm}_{\chi \in \hat{K}}\{f_\chi\}.$$

For example, for real quadratic field, f is the fundamental discriminant of the field. For cyclic cubic field, f is actually e in Theorem **??**, i.e. the arithmetic square root of the discriminant of the cyclic cubic field.

Let p be an odd prime and $K/\mathbb{Q}$ a cyclic extension of degree p. Then it is well known [**?**] that the conductor of K must have the form $f = p^e \cdot q_1 q_2 \cdot q_n$, where $e = 0$ or 2, $n \geq 0$, and the q_i are pairwise distinct rational primes satisfying $q_i \equiv 1 (\mathrm{mod}\, p)$ for $i = 1, 2, \ldots, n$. The discriminant of K is just a power of the conductor, $d_K = f^{p-1}$.

A theorem called **conductor-discriminant formula** related to the conductor of a field and the discriminant of the field was first found by Dedekind. Then at the beginning of 1930's, E. Artin and H. Hasse found this general formula (See [**?**] etc.) which is showed following:

Proposition 3.5.1. *Let K/F be a finite Galois extension of global fields with Galois group G,*

$$d(K/F) = \prod_{\chi \in \hat{G}} f_\chi^{\chi(1)},$$

since for abelian field, $\chi(1) = 1$, hence for K is an abelian number field, then we have a special form,

$$d(K) = (-1)^{r_2} \prod_{\chi \in \hat{G}} f_\chi$$

Chapter 4 Quadratic Fields

In this chapter, we are going to discover the most simplest number field that are different from $\mathbb{Q}$, i.e. quadratic fields. Let denote it as K. A quadratic field is of degree 2 over $\mathbb{Q}$, it can be given by $K = \theta$, where θ is a root of minimal polynomial $f(x) = x^2 + ax + b$ of $\mathbb{Z}[x]$. Let $d = a^2 - b$, then $K = \mathbb{Q}(\sqrt{d})$. Clearly, d is not a square, otherwise $f(x)$ won't be a irreducible quadratic polynomial. Since $\mathbb{Q}(\sqrt{m^2 d}) = \mathbb{Q}(\sqrt{d})$, hence we may assume that d is squarefree.

Since $n = 2 = r_1 + 2r_2$, the signature of quadratic field K is either $(2, 0)$ or $(0, 1)$, which is called real quadratic field or complex (or imaginary) quadratic field respectively. It's easy to show that the real quadratic field has positive discriminant and the complex quadratic field has negative discriminant.

4.1 Discriminant, Integral Basis

The integral basis and discriminant of quadratic field is easy as following theorem:

Theorem 4.1.1. *Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic field with d squarefree. Then if $d \equiv 1 (\operatorname{mod} 4)$, we have integral basis $(1, (1 + \sqrt{d})/2)$ with discriminant $d(K) = d$; if $d \equiv 2$ or $3 (\operatorname{mod} 4)$, we have integral basis $(1, \sqrt{d})$ with discriminant $d(K) = 4d$.*

Let us denote $D = d(K)$ (namely fundamental discriminant) for these two cases, then we can see that it satisfies Stickelberger's criterion **??**. What's more, $K = \mathbb{Q}(\sqrt{D})$ has integral basis $(1, \omega)$, where

$$\omega = \frac{D + \sqrt{D}}{2},$$

and therefore $O_K = \mathbb{Z}[\omega]$.

4.2 Decomposition of Primes

Note that Proposition **??** and Proposition **??** immediately shows how prime numbers decompose in a quadratic field [**?**].

Theorem 4.2.1. *Let $K = \mathbb{Q}(\sqrt{D})$, where D is the fundamental discriminant, i.e. $D = d(K)$, $O_K = \mathbb{Z}[\omega]$ where $\omega = (D + \sqrt{D})/2$ its ring of integers, and p be a prime number. Then**

1. *If $\left(\frac{D}{p}\right) = 0$, then p is ramified, i.e. $pO_K = \wp^2$. More precisely,*

$$\wp = pO_K + \omega O_K,$$

except when $p = 2$ and $D \equiv 12 (\operatorname{mod} 16)$.

* $\left(\frac{D}{p}\right)$ is Kronecker symbol which can be seen in Appendix **??**.

2. *If* $\left(\frac{D}{p}\right) = -1$, *then* p *is inert, hence* $pO_K = \wp$ *is a prime ideal.*

3. *If* $\left(\frac{D}{p}\right) = 1$, *then* p *is split, and we have* $pO_K = \wp_1\wp_2$, *where*

$$\wp_i = pO_K + (\omega - \frac{D \pm b}{2})O_K,$$

and b *is any solution to* $b^2 \equiv D(\text{mod}\, 4p)$

4.3 Unit Group of Imaginary Quadratic Fields

First we consider the unit group of quadratic field, by the Dirichlet's Unit theorem **??**, we can divide the quadratic field into two cases. The imaginary quadratic field has simple unit group since $r = r_1 + r_2 - 1 = 0$, i.e. the unit group is finite. In fact, the imaginary quadratic field is the only number field apart from $\mathbb{Q}$ who has finite units. A theorem for the unit group of Imaginary Quadratic fields could be found in [**? ?**] etc.:

Theorem 4.3.1. *Let* $K = \sqrt{D}$, *where the fundamental discriminant* $D < 0$, *then the group* $U(K) = \mu(K)$ *of units is equal to the group of* $\omega(D) - th$ *roots of unity, where*

$$\omega(D) = \begin{cases} 2, & \textit{if}\, D < -4 \\ 4, & \textit{if}\, D = -4 \\ 6, & \textit{if}\, D = -3 \end{cases}$$

4.4 Class number of Imaginary Quadratic Fields

Let us now consider the problem of computing the class number of imaginary quadratic field. Here we give a beautiful result from L-function. Since it's to far to enter into the details of the analytic theory of **L-functions**, so we just recall the results. Our main result is a corollary of Dirichlet's Theorem (We have reorganized this theorem to fit all imaginary quadratic number field. In the original theorem, it just states $D < -4$ cases.) [**?**].

Theorem 4.4.1. *If* D *is a negative fundamental discriminant, then*

$$h(K) = \frac{\omega(D)}{4 - 2\left(\frac{D}{2}\right)} \sum_{1 \leq r < |D|/2} \left(\frac{D}{r}\right),$$

where $\omega(D)$ *is defined in Theorem* **??**.

Remark 4.4.1. *For* $D < -4$, *we have*

$$h(K) = \frac{1}{2 - \left(\frac{D}{2}\right)} \sum_{1 \leq r < |D|/2} \left(\frac{D}{r}\right).$$

Of course, we can get $h(-3) = h(-4) = 1$ *by calculation.*

More precise list for class number can be seen in the book [**?**].

4.5 Unit group of Real Quadratic Fields

For real quadratic fields, ZHANG [**?**] has given a precise algorithm to compute it through the Pell's equation. Since the unit circle of a real quadratic field only hits two time real axis, then we have $\mu K = \{\pm 1\}$. By Dirichlet Unit Theorem **??**, we have

$$U(K) = \{\pm 1\} \times \epsilon^{\mathbb{Z}},$$

where ϵ generates an infinite cyclic group $\langle \epsilon \rangle = \epsilon^{\mathbb{Z}}$. There exists only one unit in the set (all of them can generate whole infinite cyclic group) $\{\pm\epsilon, \pm\epsilon^{-1}\}$ which is larger than 1, and we denote it as fundamental unit of K. Now we just need to compute the fundamental unit. Let $K = \mathbb{Q}(\sqrt{d})$, where d is squarefree. Let $\alpha = a + b\sqrt{d}(a, b \in \mathbb{Q})$ be unit of K, then $N(\alpha) = \pm 1$. If $d \equiv 2$ or $3 \mod 4$, then $O_K = \mathbb{Z}[\sqrt{d}]$. A integer $\alpha = x + y\sqrt{d}(x, y \in \mathbb{Z})$ is unit if and only if $N(\alpha) = \pm 1$, i.e. we have following Pell's equation:

$$x^2 - dy^2 = \pm 1 \tag{4.1}$$

From the Unit Theorem, we note that if $\epsilon = a_1 + b_1\sqrt{d}$ is a fundamental unit of $K(a_1, b_1 > 0)$, then

$$\epsilon^n = (a_1 + b_1\sqrt{d})^n = a_n + b_n\sqrt{d}$$

is also a unit who larger than one. What's more, (a_n, b_n) are natural number solutions of the Pell's equation **??**. Note that $b_{n+1} = a_1 b_n + a_n b_1$, hence b_n is an increasing sequence.

Let us consider $b = 1, 2, 3, \cdots$, if $db^2 \pm 1$ is a square number (i.e. a^2), then we stop the process, i.e. we find the "smallest" solution of the Pell's equation **??** and this solution is also the fundamental unit.

Let's consider $d = 6$, $6b^2 \pm 1$ is a square number firstly when $b = 2$, i.e. we have the fundamental unit of $\mathbb{Q}(\sqrt{6})$ is $\epsilon = 5 + 2\sqrt{6}$.

Similarly, if $d \equiv 1 \mod 4$, then $O_K = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$, an integer of K has form $\alpha = (a + b\sqrt{d})/2$, where $a \equiv b \mod 2$, $a, b \in \mathbb{Z}$. α be unit of K if and only if $N(\alpha) = (a^2 - b^2 d)/4 = \pm 1$, hence, (a, b) is a solution of the following Pell's equation:

$$x^2 - dy^2 = \pm 4 \tag{4.2}$$

if $\epsilon = (a_1 + b_1\sqrt{d})/2$ is a fundamental unit of $K(a_1, b_1 > 0)$, then

$$\epsilon^n = (\frac{a_1 + b_1\sqrt{d}}{2})^n = \frac{a_n + b_n\sqrt{d}}{2}$$

is also a unit who larger than one. Similarly, consider $b = 1, 2, 3, \cdots$, if $db^2 \pm 4$ is a square number (i.e. a^2), then we stop the process and get the fundamental unit $(a + b\sqrt{d})/2$.

4.6 Class Numbers of Real Quadratic Fields

Also, as in the imaginary case, using L-function, we can also get a beautiful results[**?**]. We have modified the results through discarding regulators.

Theorem 4.6.1. *If D is a positive fundamental discriminant, then*

$$h(K) = -\frac{1}{\ln(\epsilon)} \sum_{r=1}^{\lfloor (D-1)/2 \rfloor} \left(\frac{D}{r}\right) \ln \sin\left(\frac{r\pi}{D}\right).$$

Now we see an example, let $D = 4d = 8$, then $\epsilon = 1 + \sqrt{2}$ by the result of unit group of real quadratic field. From the Theorem **??**, we have

$$h(K) = -\frac{1}{\ln(1+\sqrt{2})}\left(\ln\sin(\frac{\pi}{8}) - \ln\sin(\frac{3\pi}{8})\right) = -\frac{\ln(\tan(\frac{\pi}{8}))}{\ln(1+\sqrt{2})} = 1.$$

Chapter 5 Cyclic Cubic Fields

In this chapter, we start with a cubic polynomial with Galois group $A_3 = C_3$. A famous work with only half page given by Seidelmann in 1917 [**?**] showed the condition of the polynomial which satisfies the Galois group C_3. We have recovered the process to get this condition with a lemma which can be found in Cohen's book. Then we proceed to rearrange the explicit results for cyclic cubic field based on Cohen's book. At last, we will propose some examples on prime decomposition and computing class number.

In additional, we have offered some special examples in the last section **??** for cyclic cubic field without the standard form which we will show as follows. What's more, we also give a formula (See theorem **??**) for a type of cyclic cubic field which is given risen by the ideas of F.C. Orvay's [**?**].

Firstly, we propose some preliminaries of cyclyc cubic field K. Let K be a number field of degree 3 over $\mathbb{Q}$, i.e. a cubic field. If K is Galois over Q, with Gal$(K) = A_3$, then K is so called a cyclic cubic field. let denote the Galois group of K be $\langle\sigma\rangle$, where $\sigma^{-1} = \sigma^2$. Note that, for cyclic cubic field K can only be totally real, based on the Lemma **??**.

5.1 Cubic Polynomial and Cyclic Cubic Field

The cyclic cubic fields can be viewed as generating by cubic polynomials. let's consider a polynomial of degree 3 which has the form

$$f(x) = ax^3 + bx^2 + cx + d$$

where $a \neq 0$. There are two possible Galois groups for splitting field of cubic polynomial, namely S_3 and $A_3 = C_3$.

Now we will reduce the general cubic equation into a cubic trinomial by eliminating the quadratic term. We begin with the general cubic with rational coefficients

$$ax^3 + bx^2 + cx + d$$

and make the substitution $x = X - \frac{b}{3a}$ to get

$$aX^3 + \left(c - \frac{b^2}{3a}\right) X - \frac{bc}{3a} + d + \frac{2b^3}{27a^2}$$

Since each of these coefficients are rational, we have now have a cubic trinomial in $\mathbb{Q}$. Also, since we are working over the rational numbers, we can easily divide by the leading coefficient of the x^3 term and obtain a monic cubic equation.

The main distinction of cubics with a Galois group of C_3 is that the polynomial discriminant is equal to a square in $\mathbb{Q}$ which is a direct corollary of Theorem **??**. Seidelmann uses this fact to give a form for the coefficients of a monic cubic trinomial with a Galois group of C_3. For $p, q \in \mathbb{Q}$, the equation

$$f(x) = x^3 - 3(p^2 + 3q^2)x + 2p(p^2 + 3q^2)$$

where $f(x)$ is not reducible, represents all equations of degree 3 with a Galois group of C_3.

In Seidelmann's paper (German version), there are only few rows to show the result but without proof, so now we give a brief proof of it. We assume that K is a cyclic cubic field. Let θ be an algebraic integer such that $K = \mathbb{Q}(\theta)$, and let $f(x) = x^3 + ax + b$ be the minimal polynomial of θ as we mentioned before.

One important consequence is necessary for calculation. Since any cyclic cubic field has at least one real embedding and since K is Galois, all the roots of f must be real(See Lemma **??**). Of course, we can get this from the square discriminant of f.

Consider the primitive cube roots of unity $\zeta = e^{2\pi i/3}$, then it's easy to see that $K(\zeta)$ is a sextic field over $\mathbb{Q}$. What's more, it's also Galois with Galois group $\langle \sigma, \tau \rangle$, where σ has been defined above which fixes ζ, τ is the complex conjugation. We first prove the following lemma, one could find a similar lemma in Cohen's book [**?**].

Lemma 5.1.1. *Set $\gamma = \theta + \zeta^2\sigma(\theta) + \zeta\sigma^2(\theta) \in K(\zeta)$, and $\beta = \gamma^2/\tau(\gamma)$. Then $\beta \in \mathbb{Q}(\zeta)$ and we have*

$$f(x) = x^3 - \frac{e}{3}x - \frac{eu}{27},$$

where $e = \beta\tau(\beta)$ and $u = \beta + \tau(\beta)$.

Proof. We have $\tau(\gamma) = \theta + \zeta\sigma(\theta) + \zeta^2\sigma^2(\theta)$, also we can verify that

$$\sigma(\gamma) = \sigma(\theta) + \zeta^2\sigma^2(\theta) + \zeta\theta = \zeta\gamma$$

and

$$\sigma(\tau(\gamma)) = \sigma(\theta) + \zeta\sigma^2(\theta) + \zeta^2\theta = \zeta^2\tau(\gamma).$$

Hence, we have

$$\sigma(\beta) = \sigma(\gamma^2/\tau(\gamma)) = \gamma^2/\tau(\gamma) = \beta,$$

i.e. β is invariant under the action of σ, so by the Galois theory $\beta \in \mathbb{Q}(\zeta)$.

Note that e and u are norm and trace of β in $\mathbb{Q}(\zeta)$ respectively, hence is rational numbers.

Now we have the following matrix equation:

$$\begin{pmatrix} 0 \\ \gamma \\ \tau(\gamma) \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ 1 & \zeta^2 & \zeta \\ 1 & \zeta & \zeta^2 \end{pmatrix} \begin{pmatrix} \theta \\ \sigma(\theta) \\ \sigma^2(\theta) \end{pmatrix}$$

Then, we have

$$\begin{pmatrix} \theta \\ \sigma(\theta) \\ \sigma^2(\theta) \end{pmatrix} = \frac{1}{3} \begin{pmatrix} 1 & 1 & 1 \\ 1 & \zeta & \zeta^2 \\ 1 & \zeta^2 & \zeta \end{pmatrix} \begin{pmatrix} 0 \\ \gamma \\ \tau(\gamma) \end{pmatrix}$$

From the formula, we have

$$a = \theta\sigma(\theta) + \theta\sigma^2(\theta) + \sigma(\theta)\sigma^2(\theta) = -\frac{\gamma\tau(\gamma)}{3}$$

and

$$b = -\theta\sigma(\theta)\sigma^2(\theta) = -\frac{\gamma^3 + (\tau(\gamma))^3}{27}.$$

Note that $\tau(\beta) = \tau(\gamma^2/\tau(\gamma)) = \tau(\gamma^2)/\gamma = (\tau(\gamma))^2/\gamma$. We can easily verify that the norm and trace of β coincide e and u. □

Now since $\mathbb{Q}(\zeta) = \mathbb{Q}(\sqrt{-3})$, we can assume that $\beta = p + q\sqrt{-3} \in \mathbb{Q}(\zeta)$, where $p, q \in \mathbb{Q}$ then $e = \mathrm{N}(\beta) = (p + q\sqrt{-3})(p - q\sqrt{-3}) = p^2 + 3q^2$, $u = \mathrm{Tr}(\beta) = 2p$, hence we have

$$f(x) = x^3 - \frac{p^2 + 3q^2}{3}x - \frac{2p(p^2 + 3q^2)}{27},$$

which is equivalent to $f(x) = x^3 - 3(p^2 + 3q^2)x - 2p(p^2 + 3q^2) = x^3 - 3ex - eu$ up to scaling. (The sign of the constant term's coefficient can be change by replace p into $-p$.)

5.2 Discriminant and Integral Basis

Now, for simplicity, up to suitable scaling, we use $f(x) = x^3 - 3ex - eu$, where wlog, we assume that e, u are rational integer. Note that then β can be written down an algebraic integer of $\mathbb{Q}(\zeta)$,i.e. we have $\beta = \frac{u+v\sqrt{-3}}{2}$, $u, v \in \mathbb{Z}$. What's more, u cannot be divisible by 3 since β is not divisible by the ramified prime. Hence, by suitable choosing β or $-\beta$, we may assume that $u \equiv 2 (\mathrm{mod}\, 3)$. In this notation, $e = \frac{u^2+3v^2}{4}$, then $e \equiv 1 (\mathrm{mod}\, 3)$. In fact, e is the product of distinct primes which congruent to 1 modulo 3 (including $e = 1$) [**?**]. i.e. we have following lemma:

Lemma 5.2.1. *For any cyclic cubic field K, there exists a unique pair of integer e, u such that e is equal to a product of distinct primes congruent to 1 modulo 3, $u \equiv 2 (\mathrm{mod}\, 3)$, $v > 0$ and such that $K = \mathbb{Q}(\theta)$, where θ is a root of the polynomial*

$$f(x) = x^3 - 3ex - eu.$$

Moreover, the conjugates of θ are given by following formulas:

$$\sigma(\theta) = \frac{-2e}{v} - \frac{u+v}{2v}\theta + \frac{\theta^2}{v}, \tag{5.1}$$

$$\sigma^2(\theta) = \frac{2e}{v} + \frac{u-v}{2v}\theta - \frac{\theta^2}{v} \tag{5.2}$$

Proof. For simplicity, we just give the proof of the conjugates. Firstly, since the discriminant of $x^3 + ax + b$ is equal to $-(4a^3 + 27b^2)$ (Also can refer the Appendix **??**), hence the discriminant of f is equal to

$$-(4(-3e)^3 + 27e^2u^2) = -27e^2(u^2 - 4e) = 81e^2v^2.$$

Then from the definition of Polynomial we have $d = (\theta - \sigma(\theta))(\sigma(\theta) - \sigma^2(\theta))(\sigma^2(\theta) - \theta) = \pm 9ev$. If necessary, by exchanging the $\sigma(\theta), \sigma^2(\theta)$, we may assume that

$$\sigma(\theta) - \sigma^2(\theta) = \frac{9ev}{(\theta - \sigma(\theta))(\theta - \sigma^2(\theta))} = \frac{9ev}{f'(\theta)} = 9ev/(3\theta^2 - 3e).$$

Now we should simplify this equation. Since $f(\theta) = \theta^3 - 3e\theta - eu = 0$, hence we can use the extended Euclidean algorithm with $A(x) = x^3 - 3ex - eu$ and $B(x) = x^2 - e$, then we got the inverse of B modulo A is equal to $(2x^2 - ux - 4e)/(3v^2 e)$ (note that gcd$(A, B) = 1$ for there is no multiple roots in $f(x)$.), hence

$$\sigma(\theta) - \sigma^2(\theta) = \frac{2\theta^2 - u\theta - 4e}{v}$$

On the other hand, since the trace of θ is equal to 0, so we have $\sigma(\theta) + \sigma^2(\theta) = -\theta$, we can get the final result of $\sigma(\theta)$ and $\sigma^2(\theta)$ from above equations. □

The following theorem[**?**] shows the integral basis and discriminant of cyclic cubic field:

Theorem 5.2.1. *Let $K = \mathbb{Q}(\theta)$ be a cyclic cubic field where θ is a root of $x^3 - 3ex - eu = 0$ and where, as above, $e = \frac{u^3+3v^2}{4}$ is equal to a product of distinct primes (namely t distinct primes) congruent to 1 modulo 3, $u \equiv 2 (\mathrm{mod}\, 3)$, then*

1. *Assume that $3 \nmid v$, i.e. 3 is ramified in K. Then $(1, \theta, \sigma(\theta))$*[*] *is an integral basis of K and the discriminant of K is equal to $(9e)^2$. What's more, there exists up to isomorphism exactly 2^t cyclic cubic fields of discriminant $(9e)^2$ defined by the polynomial.*
2. *Assume that $3 \mid v$, i.e. 3 is unramified in K. Then let $\theta' = (\theta + 1)/3$, $(1, \theta', \sigma(\theta'))$ is an integral basis of K and the discriminant of K is equal to e^2. What's more, there exists up to isomorphism exactly 2^{t-1} cyclic cubic fields of discriminant e^2 defined by the polynomial.*

For the first case, not that $\theta^2 = v\sigma(\theta) + ((u + v)/2)\theta + 2e$ from the result of $\sigma(\theta)$, so the $\mathbb{Z}$-module O_K generated by $(1, \theta, \sigma(\theta))$ contains $\mathbb{Z}[\theta]$. So the index $[O_K : \mathbb{Z}[\theta]] = v$. For the second case, ie, if the prime 3 is unramified in K, then we can write the minimal polynomial of θ', i.e. θ' is a root of the equation with coefficients in $\mathbb{Z}$

$$f(x) = x^3 - x^2 + \frac{1 - e}{3}x - \frac{1 - 3e + eu}{27}, \tag{5.3}$$

where $e = \frac{u^2+27v'^2}{4}, u \equiv 2 (\mathrm{mod}\, 3), u \equiv v' (\mathrm{mod}\, 2), v' > 0$, and e is the product of distinct primes congruent to 1 modulo 3. For the same reason, we have $[O_K : \mathbb{Z}[\theta']] = v/3 = v'$.

With new notation on e, u, v, Cohen's book[**?**] given us another theorem as follows:

Theorem 5.2.2. *All cyclic cubic fields K are given exactly once (up to isomorphism) in the following way:*

[*] σ is given by lemma **??**.

1. *If the prime 3 is ramified in K, then $K = \mathbb{Q}(\theta)$ where θ is a root of the equation with coefficients in $\mathbb{Z}$*
$$f(x) = x^3 - \frac{e}{3}x - \frac{eu}{27}, \tag{5.4}$$
where $e = \frac{u^2+27v^2}{4}, u \equiv 6(\bmod 9), 3 \nmid v, u \equiv v(\bmod 2), v > 0$, and $e/9$ is the product of distinct primes congruent to 1 modulo 3 (could be 1).

2. *If the prime 3 is unramified in K, then $K = \mathbb{Q}(\theta)$ where θ is a root of the equation with coefficients in $\mathbb{Z}$*
$$f(x) = x^3 - x^2 + \frac{1-e}{3}x - \frac{1-3e+eu}{27}, \tag{5.5}$$
where $e = \frac{u^2+27v^2}{4}, u \equiv 2(\bmod 3), u \equiv v(\bmod 2), v > 0$, and e is the product of distinct primes congruent to 1 modulo 3.

3. *In both cases, the discriminant of f is equal to e^2v^2 and the discriminant of number field K is equal to e^2.*

4. *Conversely, if e is equal to 9 times the product of $t-1$ distinct primes congruent to 1 modulo 3, (resp. is equal to the product of t distinct primes congruent to 1 modulo 3), then there exists up to isomorphism exactly 2^{t-1} cyclic cubic fields of discriminant e^2 defined by the polynomials $f(x)$ given in (1) (resp. (2)).*

For this case, the integral basis is showed as follows.

Theorem 5.2.3. *With the notation in Theorem **??**, the conjugates of θ are given by the formulas:*

1. *If 3 is ramified in K,(i.e. in case (1)) then*
$$\sigma^{\pm 1}(\theta) = \mp\frac{2e}{9v} + \frac{-3v \mp u}{6v}\theta \pm \frac{\theta^2}{v};$$

2. *If 3 is unramified in K,(i.e. in case (2)) then*
$$\sigma^{\pm 1}(\theta) = \frac{9v \pm (u+2-4e)}{18v} + \frac{-3v \mp (u+4)}{6v}\theta \pm \frac{\theta^2}{v}$$

In all cases, $(1, \theta, \sigma(\theta))$ is an integral basis of K.

5.3 Prime Decomposition

Without loss of generality, we use the symbol in theorem **??** for simplicity. The situation of the decomposition of prime number in cyclic cubic field is quite easy, from the transitivity properties of Galois group, there are only three cases for decomposition, inert, totally ramified, splits completely.

From the fundamental theorem of ramification, i.e. theorem **??**, it follows that if $p|e$, i.e. p is one of the prime number (including 3) lies in e's factorization expression, then p is totally ramified. If $p \nmid e$, then p is unramified, even from theorem **??**, we can not determine the inert or splits completely. However if $p \nmid v$, then we can use the theorem **??** to determine the prime decomposition. In fact, the result is similar to quadratic field but change the Kronecker symbol to a cubic residue symbol, i.e. consider the congruence $x^3 \equiv e (\operatorname{mod} p)$ is solvable or not.(or equivalently $p^{(e-1)/3} \equiv 1(\operatorname{mod} p)$).

If $p \mid v$, then f has at least a double root modulo p. If f has a double root, but not a triple root, then f also has a simple root which corresponds to a prime ideal of degree 1. In this case pO_K is the product of three ideals of degree 1, i.e. splits completely. Finally, if f has a triple root modulo p, we must apply other techniques, see Cohen's book 6.2.5 [**?**].

5.4 Units and Class Number

From Dirichlet Unit Theorem, since K is a real field, hence $\mu(K) = \{\pm 1\}$ and we have $U(K) = \{\pm 1\} \times \mathbb{Z}^2$. A unit τ of K is called the fundamental unit of K if and only if $\{-1, \tau, \sigma(\tau)\}$ generate the group of units of K. From the property of units, we have $\mathrm{N}(\tau) = \pm 1$. The only fundamental units are $\pm\tau^{\pm 1}, \pm(\sigma(\tau))^{\pm 1}, \pm(\sigma^2(\tau))^{\pm 1}$. The fundamental unit τ is uniquely determined except for taking conjugates and inverses.

This fundamental system of units can be calculated by means of generalized continued fraction algorithms by Voronoi [**?**], which have been interpreted geometrically by Delone and Faddeev [**?**].

Harvey Cohn and Saul Gorn first give the units of 45 cyclic cubic fields of discriminants, where e is the prime congruent to 1 modulo 3 between 7 to 499.

Then, a table of class numbers and units in cyclic cubic fields with $e < 4000$* has been given by Marie-Nicole Gras [**?**], after that Veikko Ennola and Reino Turunen [**?**] have constructed an extended table for $e < 16000$.

5.5 Conductor of Cyclic Cubic Field

From the definition of conductor and some results in chapter **??**, we can get the conductor of a cyclic cubic field f_3 is of the form [**?**]

$$f_3 = \begin{cases} q_0 q_1 \cdots q_n & if 3 \nmid f_3 \\ 9 q_1 \cdots q_n & if 3 \mid f_3 \end{cases}$$

where q_i are pairwise distinct rational primes satisfying $q_i \equiv 1 (\operatorname{mod} 3)$ for $i = 1, 2, \ldots, n$. And the discriminant of K_3 is $d_3 = f_3^2$.

*this e is the same to the one in Theorem **??**

5.6 Examples

In this section, we would propose some examples on prime decomposition and computing class number.

5.6.1 An Example for Prime Decomposition

Example 5.6.1. *Consider $K = \mathbb{Q}(\theta)$, where θ is a root of $f(x) = x^3 - 93x - 124$, it's easy to compute the discriminant of it is $e^2 = 31^2 = 961$, and $v = 2$. Hence, we have $p = 31$ is ramified totally in O_K, while the other special prime is $p = 2$, since $2 \mid v$. Consider $f(x) \equiv x(1+x)^2 \mod 2$, hence $p = 2$ is splits completely in O_K. Other prime numbers can be determined by the Kummer's theorem* **??**. *Note that for $p = 2$, this decomposition in $\mathbb{F}_2$ has no meaning in Dedekind's criterion* **??**.

5.6.2 Some Examples for computing class group

First of all, we consider the class group of the the number field $K = \theta$, where θ is a root of $f(x) = x^3 - 3x + 1$, since the discriminant of the polynomial is $81 = 9^2$, hence K is a cyclic cubic field. From Theorem **??**, we get the integral basis of the field is $(1, \theta, \sigma(\theta)) = (1, \theta, \theta^2 - 2) = (1, \theta, \theta^2)$, i.e. it has a power integral basis, $O_K = \mathbb{Z}[\theta]$. The discriminant of the field is $d(K) = (9)^2 = 81$, then from the definition of Minkowski's bound, we have $C_K = \frac{2}{9}|81|^{1/2} = 2$, hence $Cl(K) = \langle [\wp] | \wp | 2 \rangle$. Now we consider the decomposition of 2, for $p = 2$, $f(x) \equiv x^3 + x + 1 (\mathrm{mod}\, 2)$ is an irreducible polynomial, i.e. 2 is inert in K. Hence $Cl(K) = \{1\}$, and $h(K) = 1$.

Then we see another example, the number field $K = \mathbb{Q}(\theta)$ with θ is a root of $f(x) = x^3 - x^2 - 4x - 1$. This is a standard form of cyclic cubic field with the secdond case of Theorem **??**, we yield that $e = 13, u = 5, v = 1$ for this case. Hence, the discriminant of the field is $13^2 = 169$, with $v = [O_K : \mathbb{Z}[\theta]] = 1$, hence for any case, we can use theorem **??**, since K is monogenic with integral basis $(1, \theta, \theta^2)$. From the definition of Minkowski's bound, we have $C_K = \frac{2}{9}|169|^{1/2} = 2.889 < 3$, hence just consider $p = 2$. Since $f(x) \equiv x^3 + x^2 + 1 (\mathrm{mod}\, 2)$ is irreducible, i.e. we have 2 is inert in K. Hence $Cl(K) = \{1\}$, and $h(K) = 1$.

5.7 Some Special Cyclic Cubic Fields

In this section, we'd like to share some cyclic cubic fields which have been researched by some mathematicians.

5.7.1 Cubic Trinomials

First, we would like to introduce F.C. Orvay's work [**?**]. Some important results for the structure of cyclic cubic fields with cubic trinomials are listed as followings. For the sake of brevity, we just write down these lemma without proofs. These results can be found in F.C. Orvay's article.

Lemma 5.7.1. *Let* $K = \mathbb{Q}(\theta)$*,* $\mathrm{Irr}(\theta, \mathbb{Q}) = x^3 - px + p$ **,* $p = 3^\delta p_1 \cdots p_r, p_i \equiv 1(\bmod 3)$ *(distinct),* $\delta \in \{0, 2\}$*,* $4p - 27 \in \mathbb{Z}^2$*, then the following hold:*

1. $d(K) = p^2$*,* K *is monogenic*† *with integral basis* $\{1, \sigma, \sigma^2\}$*.*

2. $\{\sigma, \sigma'\}$ *is a system of fundamental units of* K*, where* $\sigma = (m + \theta_1)/3$*,* σ' *denote the conjugate of* σ*,* $\theta_1 = (4p - 9\theta - 6\theta^2)/\sqrt{4p - 27}$ *and* $m = (\sqrt{4p - 27} - 3)/2$*.*

This lemma is suitable for $p = 9, 13, 19, 37, 63, 79, 97, 117, 139, 163, \cdots$.

Lemma 5.7.2. *Let* $K = \mathbb{Q}(\theta)$*,* $\mathrm{Irr}(\theta, \mathbb{Q}) = x^3 - px + pq, p = p_1 \cdots p_r, p_i \equiv 1(\bmod 3)$ *(distinct),*$q > 2$*,* $4p - 27q^2 = 1$*, then the following hold:*

1. $d(K) = p^2$*,* K *is monogenic with integral basis* $\{1, \theta, \theta^2\}$*.*

2. $\{\mu, \mu'\}$ *is a system of fundamental units of* K*, where* $\mu = 2 + 3\sigma + 3\tau$*,* $\sigma = (-1 + \theta_1)/3$*,*$\tau = (\sigma^2 + ((q + 1)/2)\sigma)/q$*,* $\theta_1 = 4p - 9q\theta - 6\theta^2$ *and* $\mu' = -1 - 6\sigma + 3\tau$*.*

3. $\mathrm{Irr}(\mu, \mathbb{Q}) = x^3 - 3((1 + 9q)/2)x^2 + ((27q - 3)/2)x + 1$*.*

4. $\{1, \sigma, \tau\}$ *is another integral basis.*

This lemma is suitable for $p = 61, 331, 547, 817, 1141, \cdots$.

For the first lemma, on choosing p more precisely , we have found a results as follows:

Theorem 5.7.1. *For any integer k, set* $p = k^2 + k + 7$*. The polynomial* $X^3 - pX + p$ *is irreducible over Q and has Galois group* A_3*.*

Proof. For any odd number p, $x^3 - px + p \equiv x^3 + x + 1(\bmod 2)$, hence $x^3 - px + p$ is irreducible over $\mathbb{Q}$. Its discriminant is $(-4)(-p)^3 - 27p^2 = p^2(4p - 27)$. To have a Galois group A_3, we need $4p - 27 \in \mathbb{Z}^2$. Writing $c^2 = 4p - 27$, then we have $p = \frac{1}{4}(c^2 + 27)$. To make it integral we need c odd, and write $c = 2k + 1$, then

$$p = \frac{1}{4}(4k^2 + 4k + 28) = k^2 + k + 7.$$

For any $k, k^2 + k + 7$ is odd so if we defined this expression to be p, then $x^3 - px + p$ has Galois group A_3 over $\mathbb{Q}$. □

*Note that this is not the standard form of cyclic cubic field, however, it is isomorphisic to $f(x) = x^3 - 3px - (4p - 27)p$.

†with power integral basis

5.7.2 Simplest Cubic Fields

There is another special class of cyclic cubic fields called the simplest cubic fields first studied by Daniel Shanks [**?**], Shanks computed the discriminant of the polynomial, fundamental units of the field, the regulator and some class number. A recent job for this type of cyclic cubic fields can be find in Lang's article [**?**].

The simplest cubic field is defined by the following polynomial,

$$f(x) = x^3 - ax^2 - (a+3)x - 1, \tag{5.6}$$

where $a \in \mathbb{Z}$. One can calculate the discriminant from the formula of the discriminant of polynomials (Refer to **??**), then $\mathrm{Disc}(f) = (a^2 + 3a + 9)^2$.

D. Shanks only focuses on that $e := a^2 + 3a + 9$ is a prime, then from theorem **??**, there is only one cyclic cubic satisfies this polynomial equation up to isomorphism, and e is also discriminant of the field.

What's more, one can verify that if θ is a root of equation **??**, then $\theta' = 1/(\theta + 1)$ and $\theta'' = 1/(\theta' + 1)$ are also a root of the equation **??**. And since $\theta(\theta^2 - a\theta - a - 3) = 1$, i.e. θ is a unit, so is θ', then $1 + \theta = -1/\theta'$ is also a unit. In fact, $(\theta, 1 + \theta)$ are independent fundamental units, which can be verified by Godwin's criterion [**?**]. More generally, we have following theorem which could be found in Lang's article [**?**].

Theorem 5.7.2. *If $e := a^2 + 3a + 9$ is square-free, then $(1, \theta, \theta^2)$ is an integral basis of K, and $(-1, \theta, \theta')$ generates the full group of units O_K.*

A simple result about decomposing prime is that 2 is inert in K, since $O_K = \mathbb{Z}[\theta]$ and $\bar{f}(x) \equiv x^3 + x^2 + 1 (\mathrm{mod}\, 2)$ when m is odd, while $\bar{f}(x) \equiv x^3 + x + 1 (\mathrm{mod}\, 2)$ when m is even.

The explicit solution (a positive root) of equation **??** is

$$\theta = \frac{1}{2}(2\sqrt{e}\cos\phi + a),$$

where

$$\phi = \frac{1}{3}\arctan\frac{\sqrt{27}}{2a+3}$$

As for the class number of them, D. Shanks [**?**] finally give a formula to compute them:

$$h = \frac{a^2 + 3a + 9}{4\log^2 a}\left[1 - \frac{3}{a\log a} + o(\frac{1}{a^2})\right]\prod_{p=2}^{\infty} f(p). \tag{5.7}$$

where $f(p)$ is defined by

$$f(p) = \begin{cases} 1 & \text{for } p = e, \\ \left(\frac{q}{q-1}\right)^2 & \text{for } p^{(e-1)/3} \equiv 1 (\mathrm{mod}\, p), \\ \frac{q^2}{q^2+q+1} & \text{otherwise}. \end{cases} \tag{5.8}$$

Shanks give a table of class number for $-1 \le a \le 410$, where e is a prime.

Chapter 6 Cyclic Sextic Fields

In this chapter, we will study cyclic sextic number fields. First of all, the result of discriminant of a cyclic sextic field could be found in Mäki's book [**?**], while we would recover the result using the conductor-discriminant formula **??**. Then, from a necessary theorem given by Mäki, together with the result of discriminant, we give the integral basis of a cyclic sextic number field. After that, with the help of the fundamental ramification theorem **??**, Stickelberger's theorem **??** on unramified primes and decomposition results for cyclic cubic field and quadratic field, we obtain the prime decomposition for cyclic sextic number fields. As for the unit groups and class numbers for real cyclic sextic fields, Mäki has solved those problem, and give a table on them. For complex case, it's a CM-field, hence the class number and the unit group could be reduced into its cyclic cubic field. But unfortunately, we haven't got the final precise results of them.

Let K_6 be a cyclic sextic number field over $\mathbb{Q}$ with Galois group $G = C_6$, then from Lemma **??**, we have that the signature of K_6 can only be $(6, 0)$ or $(0, 3)$ i.e. K_6 is totally real or totally complex field. It's easy to see that G has exactly two nontrivial subgroups, namely those are of order 2 and order 3, thus the field K_6 has exactly two nontrivial subfields: a (real) cyclic cubic field K_3 and a quadratic field K_2.

Consider $K_2 = \mathbb{Q}(\sqrt{m})$ where m is a square-free integer. $K_3 = \mathbb{Q}(\theta)$. Hence, $K_6 = \mathbb{Q}(\theta, \sqrt{m})$. Let an odd integer s be such that the automorphism σ induced by the mapping $\zeta_{f_6} \to \zeta_{f_6}^s$, where f_6 is the conductor of K_6, satisfies the conditions:

$$\sigma(\theta) = \theta', \sigma(\theta') = \theta'', \sigma(\sqrt{m}) = -\sqrt{m}$$

where the θ' and θ'' denote the conjugates of θ in the cyclic cubic subfield, which are defined in theorem **??**. What's more, we use the following notations $\gamma^{(i)} = \sigma^i(\gamma), i \in \mathbb{Z}$. For simplicity, we will continue to use these notations for the following content.

6.1 Discriminant and Integral Basis

From the Kronecker−Weber theorem, if K_6 is a subfield of a cyclotomic field $\mathbb{Q}(\zeta_k)$ then also $Q(\zeta_{f_2})$ and $Q(\zeta_{f_3})$ are contained in $Q(\zeta_k)$. Hence, we have

$$f_6 = \text{lcm}(f_2, f_3)$$

As we all known, the conductor f_2 of real quadratic field $\mathbb{Q}(\sqrt{m})$ is equal to its fundamental discriminant D, and the conductor $f_3 = e^2$ as we mentioned in **??**. The characters of K_6 [**?**] are the principal character 1, the quadratic character χ_2 of K_2, the generating characters χ_3 and $\bar{\chi}_3$ of K_3 and the generating characters $\chi_6 = \chi_2\chi_3$ and $\bar{\chi}_6 = \chi_2\bar{\chi}_3$ of K_6. The conductor of the character χ_n and $\bar{\chi}_n$ is f_n (since they service for same cyclic galois group). Hence we have following results [**?**]:

Theorem 6.1.1. *The discriminant $d(K_6)$ of the real field K_6 is*

$$d(K_6) = f_6^2 f_3^2 f_2.$$

The proof is easy, as we mentioned above, we have found all characters of K_6, then by the conductor-discriminant formula **??**, we immediately get

$$d(K_6) = f_6^2 f_3^2 f_2.$$

What's more, for complex cyclic sextic fields, we have similar results:

Theorem 6.1.2. *The discriminant $d(K_6)$ of the complex field K_6 is*

$$d(K_6) = f_6^2 f_3^2 f_2.$$

The next theorem [**?**] gives a necessary condition for a number $\alpha \in K_6$ to belong to O_{K_6}. For simplicity, let us denote gcd(f_2, f_3) to be f_*.

Lemma 6.1.1. *If $\alpha \in O_{K_6}$, then α is of the form*

$$\alpha = \frac{1}{2}(x_0 + x_1\theta + x_2\theta') + \frac{1}{2f_*}(y_0 + y_1\theta + y_2\theta')\sqrt{m}$$

where $\frac{1}{2}x_i + \frac{1}{2}y_i\sqrt{m} \in O_{K_2}, (i = 0, 1, 2)$.

Proof. Let $\alpha = a_0 + a_1\theta + a_2\theta' + (b_0 + b_1\theta + b_2\theta')\sqrt{m}$, where $a_i, b_i \in \mathbb{Q}(i = 0, 1, 2)$ be a number of O_{K_6}. Then from the definition of σ, we have

$$\alpha + \alpha^{(3)} = 2(a_0 + a_1\theta + a_2\theta') \in O_{K_3}.$$

Recall the theorem **??**, we have $(1, \theta, \theta')$ is an integral basis of K_3. So we have $a_i = x_1/2$, where $x_i \in \mathbb{Z}(i = 0, 1, 2)$. Also we have

$$\sqrt{m}(\alpha - \alpha^{(3)}) = 2m(b_0 + b_1\theta + b_2\theta')$$

is an algebraic integer. Hence $b_i = z_i/(2m)$ where $z_i \in \mathbb{Z}(i = 0, 1, 2)$. Let $\lambda_i = \frac{1}{2}x_i + \frac{1}{2m}z_i\sqrt{m}$. Now we have the equations:

$$\begin{aligned} \alpha &= \lambda_0 + \lambda_1\theta + \lambda_2\theta' && (6.1)\\ \alpha^{(4)} &= \lambda_0 + \lambda_1\theta' + \lambda_2\theta'' && (6.2)\\ \alpha'' &= \lambda_0 + \lambda_1\theta'' + \lambda_2\theta && (6.3) \end{aligned}$$

the determinant of the system of linear equation is $\pm f_3$ ($-f_3$ actually, but no need to determine the sign), since this can be viewed as the determination of integral basis and its conjugates. From the definition of discriminant, we have the discriminant is a square root of the discriminant, namely $\pm f_3$. By any case, this follows that the number $f_3\lambda_i(i = 0, 1, 2)$ are algebraic integers.

Then, the numbers $f_3 z_i/m(i = 0, 1, 2)$ are rational integers. Since f_3 is odd, gcd$(m, f_3) = f_*$. Hence $z_i/m = y_i/f_*$ where $y_i \in \mathbb{Z}(i = 0, 1, 2)$, and $\frac{1}{2}x_i + \frac{1}{2}y_i\sqrt{m} \in O_{K_2}$, because f_3 is odd and $f_3\lambda_i$ is integral. □

Note that if $f_* = \gcd(m, f_3) = 1$, it follows that $O_{K_6} = O_{K_2}O_{K_3}$, which coincides the result which can be found in [**? ?**] etc.

Next we will using above lemma to determine the integral basis of the cyclic sextic field.

Theorem 6.1.3. *The integral basis of the cyclic sextic field $K_6 = \mathbb{Q}(\theta, \sqrt{m})$(m is a square-free integer.) is of form*

$$(1, \theta, \theta', \eta, \eta\theta, \eta\theta'),$$

where $\eta = \frac{Df_*+\sqrt{D}}{2f_*}$, $f_* = \gcd(f_2, f_3)$ and $D = f_2$ is the (fundamental) discriminant of the quadratic subfield.

Proof. From lemma **??**, it's easy to show that each element in the basis is of course integral in K_6. So we need to calculate the discriminant of these elements. Let A denote the matrix

$$\begin{pmatrix} 1 & \theta & \theta' \\ 1 & \theta' & \theta'' \\ 1 & \theta'' & \theta \end{pmatrix},$$

and

$$B = \begin{pmatrix} \eta & \eta\theta & \eta\theta' \\ \eta & \eta\theta' & \eta\theta'' \\ \eta & \eta\theta'' & \eta\theta \end{pmatrix}, C = \begin{pmatrix} \bar{\eta} & \bar{\eta}\theta & \bar{\eta}\theta' \\ \bar{\eta} & \bar{\eta}\theta' & \bar{\eta}\theta'' \\ \bar{\eta} & \bar{\eta}\theta'' & \bar{\eta}\theta \end{pmatrix}$$

where $\bar{\eta} = \frac{Df_*-\sqrt{D}}{2f_*}$, then the discriminant of the elements is following:

$$\begin{aligned} & \text{Disc}(1, \theta, \theta', \eta, \eta\theta, \eta\theta') \\ = & \left(\det\begin{pmatrix} A & B \\ 0 & C-B \end{pmatrix}\right)^2 \\ = & (\det(A) \cdot \det(C-B))^2 \\ = & \left(-f_3 \cdot ((\sqrt{D})^3 \cdot (-f_3)/f_*)\right)^2 \\ = & \frac{f_3^4 D^3}{f_*^2} \\ = & f_3^2 f_2 \frac{f_3^2 f_2^2}{f_*^2} \\ = & f_3^2 f_2 f_6^2 \end{aligned}$$

i.e. we have the basis's discriminant is equal to the discriminant of the field, hence

$$(1, \theta, \theta', \eta, \eta\theta, \eta\theta')$$

is an integral basis. □

6.2 Prime Decomposition

For the prime decomposition in cyclic sextic field, we should consider the situation of its two subfields, which are solved in Chapter **??** and **??**. First of all, let us consider the ramified primes in the cyclic sextic field. As we known in previous theorem, the discriminant of the cyclic sextic field is $d(K_6) = f_2 f_3^2 f_6^2$, from the fundamental ramification theorem **??**, we should consider the prime numbers and discriminant. Since $f_6 = \mathrm{lcm}(f_2, f_3)$, hence if $p \mid d(K_6)$, then $p \mid f_2$ or $p \mid f_3$. More precisely, form the chain rules for ramification index and decomposition number, we can immediately get the following results.

Theorem 6.2.1. *Let $K_6 = \mathbb{Q}(\theta, \sqrt{m})$ be the cyclic sextic field, suppose $f_3 = 3^\delta p_1 p_2 \cdots p_t$, and $f_2 = D = 2^\delta q_1 q_2 \cdots q_s$ where $\delta = \{0, 2\}$, $p_i \equiv 1 (\bmod 3)$ and $q_i \equiv 1 (\bmod 2)$; s, t are rational integers. What's more, without loss of generality, suppose $p_i = q_i$ for $0 < i \leq t_0 \leq \min\{s, t\}$, Then we have*

1. *if $p = p_i = q_i$, where $0 < i \leq t_0 \leq \min\{s, t\}$, then p is totally ramified, i.e. $pO_{K_6} = \wp^6$*
2. *if $p = p_i$, where $i > t_0$, then p is ramified in the subfield $K(\theta)$, and we have $pO_{K_6} = \wp_1^3 \wp_2^3$ if $\left(\frac{f_2}{p}\right) = 1$ or $pO_{K_6} = \wp^3$ if $\left(\frac{f_2}{p}\right) = -1$.*
3. *if $p = q_i$, where $i > t_0$, then p is ramified in the subfield $K(\sqrt{m})$, and we have $pO_{K_6} = \wp_1^2 \wp_2^2 \wp_3^2$ or $pO_{K_6} = \wp^2$. To determine which case is suitable for p, we should used the results in section* **??** *in chapter* **??**.

As for the results for unramified cases, suppose p is an unramified prime in O_{K_6}, i.e. $p \nmid f_2$ and $p \nmid f_3$, then from the theorem **??**, we have

Theorem 6.2.2. *Let $K_6 = \mathbb{Q}(\theta, \sqrt{m})$ be the cyclic sextic field, p be an unramified prime in O_{K_6}, then*

1. *if $\left(\frac{d(K_6)}{p}\right) = 1$, then $pO_{K_6} = \prod_{i=1}^{6} \wp_i$ (splits completely), or $pO_{K_6} = \wp_1 \wp_2$.*
2. *if $\left(\frac{d(K_6)}{p}\right) = -1$, then $pO_{K_6} = p$ (inert) or $pO_{K_6} = \wp_1 \wp_2 \wp_3$.*

To determined the exact cases for above unramified theorem, we should refer to chapter **??**.

6.3 Unit and Class Number of Real Cyclic Sextic Field

For real cyclic sextic field, we have the signature of K_6 can only be $(6, 0)$, then according to Dirichlet's theorem **??** on units in K_6 there are 5 fundamental units, which together with -1 generate the multiplicative group U_6 of units of K_6. The unit group U_6 has the unit groups U_2 and U_3 of the subfields K_2 and K_3 as subgroups.

As we known before, suppose U_2 is generated by -1 and the fundamental unit μ, and U_3 is generated by -1, a fundamental unit τ and one of its conjugates $\tau' = \sigma(\tau)$. From Latimer's work [**?**], we know that K_6 has a system of fundamental units containing μ, τ, τ'. So there are three fundamental units are known, i.e. those belonging to the proper subfields, namely ϵ, τ, τ'.

To determine the other two units we should first get a so called cyclotomic unit which is calculable from a definite expression. This unit, together with its conjugates, and the units of the proper subfields generate a subgroup of finite index in the whole unit group, and it is in principle relatively easy to obtain the whole group from this subgroup.

First of all, we need a so-called relative units, a unit ϵ of K_6 for which $N_{6/3}(\epsilon) = \pm 1$ and $N_{6/2}(\epsilon) = \pm 1$ is called a **relative units**. Let U_R denoted the group of relative units, i.e. we have

$$U_R = \{\epsilon \in U_6 | N_{6/3}(\epsilon) = \pm 1, N_{6/2}(\epsilon) = \pm 1\}$$

Note that if $\epsilon \in U_R$, then $N_{6/1}(\epsilon) = N_{2/1}(N_{6/2}(\epsilon)) = N_{2/1}(\pm 1) = 1$. On the other hand, $1 = N_{6/1}(\epsilon) = N_{3/1}(N_{6/3}(\epsilon)) = (N_{6/3}(\epsilon))^3$ so that for $\epsilon \in U_R$, we have $N_{6/3}(\epsilon) = 1$

What's more, Mäki has proved that in K_6, there exists a generating relative unit ξ_R such that

$$U_R = \{\pm \xi_R^k \xi_R'^l | k, l \in \mathbb{Z}\}.$$

On the contrary, every relative unit in K_6 has a unique representation in this form. Mäki also showed that how to calculate ξ_R and then establish a solution of the unit.

As for the class number, using the cyclotomic unit, Mäki has prove a theorem that $h_6 = h_2 h_3 h_R$, where h_2, h_3 are class number of the subfield K_2 and K_3, and the h_R is so-called relative class number of K_6. These numbers can be calculated by the cyclotomic units together with fundamental units.

Mäki lists a huge number with conductor $f_6 \leq 2021$ of cyclic sextic field with class number and unit group in her book. Then, together with Ennola and Turunen, she extend this table for $f_6 < 4000$.

6.4 Unit and Class Number of Complex Cyclic Sextic Fields

For complex situation, then the signature of K_6 can only be $(0, 3)$, then according to Dirichlet's theorem **??** on units in K_6 there are 2 fundamental units, which together with $\mu(K_6)$ generate the multiplicative group U_6 of units of K_6.

To start discussing the unit and class number of complex cyclic sextic fields, we first introduce the CM-field. Then idea of CM-field is the extension of complex quadratic field and cyclotomic field. A CM-field K is a totally imaginary extension of a totally real number field k^+, i.e.

$$K = K^+(\sqrt{a}),$$

where K^+ is totally real, and $a \in K^+$ has negative conjugates.

For example, $K = \mathbb{Q}(\zeta_m)$ is a CM-field, since $K = K^+(\sqrt{a})$, where $K^+ = \mathbb{Q}(\zeta + \zeta^{-1})$, and $a = \zeta^2 + \zeta^{-2} - 2$.

The relationship between the largest totally real subfield and the CM-field are very useful:

Theorem 6.4.1. *Let $\mathbb{Q} \subset F \subset K$ be nontrivial extensions of number fields. Then K is a CM-field, with F its totally real subfield, if and only if U_K/U_F is finite.*

Another useful theorem [**?**] for class number and unit group is showed as follows:

Theorem 6.4.2. *Let K be a CM-field, K^+ its largest totally real subfield, h and h^+ be the class number of them respectively, U and U^+ be the unit group of K and K^+, then:*

1. $h^- = h/h^+$ *is so-called the relative class number, which is a rational integer.*
2. $Q := [U : \mu(K)U^+] = 1$ *or* 2

More precisely, S. Louboutin has given the class number for complex cyclic sextic field with $f_6 \leq 220000$.

Chapter 7 Examples for Cyclic Sextic Fields

In this chapter, we will give some examples for cyclic sextic field, using our results or methods given by chapter **??** to a series of problems: discriminant, integral basis, decomposition of prime, unit group and class number etc. For the first example in cyclotomic field, there exists a complete theory for that. But as a cyclic sextic number field, using the methods given by chapter **??**, we also got the structures of it. More precisely, we discover two subfields of it, and then calculate the discriminant which is equal to the result in cyclotomic fields' theorem. Then we also give the prime decomposition of it based on our theorems in section **??**. Also, we calculate the class number using the general theory. To solve the second field in section **??**, we use almost all preliminaries we mentioned before. We first determine the Galois group of it, then we calculate the polynomial discriminant of it, based on the discriminant formula, then we find two subfields of it. After that, we also find its integral basis and get the prime decompositions. Also, we have tried to calculate the class number of it using general theory, and get the same result as Mäki did. The third section is another example given by A Bremner and B Spearman[**?**] with sextic trinomial, but unfortunately, we haven't got the final results.

7.1 7-th Cyclotomic Field

7.1.1 Cyclotomic Fields

Let ζ_n denote a fixed primitive n^{th} root of unity, and let $\mathbb{Q}(\zeta_n)$ be the number field generated by all the n^{th} root of unity. The field $\mathbb{Q}(\zeta_n)$ is called the n^{th} **cyclotomic field**. A following result is very import theorem.

Theorem 7.1.1. *Let $\phi(n)$ denote the (Euler) totient of n, then $\mathbb{Q}(\zeta_n)$ is an Abelian extension of $\mathbb{Q}$ of degree $\phi(n)$. More precisely, there is an isomorphism:*

$$\begin{array}{rcl} (\mathbb{Z}/n)^{\times} & \to & \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \\ \bar{a} & \mapsto & \sigma_a, \end{array}$$

where $\sigma_a(\zeta_n) = \zeta_n^a$

Since a sub-extension of an Abelian extension is also Abelian, cyclotomic fields and their subfields already give us an abundant supply of Abelian extensions of $\mathbb{Q}$. More formally, we have the

Theorem 7.1.2 (Kronecker-Weber)**.** *Every finite abelian extension of $\mathbb{Q}$ is contained in a cyclotomic field.*

7.1.2 7-th Cyclotomic Field

Now let us consider the simplest cyclic sextic field, a 7-th cyclotomic field. As we all know, $K_6 = \mathbb{Q}(\zeta_7)$ is generated by ζ_7, which is a root of unity, and its minimal polynomial is

$$f(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1.$$

First of all, we would know its structure. As we known in Section **??**, this field is a CM-field, i.e. a totally imaginary extension of a totally complex cyclic cubic field. Write as before, we have $K_6 = \mathbb{Q}(\sqrt{m}, \theta)$, where m is a negative squarefree integer. Now we need to find the minimal polynomials for $\sqrt{m}$ and θ.

Note that ζ_7^i is complex conjugate to ζ_7^{-i}, so let $\xi = \zeta_7 + \frac{1}{\zeta_7}$, then ξ is a real number*. Since ζ_7 is a root of the minimal polynomial, then we have

$$\zeta_7 + \frac{1}{\zeta_7} + \zeta_7^2 + \frac{1}{\zeta_7^2} + \zeta_7^3 + \frac{1}{\zeta_7^3} + 1 = 0,$$

Substitute ξ into the equation, we have

$$g(\xi) = \xi^3 + 2\xi^2 - 2\xi - 1 = 0 \tag{7.1}$$

Let $x = \xi - \frac{2}{3}$, we can change it into the standard form, i.e.

$$x^3 - x^2 - 2x + \frac{13}{27},$$

where we can get $e = 7, u = -1, v = 1$, hence, the cyclic cubic subfield defined by ξ, where ξ is a solution of equation **??**. i.e. $K^+ = K_3 = \mathbb{Q}(\xi)$.

From theorem **??**, we got the discriminant of K_3 is $49 = f_3^2$, and since $v = 1$, we got that $(1, \xi, \xi^2)$ is a power integral basis of K_3.

On the other hand, note that the automorphism $\sigma_2 : \zeta_7 \to \zeta_7^2$ generates the subgroup of order 3. Thus consider $\omega = \zeta_7 + \zeta_7^2 + \zeta_7^4$. From the properties of root of unity, we have following two equations:

$$(\zeta_7 + \zeta_7^2 + \zeta_7^4) + (\zeta_7^3 + \zeta_7^6 + \zeta_7^{12}) = -1,$$

$$(\zeta_7 + \zeta_7^2 + \zeta_7^4)(\zeta_7^3 + \zeta_7^6 + \zeta_7^{12}) = 3 - 1 = 2$$

Then ω satisfies a quadratic equation:

$$h(x) = x^2 + x + 2 = 0,$$

hence $\mathbb{Q}(\omega)$ is a quadratic subfield, and $K_2 = \mathbb{Q}(\sqrt{-7})$. Then the discriminant of K_2 is $-7 = f_2$. From theorem **??**, we have the discriminant of K_6 is $d(K_6) = (-7) \times (7)^2 \times (7)^2 = -7^5$.

*One can find that $\xi = 2\cos\frac{2\pi}{7}$.

A famous result for discriminant of $\mathbb{Q}(\zeta_p)$, where p is a prime, is that $\text{Disc}(\mathbb{Q}(\zeta_p)) = (-1)^{(p-1)/2}p^{p-2}$. In this field, we have $\text{Disc}(\mathbb{Q}(\zeta_7)) = (-1)^3 7^{7-2} = -7^5$, which coincides our result.

To sum up, we got that $K_6 = \mathbb{Q}(\xi, \sqrt{-7})$. As for the prime decomposition, the discriminant has only one prime divisor, namely 7, hence only 7 is ramified in K_6. what's more, since 7 is common factor of f_2 and f_3, hence it is totally ramified. In fact, since K_6 is monogenic, we have $(x+6)^6 (\bmod 7)$. For other primes, we just need to consider the decomposition in subfields, the using the result in section **??**. For example, consider $p = 37$, note that

$$\left(\frac{-7}{37}\right) = (-1)^{(37-1)/2}\left(\frac{7}{37}\right) = (-1)^{(7-1)(37-1)/4}\left(\frac{37}{7}\right) = -\left(\frac{2}{7}\right) = 1$$

Hence 37 is ramified in K_2. On the other hand, similarly, consider we just need to verify that $49^{(37-1)/3} \equiv 1 (\bmod 37)$ or not. However, $49^{(37-1)/3} \equiv 12^{12} \equiv (-4)^6 \equiv (-10)^2 \equiv 26 \not\equiv 1 (\bmod 37)$, hence 37 is inert in K_2. Hence, $37 = \wp_1\wp_2$.

As for the unit group of K_6, we first refer a theorem [**?**] which is a corollary of theorem **??** as follows:

Theorem 7.1.3. *Let $m = p^s$, where p is an odd prime, $s \in \mathbb{N}^*$, then $K = \mathbb{Q}(\zeta_m)$ has the same system of fundamental units to $K^+ = \mathbb{Q}(\zeta_m + \zeta_m^{-1})$.*

So from Dirichrlet Theorem **??**, $U(K_6) = \mu(K_6) \times \mathbb{Z}^2$, where $\mu(K_6) = \langle\zeta_7\rangle$ is the root of unity of K and the fundamental units are the same to K_3. The fundamental units in K_3 are

$$(-1+\xi+\xi^2, 2-\xi^2) = (1+\zeta_7+\zeta_7^2+\zeta_7^{-1}+\zeta_7^{-2}, -\zeta_7^{-2}-\zeta_7^2).$$

As for the class number, firstly, we compute the Minkowski's bound, and we get

$$C(K_6) = \left(\frac{4}{\pi}\right)^3 \frac{6!}{6^6}\sqrt{|-7^5|} = 4.13$$

Hence $Cl(K_6) = \langle[\wp]|\wp|2 \text{ or } 3\rangle$

now we consider the decomposition of 2 and 3. since $\left(\frac{-7}{2}\right) = 1$, hence it splits in K_2. On the other hand, $x^3+x^2-2x-1 \equiv x^3+x^2+1 (\bmod 2)$, i.e. it's inert in K_3, hence $2 = \wp_1\wp_2$*. In fact, $\wp_1 = (2, 1+\xi+\xi^3)$, $\wp_2 = (2, 1+\xi^2+\xi^3)$, since $1+\xi^2+\xi^3$ is conjugate to $1+\xi+\xi^3$, hence $[\wp_1] = [\wp_2] = 1$.

For $p = 3$, it's easy to see that $\left(\frac{-7}{3}\right) = -1$ and x^3+x^2-2x-1 is irreducible in $\mathbb{F}_3$, hence $p = 3$ is inert in K_6. To sum up, we have the class number is 1.

*Here we haven't use cubic reciprocity, since there is no definition for $p = 2$(in fact it only define in $p = 3k+1$, like quadratic reciprocity defined in $p = 2k+1$).

7.2 A Real Cyclic Sextic Field

Consider the sextic field K_6 generated by a root of

$$f(x) = x^6 - x^5 - 6x^4 + 6x^3 + 8x^2 - 8x + 1.$$

First note that $f(x)$ is irreducible over $\mathbb{Q}$, since $f(x) \equiv x^6 + x^5 + 1 (\bmod 2)$. In order to verify the Galois group of the splitting field of f, we should first compute the resolvent polynomials. Let $p_1 = x_1 + x_2$, $p_2 = x_1 + x_2 + x_3$, then use the numerical method, we have the approximate root of f are:

$$(r_1, r_2, r_3, r_4, r_5, r_6) = (-1.97766, -1.46610, 0.14946, 0.73068, 1.65248, 1.91115)$$

Then,

$$\begin{aligned}
R_{p_1,f}(y) &= \prod_{p_{1i} \in orb(p)} (y - p_{1i}(r_1, \ldots, r_6)) \\
&= x^{15} - 5x^{14} - 14x^{13} + 98x^{12} + 7x^{11} - 567x^{10} + 280x^9 + 1404x^8 \\
&\quad -818x^7 - 1596x^6 + 735x^5 + 700x^4 - 203x^3 - 77x^2 + 11x + 1 \\
&= (x^3 - x^2 - 2x + 1)(x^6 - 2x^5 - 10x^4 + 6x^3 + 30x^2 + 17x + 1) \\
&\quad (x^6 - 2x^5 - 10x^4 + 27x^3 - 12x^2 - 4x + 1)
\end{aligned}$$

So we have $(3, 6^2)$ cycle, from table **??**, we have that the Galois group of f is either C_6 or D_6. Then we calculate $R_{p_2,f}$,

$$\begin{aligned}
R_{p_2,f}(y) &= \prod_{p_{2i} \in orb(p)} (y - p_{2i}(r_1, \ldots, r_6)) \\
&= x^{20} + 2x^{19} - 106x^{18} - 600x^{17} - 593x^{16} + 3252x^{15} - 6530x^{14} \\
&\quad -2589x^{13} + 4875x^{12} - 675x^{11} - 1759x^{10} + 3349x^9 + 5376x^8 + 1260x^7 \\
&\quad +1188x^6 + 865x^5 + 316x^4 + 77x^3 + 23x^2 + 11x + 1 \\
&= (x^2 - x + 1)(x^6 - 12x^5 + 3x^4 + 7x^3 + 6x^2 - 2x + 1) \\
&\quad (x^6 + 8x^5 + 25x^4 + 2x^3 + 5x^2 + 2x + 1) \\
&\quad (x^6 + 7x^5 - 8x^4 + 4x^3 + 27x^2 + 12x + 1)
\end{aligned}$$

So we have $(2, 6^3)$ cycle, from table **??**, we have that the Galois group of f is C_6, also we know K_6 is totally real.

The polynomial discriminant of f could be given by formula **??**, in fact, $\text{Disc}(f) = 453789 = 3^3 \times 7^5$ Note that, $d(K_6) = f_2 f_3^2 f_6^2$ by theorem **??**, since $f_6 = \text{lcm}(f_2, f_3)$, hence we have $f_2^3 | d(K_6)$ and $f_3^4 | d(K_6)$. The relation between $d(K_6)$ and $\text{Disc}(f)$ is showed in lemma **??**, i.e. $\text{Disc}(f) = a^2 d(K_6)$, here we have

$$3^3 \times 7^5 = a^2 f_2 f_3^2 f_6^2,$$

from the requirements we mentioned above, we have

$$a^2f_3^4|3^3\times 7^5,$$

this force $f_3=7$, and $a=1$ or $a=3$. Then $a^2f_2^3f_3^2|3^3\times 7^5$, i.e.

$$a^2f_2^3|3^3\times 7^3.$$

If $a=3$, then $f_2=7$, and for this case $d(K_6)=7^5$, and we get $3^3d(K_6)=\mathrm{Disc}(f)$. An contradiction! Hence, $a=1$, and we could get $f_2=3\times 7$.

To sum up, we have $f_2=21, f_3=7$. So we can immediately get the quadratic subfield is $\mathbb{Q}(\sqrt{21})$, with minimal polynomial $g(x)=x^2-x-5$, and integer ring $\mathbb{Z}\left[\frac{1+\sqrt{21}}{2}\right]$. [*] As for the cyclic cubic subfield, since $e=f_3=7$, and $v=1$, hence we have the minimal polynomial of θ, $h(x)=x^3-x^2-2x+\frac{13}{27}$ with power integral $(1,\theta,\theta^2)$. To sum up,

$$K_6=\mathbb{Q}(\theta,\sqrt{21})$$

Since $d(K_6)=\mathrm{Disc}(f)$, hence K_6 has a power integral basis, wlog, let r be a root of f, then $(1,r,r^2,\ldots,r^5)$ is a integral basis. On the other hand, we have another integral basis given by theorem **??**.

The prime decomposition is quite easy, 7 is totally ramified in K_6, since it is ramified in both two subfield. In fact, $f(x)\equiv(x+1)^6(\operatorname{mod}7)$. Hence $7O_{K_6}=\wp^6$, where $\wp=(7,r+1)$. 3 is ramified in K_2, and inert in K_3, hence $2O_{K_6}=\wp'^2$. The other prime's situation could be solved through theorem **??**.

As for the class number, we first compute the Minkowski's bound,

$$C_{K_6}=(4/\pi)^0\frac{6!}{6^6}\sqrt{453789}=10.4,$$

now we should consider $p=2,3,5,7$. we can find that 2 is inert in O_{K_6}. 7 is totally ramified with $\wp=(7,r+1)$, while $N(r+1)=7$[†], $(r+1)\subset(7)$, hence $\wp=(r+1)$ is a principal ideal.

As for $p=3$, we have $f(x)\equiv(2+x+x^2+x^3)^2(\operatorname{mod}3)$, hence $\wp'=(3,2+r+r^2+r^3)$, $N(2+r+r^2+r^3)=3$ hence $\wp'=(2+r+r^2+r^3)$. Similar result for $p=5$. Finally, we get $h(K_6)=1$.

7.3 Sextic Trinomials

As expected, increasing the degree of a polynomial will increase its complexity. In the case of sextics, however, the number of possible Galois groups jumps up to sixteen. We

[*] In fact, since $\phi(21)=\phi(3)\times\phi(7)=12$ and $6|12$, actually this cyclic sextic field is a subfield of the cyclotomic field $\mathbb{Q}(\zeta_21)$.

[†] calculate through $f(x-1)$

can once again find a list of these groups in Cohen's book and we expect S_6 to be the most frequently occurring group.

It is much more preferable to work with sextic trinomials rather than general sextics. Again, we can reduce the possible unique forms of these trinomials to only $x^6+ax+b, x^6+ax^2+b, x^6+ax^3+b$. Note that the last of these three forms can be simplified to a quadratic in x^3.

It has already been shown by A Bremner and B Spearman [**?**] that up to scaling, there exists a single, unique sextic trinomial with Galois group isomorphic to C_6; which was given as

$$f(x) = x^6 + 133x + 209$$

Now we focus on this example, i.e. K_6 is the splitting field of $f(x)$. First of all, since $f(x) \equiv x^6 + x + 1 (\bmod 2)$, hence $f(x)$ is irreducible over $\mathbb{Q}$. Then, we can compute the discriminant of the polynomial, from formula **??**, we have

$$\text{Disc}(f) = (-1)^{\frac{4\times5}{2}} \cdot 5^5 \cdot 133^6 + (-1)^{\frac{6\times5}{2}} \cdot 6^6 \cdot 209^5 = -19^5 \times 83^2 \times 277^2.$$

We have $d(K_6) = f_2 f_3^2 f_6^2$ by theorem **??**, since $f_6 = \text{lcm}(f_2, f_3)$, hence we have $f_2^3 | d(K_6)$ and $f_3^4 | d(K_6)$. The relation between $d(K_6)$ and Disc(f) is showed in lemma **??**, i.e. Disc$(f) = a^2 d(K_6)$. Whatever, $f_3^4 | d(K_6)$ force that $f_3 = 19$ and $-19 | f_2$. There are several possible cases for $d(K_6)$:

$$\begin{cases} f_3 = 19, f_2 = -19; \\ f_3 = 19, f_2 = -19 \times 83; \\ f_3 = 19, f_2 = -19 \times 277; \\ f_3 = 19, f_2 = -19 \times 83 \times 277. \end{cases}$$

To recognize the case for the field generated by a root of f, we need another method. However, this example is still under solving.

Chapter 8 Galois Extensions of Function Fields

Lüroth's theorem is one of elementary results in the classical algebra which we can find in a textbook by Van Der Waerden [**?**]. Lüroth [**?**] proved Lüroth's theorem in case $K = \mathbb{C}$ in 1876. It was first proved for general fields K by Steinitz [**?**] in 1910, by the above argument. An precisely elementary algebraic proof using field theory and Gauss's Lemma was given by G. Bergman as a series of exercises for students. The Lüroth's theorem is showing as follows:

Theorem 8.0.1 (Lüroth's Theorem)**.** *Let K and E be fields such that $K \subsetneq E \subset K(x)$, where x is transcendental extension of K. Then $E = K(u)$ for $u \in K(x)$, and $K(x)$ is finite-dimensional over E.*

In our work, we are focus on a special case in Lüroth theorem, i.e. we add a condition on the field extension $K(x)/E$, namely we suppose that $K(x)/E$ is Galois. And for this case, we will first give a simple proof of the similar results. Of course, we won't use the result of Lüroth's thorem. Then, we will give a explicit form of the invariant rational function due to the Galois group.

8.1 Existence Theorem

First, we'd like to give the following theorem:

Theorem 8.1.1. *Let K and E be fields such that $K \subsetneq E \subset K(x)$, where x is transcendental extension of K and $K(x)$ is Galois over E. Then $E = K(u)$ for $u \in K(x)$.*

For simplicity, we start with a definition of height of a rational function.

Definition 8.1.1 (height)**.** *The **height** of a rational function $u(x) = f(x)/g(x)$ in a rational function field is defined to be*

$$\mathrm{ht(u)} = \max\{\deg(f(x)), \deg(g(x))\}$$

Gauss's Lemma is necessary in our proof, which is either of two related statements about polynomials with integer coefficients. The first one is the primitivity statement and the second is the irreducible statement [**?**].

Lemma 8.1.1 (Gauss's Lemma)**.** *Let R be a unique factorization domain.*

1. *The product of two primitive polynomials is primitive, what's more, for $f, g \in R[x]$, we have $C(f)C(g) = C(fg)$, where $C(f)$ is the great common divisor of the coefficients of f.*

2. *If $f \in R[x] \backslash R$ is irreducible in $R[x]$, then f is irreducible in $Frac(R)[x]$.*

We give the following lemma **??** which solve the finiteness of the extension in Lüroth's theorem and our special case.

Lemma 8.1.2. *If K is a field and $u(x) \in K(x)\backslash K$, then $[K(x) : K(u)] = \mathrm{ht}(u)$.*

Proof. Write $u(x) = a(x)/b(x)$, where $a, b \in K[x]$ are coprime. Then x is a root of the polynomial $f := a(T) - u(x)b(T) \in K(u)[T]$. Since this polynomial has degree one in u, then the coprimality of $a(T), b(T)$ implies that f is irreducible in $(K[T])[u] = (K[u])[T]$. From Gauss's Lemma, we have that f is irreducible in the fractional polynomial field $K(u)[T]$, i.e. f is a constant multiple of the minimal polynomial of x over $K(u)$. i.e. we have $[K(x) : K(u)] = \deg_t(f) = \mathrm{ht}(u)$. □

Since $K(x)/E$ is Galois, hence is a finite separable and normal extension. From the following so called primitive element theorem , we could know that $K(x)/E$ is finite simple extension.

Lemma 8.1.3 (Primitive Element Theorem)**.** *Let $E \supseteq F$ be a finite degree separable extension. Then $E = F(\alpha)$ for some $\alpha \in E$.*

Proof of Theorem **??**. Since $K(x)/E$ is Galois, so is finite simple extension (simple algebraic extension).Since $K(x) = E(x)$, i.e. $K(x)$ can be viewed as a simple algebraic extension by adding x into E. Then we may assume that $p(t)$ be the minimal polynomial of x over E,

$$p(t) = t^n + r_{n-1}t^{n-1} + \cdots + r_1 t + r_0, (r_i \in E \subset K(x)).$$

Consequently, $n = \deg_t(p) = [K(x) : E]$. Let rewrite $r_i = a_i/b_i, (i = 0, 1, \ldots, n-1)$ where $a_i, b_i \in K[x]$, and a_i is coprime to b_i. Then $p(t)$ could be multiplied by the l.c.m. of the b_i's in order to get a primitive polynomial over the ring $K[x]$, namely

$$q(t) = c_n t^n + c_{n-1}t^{n-1} + \cdots + c_0 \in K[x][t].$$

Here, we get $\deg_t(q) = \deg_t(p)$

Note that (at least) one of the r_i's, i.e. $u := r_k \in E$, doesn't not belong to K, else x would be algebraic over K. Let's consider the polynomial:

$$R(x,t) = a_k(t)b_k(x) - a_k(x)b_k(t) \in K[x,t]$$

Since $R(x,x) = 0$, $q(t)$ is the minimal polynomial of x, then $q(t)$ divides $R(x,t)$ in $K(x)[t]$. Since $K[x]$ is a UFD, hence by Gauss's lemma, $q(t)$ divides $R(x,t)$ in $K[x,t]$. Therefore $\deg_x(R) \geq \deg_x(q)$.

On the other side,

$$\deg_x(R) \leq \mathrm{ht}(u) = \max(\deg a_k, \deg b_k) \leq \max(\deg c_k, \deg c_n).$$

Therefore $\deg_x(R) \leq \deg_x(q)$. Hence, $\deg_x(R) = \deg_x(q)$, that is we have

$$R(x,t) = q(t)m(t),$$

where $m \in K[t]$.

Then we will show that $m(t)$ is constant, i.e. $m(t) \in K$. Assume on the contrary deg$(m) > 0$, then we have

$$a_k(t) = q_1(t)m(t) + l_1(t), b_k(t) = q_2(t)m(t) + l_2(t)$$

with deg$(l_i) <$ deg$(m)(i = 1, 2)$. Since $m(t)$ divides $a_k(t)b_k(x) - a_k(x)b_k(t)$, hence also divides $l_1(t)b_k(x) + a_k(x)l_2(t)$, which is possible only if

$$l_1(t)b_k(x) + a_k(x)l_2(t) = 0.$$

However, last equation is impossible since a_k is coprime to b_k, and neither of them is constant. A contradiction! Hence, deg$(m) = 0$ and $m \in K$.

Write $q(t) = c\left(a_k(t)b_k(x) - a_k(x)b_k(t)\right), c \in K$, $[K(x) : E] = \deg_t(q) = \text{ht}(u)$. From lemma **??**, we have $[K(x) : K(u)] = \text{ht}(u)$, hence we have $[K(x) : K(u)] = [K(x) : E]$. Since $u \in E$, then $E = K(u) = K(r_k)$. □

8.2 Explicit Form of Invariants

From now on, we have prove the existence of the $u(x) \in K(x)$, such that $E = K(u)$. Next, we will show the explicit form of u. Assume that Gal$(K(x)/E) =$ Gal$(K(x)/(K(u))) = \{\sigma_1, \sigma_2, \ldots, \sigma_n\}$.

In fact, we have an easy proposition that if $F \subset E \subset K$ are fields, then Aut(K/E) is a subgroup of Aut(K/F), since the operation (composition) is the same and any automorphism which fixes E must also fix the smaller field F. So, we have

$$\text{Gal}(K(x)/E) = \text{Aut}(K(x)/E) \subset \text{Aut}(K(x)/K).$$

Next we will show that the automorphism group of a rational function field $K(x)$ is PGL$(2, K)$. From lemma **??**, let $u = \frac{ax+b}{cx+d} \in K(x)$, where $a, b, c, d \in K$ and $ad - bc \neq 0$, then $[K(x)/K(u)] = \text{ht}(u) = 1$, i.e. $K(x) = K(u)$. On the other side, if we have $K(x) = K(u)$, i.e. $[K(x) : K(u)] = 1$, then ht$(u) = 1$. $u = \frac{P(x)}{Q(x)}$, where max deg$(P(x))$, deg$(Q(x)) = 1$, then $u = \frac{ax+b}{cx+d}$, where $a, b, c, d \in K$ and $ad - bc \neq 0$. i.e. We have $K(x) = K(u)$ if and only if $u \in \frac{ax+b}{cx+d}$, where $a, b, c, d \in K$ and $ad - bc \neq 0$. i.e. we have the automorphism group of $K(x)$ is

$$\text{Aut}(K(x)/K) = \left\{ x \mapsto \frac{ax+b}{cx+d} \mid a, b, c, d \in K, ad \neq bc \right\}.$$

Since general linear group is

$$\text{GL}(2, K) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in K, ad - bc \neq 0 \right\},$$

then consider the group homomorphism: GL$(2, K) \to$ Aut$(K(x)/K)$, where

$$\psi : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \frac{ax+b}{cx+d},$$

with kernel

$$\operatorname{Ker}\psi = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \mid a \in K - \{0\} \right\}.$$

We defined the projective general linear group $\mathrm{PGL}(2,K) = \mathrm{GL}(2,K)/(aI_2)$. Hence, we have

$$\mathrm{Aut}(K(x)/K) \cong \mathrm{PGL}(2,K).$$

Now we have $\mathrm{Gal}(K(x)/E) \subset \mathrm{PGL}(2,K)$ up to isomorphism.

We can easily write down the minimal polynomial of x over $E = K(u)$ as following,

$$p(t) = (t - \sigma_1(x))(t - \sigma_2(x)) \cdots (t - \sigma_n(x))$$

Then $n = |\,\mathrm{Gal}(K(x)/E)| = [K(x) : E] = [K(x) : K(u)] = \mathrm{ht}(u)$.

To sum up, we have following theorem:

Theorem 8.2.1. *Suppose $K(x)/E$ is Galois, then $G = \mathrm{Gal}(K(x)/E) \subset \mathrm{PGL}(2,K)$. What's more, suppose the minimal polynomial of $K(x)/E$ is*

$$p(t) = (t - \sigma_1(x))(t - \sigma_2(x)) \cdots (t - \sigma_n(x)) = t^n + c_{n-1}t^{n-1} + \cdots c_1 t + c_0,$$

where $c_i(x) \in K(x)$. Then $\forall c_i(x) \notin K$ can be defined as $u = u(x)$, which satisfies $F(x)^G = F(u)$.

Proof. The first statement has been solved above, and the second statement is also a direct corollary of theorem **??**'s proof, since now the elementary symmetry polynomials of $\sigma_i(x)$ are the coefficients of the minimal polynomial of x over $E = K(u)$. At last, as for $F(x)^G = F(u)$, since G is a finite subgroup of $\mathrm{Aut}(K(x))$, then $K(x)/K(x)^G$ is Galois with Galois group $Gal(K(x)/(K(x)^G)) = G$, hence $F(x)^G = F(u)$ which is directly from Artin's Theorem. □

We would like to give some examples. First of all, let us consider a simple case, that $\mathrm{Gal}(K(x)/E) = G = \{x \mapsto x, x \mapsto 1 - x\} := \{1, \sigma\}$, then the minimal polynomial of x will be $p(t) = (t - x)(t - 1 + x) = t^2 - t + x(1 - x)$, hence $E = K(u) = K(x(1 - x))$. Similarly, we can also find that there exists an isomorphism group of G, say $G' = \{x \mapsto x, x \mapsto 1/x\} =: \{1, \tau\}$, then $K(x)^{G'} = K(x + 1/x)$.

Let us combine these two groups, then we will get a new group from the composition (in fractional linear transformation) of the elements in G and G', i.e.

$$\hat{G} := \langle \sigma, \tau \rangle = \{1, \sigma, \tau, \sigma\tau, \tau\sigma, \tau\sigma\tau = \sigma\tau\sigma\} \cong S_3 \cong D_3.$$

Note that $\sigma, \tau, \sigma\tau\sigma$ are 2-cycles and $\sigma\tau, \tau\sigma$ are 3-cycles. In explicit,

$$\hat{G} = \{x \mapsto x, x \mapsto 1/x, x \mapsto 1 - x, x \mapsto 1/(1 - x), x \mapsto 1 - 1/x, x \mapsto x/(x - 1)\}.$$

Clearly, $\hat{G}$ is a finite subgroup of $\mathrm{PGL}(2, K)$, let $F(v) = F(x)^{\hat{G}}$, then consider the minimal polynomial of x over $F(v)$:

$$p'(t) = (t - x)(t - (1 - x))\left(t - \frac{1}{x}\right)\left(t - \frac{1}{1 - x}\right)\left(t - \left(1 - \frac{1}{x}\right)\right)\left(t - \frac{x}{x - 1}\right)$$

Since the Norm and Trace of x belong to F, we can find one of the nontrivial elementary polynomials of $g_i(x) \in \hat{G}$,

$$\prod_{1 \leq i < j \leq 6} g_i(x)g_j(x) = \frac{(x^2 - x - 1)^3}{x^2(1 - x)^2}.$$

One can find that $\mathrm{ht}(v) = 6 = |\hat{G}| = |D_3|$. This example has been directly showed in Prof. Yu's course for Advanced Galois Theory.

As for more possibilities of the finite subgroup $\mathrm{Gal}(K(x)/K(u))$ of $\mathrm{Aut}(K(x)/K) = \mathrm{PGL}(2, K)$ is known. If K is characteristics 0, then Klein showed that G is either cyclic, dihedral, A_4, S_4 or A_5. If K has characteristic $p > 0$, then Dickson showed that the only other possibilities for G are $\mathrm{PGL}(2, p^n)$,$\mathrm{PSL}(2, p^n)$, and subgroups of the group of upper-triangular matrices in $\mathrm{PGL}(2, p^n)$. Further, for any K, one knows explicitly all subgroups of $\mathrm{Aut}(K(x)/K)$ isomorphic to any of the above groups.

Conclusions

After sorting out the preliminaries for cyclic sextic field, we succeed in finding the integral basis for cyclic sextic field and giving an algorithm for prime decomposition. We also proposed many examples for cyclic cubic and sextic fields as well as some small theorems. On the other hand, using the Galois theory, we have prove two theorems for the Galois extensions over one-variable function field. The existence theorem is also a direct corollary of Lüroth's theorem, and the explicit form given by the second theorem is very useful in finding the automorphism subgroups of a function field.

Appendix A Table of Orbit-length Partition for Small Degree Polynomials

This table can be found in L. Soicher and J. McKay's [**?**] articles.

G	$x_1 + x_2$	$x_1 + x_2 + x_3$	$x_1 - x_2$
Degree 3			
+A_3			3^2
S_3			6
Degree 4			
Z_4	2,4		4^3
+V_4	2^3		4^3
D_4	2,4		4,8
+A_4	6		12
S_4	6		12
Degree 6			
Z_6	$3,6^2$	$2,6^3$	6^5
S_3	$3^3,6$	$2,6^3$	6^5
D_6	$3,6^2$	$2,6,12$	$6,12^2$
+A_4	3,12	$4^2,6^2$	$6,12^2$
G_{18}	6,9	2,18	$6^2,18$
G_{24}	3,12	$6^2,8$	$6,12^2$
+S_4/V_4	3,12	$4^2,12$	6,24
S_4/Z_4	3,12	8,12	6,24
G_{36}^1	6,9	2,18	12,18
+G_{36}^2	6,9	2,18	12,18
G_{48}	3,12	8,12	6,24
+PSL$_2(5)$	15	10^2	30
G_{72}	6,9	2,18	12,18
PGL$_2(5)$	15	20	30
+A_6	15	20	30
S_6	15	20	30

Table A.1: Orbit-length Partition of Polynomial with Degree 3,4,6

where "+" means that the discriminants of the corresponding polynomial is square. Note that we need a non-linear resolvent to determine $PGL_2(5)$ and S_6 etc.

Appendix B Resultant and Discriminant of a Polynomial

We begin with some useful definitions regarding polynomials. The reason why we refer resultant is that we can calculate the discriminant of the polynomial through this tool, especially when the degree of polynomial is large. First of all, we give a definition of resultant[**?**]:

Definition B.0.1. *Let R be an integral domain, given two polynomials $f(x), g(x) \in R[x]$ with roots $\alpha_1, \dots, \alpha_m$ and $\beta_1, \dots, \beta_n$ respectively, then the resultant* $\operatorname{Res}(f, g)$ *of f, g is defined to be*

$$\operatorname{Res}(f, g) = l(f)^n l(g)^m \prod_{i,j} (\alpha_i - \beta_j)$$

which is equivalent to both

$$\operatorname{Res}(f, g) = l(f)^n \prod_{i}^{m} g(\alpha_i)$$

and

$$\operatorname{Res}(f, g) = (-1)^{nm} l(g)^m \prod_{i}^{n} f(\beta_i)$$

From this definition, on can easily see that f, g have a common root in some if and only if $\operatorname{Res}(f, g) = 0$. An important proposition shows the relationship of this definition to the **Sylvester's matrix** (Some books take that as definition): Let S be the Sylvester's matrix of polynomials $f(x)$ and $g(x)$, then $\operatorname{Res}(f, g) = \det(S)$.

Also for convenience, I choose a definition of normalized discriminant [**?**] of polynomial as follows in this paper.

Definition B.0.2. *Let f be a polynomial of degree $n \geq 1$ with coefficients in a field F. Let F_1 be an extension of F where f splits, and let $r_1, \dots, r_n$ be the roots of f in F_1. Then the discriminant of f is*

$$\operatorname{Disc}(f) := \prod_{1 \leq i < j \leq n} (r_i - r_j)^2$$

Note further that $\operatorname{Disc}(cf) = \operatorname{Disc}(f)$ for any nonzero constant. The following theorem give the relation between the discriminant and resultant.

Proposition B.0.1. *Let $f = a_n x^n + \cdots + a_0$ be polynomial of degree $n \geq 1$ with coefficients in a field F. The the discriminant of f is given by*

$$\operatorname{Disc}(f) = (-1)^{n(n-1)/2} a_n^{-(2n-1)} \operatorname{Res}(f, f')$$

Example B.0.1. *Let $f(x) = x^n + px + q$ for $n \geq 2$, then $f'(x) = nx^{n-1} + p$, then from the Proposition* **??**, *we have*

$$\operatorname{Disc}(f) = (-1)^{(n-1)(n-2)/2} (n-1)^{n-1p^n} + (-1)^{n(n-1/2)} n^n q^{n-1}$$

Appendix C The Legendre-Jacobi-Kronecker Symbol

All the symbols with the form $\left(\frac{a}{b}\right)$ I used in the paper are Kronecker Symbols. But first, let us review the definition and some properties of Legendre symbol.

C.1 The Legendre Symbol

In number theory, the Legendre symbol is a multiplicative function with values 1,-1,0 that is a quadratic character modulo an **odd** prime number p: its value on a (nonzero) quadratic residue mod p is 1 and on a non-quadratic residue (non-residue) is -1. Its value on zero is 0. Furthermore, one can easily show that this symbol has the following properties:

Proposition C.1.1. *1. The Legendre symbol is periodic, if $a \equiv b(mod\, p)$, then*

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

2. The Legendre symbol is multiplicative, i.e.

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

3. We have the congruence $a^{(p-1)/2} \equiv \left(\frac{a}{p}\right)$ $(mod\, p)$.

4. There are as many quadratic residues as non-residues mod p, say $(p-1)/2$.

5. Let p be an odd prime, then

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

6. Let p, q be two different odd primes, then we have reciprocity law:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}$$

C.2 The Kronecker Symbol

Now we extend the definition of the Legendre symbol [**?**].

Definition C.2.1. *we define the Kronecker (or Kronecker-Jacobi) symbol $\left(\frac{a}{b}\right)$ for any a and b in $\mathbb{Z}$ as follows:*

1. If $b = 0$, then $\left(\frac{a}{0}\right) = 1$ if $a = \pm 1$, and is equal to 0 otherwise.

2. *For $b \neq 0$, firstly $\left(\frac{a}{1}\right) = 1$. For other case write $b = \prod p$, where p are not necessarily distinct primes (including $p = 2$), or $p = -1$ to take care of sign. The we set*

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

where $\left(\frac{a}{p}\right)$ is the Legendre symbol defined above for $p > 2$, and where $p = 2$ we define:

$$\left(\frac{a}{2}\right) = \begin{cases} 0, & \text{if } a \text{ is even} \\ (-1)^{(a^2-1)/8}, & \text{if } a \text{ is odd.} \end{cases}$$

and also

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

Also the Kronecker symbol has the following simple properties:

Proposition C.2.1. *1. $\left(\frac{a}{b}\right) = 0$ iff $(a, b) \neq 1$*

2. *for all a, b, c, if $bc \neq 0$, we have*

$$\left(\frac{ab}{c}\right) = \left(\frac{a}{c}\right)\left(\frac{b}{c}\right), \left(\frac{a}{bc}\right) = \left(\frac{a}{b}\right)\left(\frac{a}{c}\right)$$

Acknowledgements

This thesis is the result of many years of study whereby I have been accompanied and supported by many people. It is a pleasure to convey my gratitude to all of them in my humble acknowledgement.

I want to give my sincerely thanks to my graduation designation supervisor Prof. Jingzhi Li for his earnest guidance and great help during my undergraduate study at SUSTC.

I would especially like to recognize my academic supervisors, Prof. Xianke Zhang and Prof. Jietai Yu, who have always given me encouragements and confidence in myself. They have played important roles in my decision to continue my education and inspired me for what I could achieve in the future. During the preparation of the thesis, we had many fruitful discussion. They have given me so many advises on the details of the thesis, including the tentative methods and writing techniques etc.

I am very grateful for all the encouragement I have received from my family and from a network of friends. I would also like to thank my wonderful committee of professors. The committee members Prof. Xianke Zhang, Prof. Jingzhi Li, Prof. Anyue Chen, Prof. Xuejun Jiang and Prof. Linlin Su, who have contributed to the completion of this thesis through their guidance and exceptional teaching, which have helped me get through my education this far.

Finally, I'd like to say thanks to all my teachers in SUSTC, especially teachers in the Department of Financial Mathematics for providing a stimulating environment. I am very grateful for all the encouragement I have received from my family and from a network of friends.

Wenchao Zhang
September,2014