MONOGENIC NUMBER FIELDS

by

Pınar Değirmenci

B.S., Mathematics, Ege University, 2015

Submitted to the Institute for Graduate Studies in
Science and Engineering in partial fulfillment of
the requirements for the degree of
Master of Science

Graduate Program in Mathematics

Boğaziçi University

2022

ACKNOWLEDGEMENTS

I would like to thank everyone who directly or indirectly influenced and contributed to this thesis.

My special thanks go to my supervisor, Ekin Özman who so generously took time out of her schedule to improve my research and make this project possible. I am also grateful for her patience, guidance, and support. I have benefited greatly from her wealth of knowledge and meticulous editing. I am extremely grateful that she took me on as a student and continued to have faith in me over the years.

I want to thank my committee member, Yasemin Kara. Her encouraging words and thoughtful, detailed feedback has been very important to me.

I owe my deepest gratitude to Erman Işık. I am forever thankful for the unconditional love and support throughout the entire thesis process and every day.

Most importantly, I am grateful for my mum and sister's unconditional, unequivocal, and loving support.

ABSTRACT

MONOGENIC NUMBER FIELDS

Determining whether the ring of integers $\mathcal{O}_K$ of an algebraic number field K of degree n admits a power integral basis is one of the classic problems in algebraic number theory. In other words, we want to determine whether there exists $\alpha \in \mathcal{O}_K$ such that $\{1, \alpha, \ldots, \alpha^{n-1}\}$ is a $\mathbb{Q}$-basis for K. This question dates back to the 1960s and was introduced by a German mathematician, Helmut Hasse.

In this thesis, we will study the monogenicity of cubic number fields and their lift to monogenic sextic number fields. After recalling some background material on algebraic number theory and related topics, we will focus on specific cubic fields such as pure cubic fields and cyclic cubic fields. Next, we will study the lifting of all monogenic cyclic cubic fields to monogenic sextic fields.

This thesis was supported by Boğaziçi University Research Fund Grant Number 19082.

ÖZET

MONOJENİK SAYI CİSİMLERİ

n dereceli bir cebirsel sayı cismi K'nın, $\mathcal{O}_K$ tam sayılar halkasının bir kuvvet integral bazı kabul edip etmediğini belirlemek cebirsel sayı teorisindeki klasik problemlerden biridir. Diğer bir deyişle, $\{1, \alpha, \ldots, \alpha^{n-1}\}$, K için $\mathbb{Q}$-bazı olacak şekilde $\alpha \in \mathcal{O}_K$ olup olmadığını belirlemek istiyoruz. 1960'lara kadar uzanan bu soru Alman matematikçi Helmut Hasse tarafından tanıtıldı.

Bu tezde, kübik sayı cisimlerinin monojenikliğini ve bunların monojenik sekstik sayı cisimlerine yükselişini inceleyeceğiz. Cebirsel sayı teorisi ve bağlantılı konular hakkında bazı arka plan materyallerini hatırladıktan sonra, saf kübik cisimler ve döngüsel kübik cisimler gibi belirli kübik cisimlere odaklanacağız. Daha sonra, tüm monojenik döngüsel kübik cisimlerin monojenik sekstik cisimlere yükselişini inceleyeceğiz.

Bu tez Boğaziçi Üniversitesi Bilimsel Araştırma Projeleri tarafından 19082 kodu ile desteklenmiştir.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF SYMBOLS

$\mathbb{Z}$	Set of integers
$\mathbb{Q}$	Set of rationals
$\mathbb{C}$	Set of complex numbers
K,L, ...	Number fields
$D(f)$	Discriminant of the polynomial $f(x)$
$N_{K/\mathbb{Q}}(\alpha)$	Norm of $\alpha \in K$ over $\mathbb{Q}$
$\mathrm{Tr}_{K/\mathbb{Q}}(\alpha)$	Trace of $\alpha \in K$ over $\mathbb{Q}$
$[K : \mathbb{Q}]$	Degree of K over $\mathbb{Q}$
$\mathrm{Gal}(K/\mathbb{Q})$	Galois group of K over $\mathbb{Q}$
$\mathrm{Gal}(f)$	Galois group of the splitting field of $f(x) \in \mathbb{Z}[x]$
S_n	Symmetric group of order $n!$
C_n	Cyclic group of order n
D_n	Dihedral group of order $2n$
A_n	Alternating group of order $n!/2$
$\mathcal{O}_K$	Ring of integers in the number field K
$\mathcal{O}_K^\times$	Group of units in the number field K
$\mathbb{Z}[x]$	Ring of polynomials in x with integral coefficients
$\mathbb{Z}[\alpha]$	$\mathbb{Z}$-module generated by α
D_K	Field discriminant of the field K
$D_{K/\mathbb{Q}}(\omega_1, \ldots, \omega_n)$	Discriminant of algebraic numbers $\omega_1, \ldots, \omega_n$
$I(\alpha)$	Index of α
$\mu(K)$	Field index of K
$m(K)$	Minimal index of K
$I(x_2, \ldots, x_n)$	Index form equation of $\{x_1, x_2, \ldots, x_n\}$
α, β, γ	Algebraic numbers

1. INTRODUCTION

Let K be a number field of degree n with the integer ring $\mathcal{O}_K$. If $\alpha \in K$ is a primitive element then we have $K = \mathbb{Q}(\alpha)$, i.e. $\{1, \alpha, \ldots, \alpha^{n-1}\}$ is a $\mathbb{Q}$-basis for K. It is also known that every algebraic number field has an integral basis. It is a classical problem in algebraic number theory to determine whether a given number field K satisfies the previous two properties; in other words, whether there exists $\alpha \in \mathcal{O}_K$ such that $\{1, \alpha, \ldots, \alpha^{n-1}\}$ is a $\mathbb{Q}$-basis for K. Such an integral basis is called a *power integral basis*. If a number field admits a power integral basis, it is called a *monogenic* number field. For example, quadratic fields and cyclotomic fields are monogenic number fields.

In the 1960's, Hasse [1, §25.6] asked to give an arithmetic characterization of algebraic number fields with power integral bases. The first example of a number field that does not admit a power integral basis was provided by Dedekind in [2]. Since then, many mathematicians have been trying to find an answer to the following questions: Which fields are monogenic and if a number field is monogenic, can we list all the generators? Although there are some partial solutions, both questions are still open for all number fields.

The main purpose of this master thesis is to study the monogenity of cubic number fields and their lift to monogenic sextic number fields.

In Chapter 2, we cover some background materials and preliminary results of algebraic number theory and related topics. It includes the basic definitions and theorems such as algebraic integers, discriminant and integral basis. We also describe the structure of the discriminant form, index form and their relations. The main observation of this chapter, which is a result of Proposition 2.32, is the following: Let $\mathcal{O}$ be a $\mathbb{Z}$-order in K with a fixed $\mathbb{Z}$-basis $\{1, \omega_2, \ldots, \omega_n\}$ and $\alpha = x_1 + x_2\omega_2 + \cdots + x_n\omega_n$. Then $\alpha \in \mathcal{O}$ generates a power basis for $\mathcal{O}$ if and only if $(x_2, \ldots, x_n) \in \mathbb{Z}^{n-1}$ satisfies

the index form equation

$$I(x_2, \ldots, x_n) = \pm 1 \text{ in } x_2, \ldots, x_n \in \mathbb{Z}. \tag{1}$$

Chapter 3 is devoted to the collections of some results regarding the monogenic cubic fields. The first section of this chapter includes a summary of results on monogenity of arbitrary cubic number fields with discriminant lying in the interval $[-300, 3137]$. In the following section, we give an alternative characterization of a monogenic cyclic cubic field in terms of Shank's cubic polynomial. This observation will also lead us to list some equivalent conditions for cyclic cubic fields which has a power integral basis. In the next section, we give an integral basis and the index form equation $I(x, y) = \pm 1$ attached to a pure cubic field $\mathbb{Q}(\sqrt[3]{m})$ for some $m \in \mathbb{Z}$ to determine its monogenity. For instance, if $m = r + 9k$ is square-free for some $k \in \mathbb{Z}$ and $r \in \{2, 3, 4, 5, 6, 7\}$, we conclude that the field $\mathbb{Q}(\sqrt[3]{m})$ has a power integral basis. In the last section of this chapter, we will show that there exist infinitely many triples of polynomials defining distinct monogenic cubic fields with the same discriminant.

Chapter 4 is concerned with the notion of lifting of monogenic cubic fields to monogenic sextic fields. For a sextic field containing a cubic subfield, there are eight possibilities for the Galois group of its Galois closure. For five of these Galois groups, we will provide infinitely many monogenic sextic fields that can be lifted form a monogenic cubic field. For the remaining three Galois groups, we show that there are at most finitely many monogenic sextic field. Both results are based on the work of Lavallee *et al.* in [3].

In Chapter 5, we mention our observation in regards to lifting of the monogenic cubic fields to monogenic sextic fields. The main result of this chapter is a combination of Theorem 3.4 and Lemma 4.4. In Theorem 4.2, the authors of [3] deal with only certain type of polynomials which are given in Table 4.1 and the ones of the form $g(x) = x^3 + ax^2 + bx \pm 1$ defined by finitely many integers a and b. Our observation extends their result to all monogenic cyclic cubic number fields.

2. BASIC CONCEPTS OF ALGEBRAIC NUMBER THEORY

2.1. Number Fields and Algebraic Integers

In this section, we will state some basic facts regarding number fields. The main references for this section are [4, § 13] and [5].

Let K be a field. A *field extension* L of K is a field $L \supset K$ with finite dimension $\dim_K(L)$ (as a vector space over K), and the *degree* of the extension L/K is defined to be $[L : K] := \dim_K(L)$. In particular, if L is such an extension of $\mathbb{Q}$, then it is called a *number field*.

Let L/K be a field extension of degree n, and let $\alpha \in L$. Then there must be a K-linear dependency among $\{1, \alpha, \ldots, \alpha^n\}$. In other words, there exists a polynomial $f(x) \in K[x]$ of degree n such that $f(\alpha) = 0$. Such an element $\alpha \in L$ is called *algebraic* over K. Let L/K be a field extension and $\alpha \in L$ be an algebraic element of L over K. Then α has a minimal polynomial over K; namely, there exists a unique $m_\alpha(x) \in K[x]$ such that if $f(x) \in K[x]$ satisfying $f(\alpha) = 0$, then $m_\alpha(x)$ divides $f(x)$. Here uniqueness means up to multiplication by an element of $K - \{0\}$.

Let K be a number field. An element $\alpha \in K$ is called an *algebraic integer* if it is a root of a monic polynomial $f(x) \in \mathbb{Z}[x]$.

We now have the concept of an algebraic integer in a number field. It is natural to ask whether one can determine the set of all algebraic integers in a number field. Let us first consider all algebraic integers in $\mathbb{C}$. The following theorem gives us alternative characterizations of algebraic integers.

Theorem 2.1. *The following statements are equivalent for $\alpha \in \mathbb{C}$:*

(i) α *is an algebraic integer;*
(ii) $\mathbb{Z}[\alpha]$ *is a finitely generated* $\mathbb{Z}$*-module;*
(iii) There exists a subring of $\mathbb{C}$ *containing* α *which is finitely generated;*
(iv) There exists a finitely generated non-zero $\mathbb{Z}$*-module* $M \subset \mathbb{C}$ *such that* $\alpha M \subset M$*.*

Proof. See [5, Chapter 2 Theorem 2]. □

Hence, one can deduce that the set of algebraic integers is closed under addition and multiplication.

Corollary 2.2. *Let A denote the set of algebraic integers in $\mathbb{C}$. Then A forms a ring.*

Proof. Let α and β be elements of A. It then follows from Theorem 2.1 that $\mathbb{Z}[\alpha]$ and $\mathbb{Z}[\beta]$ are finitely generated $\mathbb{Z}$-modules. Then so is $\mathbb{Z}[\alpha, \beta]$.

Since $\mathbb{Z}[\alpha, \beta]$ contains $\alpha\beta$ and $\alpha + \beta$, by Theorem 2.1 (iii), we deduce that $\alpha\beta$ and $\alpha + \beta$ are algebraic integers. □

We now go back to the set of algebraic integers in a number field. Let K be a number field and let $\mathcal{O}_K$ denote the set of algebraic integers in K, i.e. $\mathcal{O}_K = A \cap K$. One can deduce from Corollary 2.2 that $\mathcal{O}_K$ is a ring, which is called the *ring of integers of* K.

The following theorem states a relation between algebraic numbers and algebraic integers.

Theorem 2.3. *Let K be a number field and $\alpha \in K$. Then α can be written as β/d with $\beta \in \mathcal{O}_K$ and $d \in \mathbb{Z}$. Hence, K is the field of fractions of $\mathcal{O}_K$.*

Proof. Since α is algebraic over $\mathbb{Q}$ it satisfies an equation $\alpha^n + a_1\alpha^{n-1} + \cdots + a_n = 0$ where $a_i \in \mathbb{Q}$. Let d be a common denominator for the a_i, so $da_i \in \mathbb{Z}$ for all $i \in \{1, \ldots, n\}$. Multiplying through the equation by d^n we get

$$(d\alpha)^n + a_1 d(d\alpha)^{n-1} + \cdots + a_n d^n = 0.$$

It follows that $d\alpha \in \mathcal{O}_K$. □

The following theorem gives us a criteria for an algebraic element to be an algebraic integer.

Theorem 2.4. *Let α be an algebraic integer. Let $f(x) \in \mathbb{Z}[x]$ be a monic polynomial of least degree such that $f(\alpha) = 0$. Then $f(x)$ is irreducible over $\mathbb{Q}$.*

Proof. See [5, Chapter 2, Theorem 1] □

Corollary 2.5. *The number α is an algebraic integer if and only if the monic minimal polynomial of α over $\mathbb{Q}$ has coefficients in $\mathbb{Z}$.*

Proof. See [5, Chapter 1, Proposition1.1] □

The Primitive Element theorem says that for a given number field K we have $K = \mathbb{Q}(\alpha)$ for some $\alpha \in K$. Hence, it is natural to ask whether one can write the ring of integers $\mathcal{O}_K$ as $\mathcal{O}_K = \mathbb{Z}[\alpha]$ for some $\alpha \in \mathcal{O}_K$.

2.1.1. Discriminant, Norm and Trace

In this section, we will define three important functions $\mathrm{Tr}_{K/\mathbb{Q}}$, $N_{K/\mathbb{Q}}$, and D_K the *trace*, the *norm* and the *discriminant of an n-tuple* attached to a number field K. The main reference for this section is [5].

An *embedding* of a number field K into $\mathbb{C}$ is an injective $\mathbb{Q}$-homomorphism of K into $\mathbb{C}$. For a given number field K of degree n there are precisely n distinct embeddings of K into $\mathbb{C}$ (see [5, Appendix B]). By applying the Primitive Element theorem we can write $K = \mathbb{Q}(\alpha)$ for some $\alpha \in K$. Then, the embeddings can be described easily by observing that each embedding sends α to one of its n-conjugates over $\mathbb{Q}$. On the other hand, each conjugate β determines a unique embedding of K.

Definition 2.6. *Let K be a number field. We define two functions $\mathrm{Tr}_{K/\mathbb{Q}}$ and $N_{K/\mathbb{Q}}$ (the trace and the norm) on K, as follows: Let $\sigma_1, \ldots, \sigma_n$ denote the embeddings of K in $\mathbb{C}$, where $n = [K : \mathbb{Q}]$. For each $\alpha \in K$, set*

$$\begin{aligned} \mathrm{Tr}_{K/\mathbb{Q}}(\alpha) &:= \sum_{i=1}^{n} \sigma_i(\alpha) \\ N_{K/\mathbb{Q}}(\alpha) &:= \prod_{i=1}^{n} \sigma_i(\alpha). \end{aligned} \tag{1}$$

It is easy to see that $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha + \beta) = \mathrm{Tr}_{K/\mathbb{Q}}(\alpha) + \mathrm{Tr}_{K/\mathbb{Q}}(\beta)$ and $N_{K/\mathbb{Q}}(\alpha\beta) = N_{K/\mathbb{Q}}(\alpha)N_{K/\mathbb{Q}}(\beta)$. Moreover, for $r \in \mathbb{Q}$ and $\alpha \in K$, we have $\mathrm{Tr}_{K/\mathbb{Q}}(r\alpha) = r\mathrm{Tr}_{K/\mathbb{Q}}(\alpha)$ and $N_{K/\mathbb{Q}}(r\alpha) = r^n N_{K/\mathbb{Q}}(\alpha)$.

Proposition 2.7. *Let K be a number field of degree n and let $\alpha \in K$. Then*

$$\begin{aligned} \mathrm{Tr}_{K/\mathbb{Q}}(\alpha) &= \frac{n}{d}\mathrm{Tr}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha) \\ N_{K/\mathbb{Q}}(\alpha) &= (\mathrm{N}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha))^{\frac{n}{d}}, \end{aligned} \tag{2}$$

where $d = [\mathbb{Q}(\alpha) : \mathbb{Q}]$, meaning that $d|n$.

Proof. See [5, Chapter 2, Theorem 4]. □

Corollary 2.8. *Let K be a number field and $\alpha \in K$. Then we have the following:*

(i) $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha)$, $N_{K/\mathbb{Q}}(\alpha) \in \mathbb{Q}$.

(ii) If α is an algebraic integer, then $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha)$, $N_{K/\mathbb{Q}}(\alpha) \in \mathbb{Z}$.

Proof. For (i), see [5, Chapter 2, Corollary 1]. If α is an algebraic integer, its minimal polynomial over $\mathbb{Q}$ has coefficients in $\mathbb{Z}$. Hence, we obtain (ii). □

Example 2.9. *Let m be a square-free integer, and let $K = \mathbb{Q}(\sqrt{m})$ be a quadratic field. Then we have*

$$\begin{aligned} \mathrm{Tr}_{K/\mathbb{Q}}(a + b\sqrt{m}) &= 2a, \\ N_{K/\mathbb{Q}}(a + b\sqrt{m}) &= a^2 - mb^2. \end{aligned} \tag{3}$$

for $a, b \in \mathbb{Q}$.

2.1.2. The Discriminant of an n-tuple

Let K be an algebraic number field of degree n with the ring of integers $\mathcal{O}_K$ and let $\sigma_1, \sigma_2, \ldots, \sigma_n : K \hookrightarrow \mathbb{C}$ be all the embeddings of K into $\mathbb{C}$. For any n-tuple $\alpha_1, \alpha_2, \ldots, \alpha_n$, we define the *discriminant* of $\alpha_1, \alpha_2, \ldots, \alpha_n$ as

$$D_{K/\mathbb{Q}}(\alpha_1, \alpha_2, \ldots, \alpha_n) := \left|\sigma_i(\alpha_j)\right|^2, \tag{4}$$

namely, it is defined as the square of the determinant of the matrix having $\sigma_i(\alpha_j)$ in the (i, j)-th entry. Here, $|a_{ij}|$ denotes the determinant of the matrix $[a_{ij}]$ with a_{ij} in the i-th row and j-th column.

One can observe that the square makes the discriminant independent of the ordering of the σ_i and the ordering of the α_j.

Proposition 2.10. *The set* $\{\alpha_1, \ldots, \alpha_n\}$ *is a basis for* K *over* $\mathbb{Q}$ *if and only if we have* $D_{K/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n) \neq 0$.

Proof. See [6, Proposition 3.24]. □

The following theorem help us express the discriminant in terms of the trace $\mathrm{Tr}_{K/\mathbb{Q}}$.

Theorem 2.11. *We have* $D_{K/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n) = \left|\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_i\alpha_j)\right|$.

Proof. The result follows immediately from the matrix equation

$$[\sigma_j(\alpha_i)][\sigma_i(\alpha_j)] = [\sigma_1(\alpha_i\alpha_j) + \cdots + \sigma_n(\alpha_i\alpha_j)] = [\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_i\alpha_j)] \tag{5}$$

and the properties of the determinant: $|a_{ij}| = |a_{ji}|$ and $|AB| = |A||B|$ for matrices A and B. □

We can utilize the discriminant to determine whether the α_j are linearly independent:

Proposition 2.12. *If* $\alpha_1, \ldots, \alpha_n \in K$ *where* $\alpha_i's$ *are algebraic integers, then we have:*

(i) $D_{K/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}$

(ii) If $\beta_1, \ldots, \beta_n \in K$ *such that* $\beta_i = \sum_{j=1}^{n} a_{ij}\alpha_j$ *with* $a_{ij} \in \mathbb{Q}$ *for* $i = 1, 2, \ldots, n$, *then*

$$D_{K/\mathbb{Q}}(\beta_1, \ldots, \beta_n) = \left|a_{ij}\right|^2 \cdot D_{K/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n) \tag{6}$$

(iii) $D_{K/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n) = 0$ *if and only if* $\alpha_1, \ldots, \alpha_n$ *form a linearly dependent system over* $\mathbb{Q}$.

Proof. See [5, Chapter 2, Corollary 6 and Theorem 7]. □

For simplicity, we will denote the discriminant of the n-tuple $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ by $D_{K/\mathbb{Q}}(\alpha)$. The following theorem relates $D_{K/\mathbb{Q}}(\alpha)$ to the norm of $f'(\alpha)$:

Theorem 2.13. *Suppose that $K = \mathbb{Q}(\alpha)$ for some $\alpha \in K$, and that $\alpha_1, \ldots, \alpha_n$ denote the conjugates of α over $\mathbb{Q}$. Then*

$$D_{K/\mathbb{Q}}(\alpha) = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2 = \pm N_{K/\mathbb{Q}}(f'(\alpha)) \tag{7}$$

where f is the monic irreducible polynomial for α over $\mathbb{Q}$: the $+$ sign holds if and only if $n \equiv 0$ or $1 \pmod 4$.

Proof. See [5, Chapter 2, Theorem 8]. □

2.1.3. Norm of an Ideal and Fractional Ideals

In this section, we will define a norm of and ideal and the set of fractional ideals. These notions will be used in Chapter 3.

Definition 2.14. *Let K be a number field with ring of integers $\mathcal{O}_K$ and let $\mathfrak{U}$ be a non-zero ideal of $\mathcal{O}_K$, we define the norm of $\mathfrak{U}$ as*

$$N_{K/\mathbb{Q}}(\mathfrak{U}) := |\mathcal{O}_K/\mathfrak{U}|. \tag{8}$$

Lemma 2.15. *Let $\mathfrak{U}$ be a non-zero ideal of $\mathcal{O}_K$.*

(i) We have $N_{K/\mathbb{Q}}(\alpha\mathcal{O}_K) = |N_{K/\mathbb{Q}}(\alpha)|$ for all $\alpha \in \mathcal{O}_K$.
(ii) The norm of $\mathfrak{U}$ is finite.

Proof. See [6, Lemma 5.20 and 5.35]. □

Definition 2.16. *Let L/K be a cyclic Galois extension with Galois group $G =< \sigma >$. An ideal $\mathfrak{U}$ of L is called an ambiguous ideal if $\mathfrak{U}^\sigma = \mathfrak{U}$.*

Definition 2.17. *An $\mathcal{O}_K$-submodule $\mathfrak{f}$ of K is called a fractional ideal of $\mathcal{O}_K$ if there exists some non-zero $\alpha \in \mathcal{O}_K$ such that $\alpha\mathfrak{f} \subset \mathcal{O}_K$, that is, $\mathfrak{U} = \alpha\mathfrak{f}$ is an ideal of $\mathcal{O}_K$ and $\mathfrak{f} = \alpha^{-1}\mathfrak{U}$.*

Lemma 2.18. *Let $\mathfrak{p}$ be a non- zero prime ideal of $\mathcal{O}_K$. Define*

$$\mathfrak{p}^{-1} := \{x \in K \mid x\mathfrak{p} \subset \mathcal{O}_K\}. \tag{9}$$

(i) $\mathfrak{p}^{-1}$ *is a fractional ideal of* $\mathcal{O}_K$.
(ii) $\mathcal{O}_K \subsetneq \mathfrak{p}^{-1}$.
(iii) $\mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}_K$.

Proof. See [6, Lemma 5.25, 5.26 and 5.29] □

Theorem 2.19. *The non-zero fractional ideals of a number field K form a multiplicative group, denoted I_K.*

Proof. See [6, Theorem 5.30] □

Note that the set of principal fractional ideals form a subgroup of I_K and denoted by P_K.

2.1.4. The Dirichlet's Unit Theorem

The Dirichlet unit theorem says that the group of units modulo the subgroup of roots of unity in the field is a finitely generated group with $r_1 + r_2 - 1$ generators, where r_1 denotes the number of real embeddings and the number of pairs of complex conjugate embeddings are denoted by r_2 for the field. Let K be an algebraic number field of degree n with the ring of integers $\mathcal{O}_K$. Let $\mathcal{O}_K^\times$ denote the group of units of $\mathcal{O}_K$.

It then follows from the Dirichlet's unit theorem (see [7, Page 119]) that we have

$$\mathcal{O}_K^{\times} = \mu(K) \times \mathbb{Z}^r,\ r = r_1 + r_2 - 1, \tag{10}$$

where $\mu(K)$ is the group of roots of unity in K and $n = [K : \mathbb{Q}] = r_1 + 2r_2$. It is easy to see that $r = r_1 + r_2 - 1 = 0$ if and only if $r_1 = 1,\ r_2 = 0$, then $K = \mathbb{Q}$ or $r_1 = 0,\ r_2 = 1$, then $K = \mathbb{Q}(\sqrt{m})$, $m \leq 0$. In these cases, $\mathcal{O}_K^{\times}$ coincides with a finite group $\mu(K)$. On the other hand, if $K/\mathbb{Q}$ is a Galois extension, we have K is real if and only if $r_1 = n,\ r_2 = 0,\ r = n - 1$, and K is imaginary if and only if $r_1 = 0,\ r_2 = n/2,\ r = n/2 - 1$. In case of quadratic fields this number is 0 or 1 depending on whether the field is real or imaginary.

2.2. Integral Basis and Monogenity

The main references for this section are [5, Chapter 2] and [8, Chapter 1]. Let K be a number field of degree n with the ring of integers $\mathcal{O}_K$. A set $\{\alpha_1, \ldots, \alpha_n\} \subset \mathcal{O}_K$ which is linearly independent over $\mathbb{Q}$ and generates $\mathcal{O}_K$ as a $\mathbb{Z}$-module is called an *integral basis* of K.

Note that an integral basis for a number field always exists. Indeed, observe that it follows from Theorem 2.3 that for every element $\alpha \in K$ there is an integer $d \in \mathbb{Z}$ such that $d\alpha \in \mathcal{O}_K$; hence, by modifying any $\mathbb{Q}$-basis for K a basis consisting of algebraic integers can be obtained.

Let us now fix a basis $\{\alpha_1, \ldots, \alpha_n\} \subset \mathcal{O}_K$ for K over $\mathbb{Q}$. Then we obtain a free abelian group of rank n lying inside $\mathcal{O}_K$, i.e.

$$A := \{a_1\alpha_1 + \cdots + a_n\alpha_n : a_i \in \mathbb{Z}\} \subset \mathcal{O}_K. \tag{11}$$

Theorem 2.20. *Let $\{\alpha_1, \ldots, \alpha_n\}$ be a basis of K over $\mathbb{Q}$ consisting entirely of algebraic integers, and set $d := D_{K/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n)$. Then every element $\alpha \in \mathcal{O}_K$ can be expressed in the form*

$$\frac{m_1\alpha_1 + \cdots + m_n\alpha_n}{d} \tag{12}$$

with all $m_i \in \mathbb{Z}$ where $i \in \{1, \ldots, n\}$ and all m_i^2 divisible by d.

Proof. See [5, Chapter 2, Theorem 9] . □

Hence, $\mathcal{O}_K$ contains, and is contained in the free abelian groups of rank n (A and $\frac{1}{d}A$), which imply that it has a basis over $\mathbb{Z}$.

Example 2.21. *Let $K = \mathbb{Q}(\sqrt{m})$, where m is a square-free integer. Then $\{1, \alpha\}$ is an integral basis of K, where*

$$\alpha = \begin{cases} \dfrac{1+\sqrt{m}}{2}, & \text{if } m \equiv 1 \pmod 4 \\ \sqrt{m}, & \text{if } m \equiv 2, 3 \pmod 4. \end{cases} \tag{13}$$

As we have seen in Example 2.21, the ring of integers of a quadratic number field can be written as $\mathbb{Z}[\alpha]$ for some α. This observation leads us to the following definition:

Definition 2.22. *Let K be a number field with the ring of integers $\mathcal{O}_K$. The field K is called monogenic if its ring of integers $\mathcal{O}_K$ is a simple ring extension $\mathbb{Z}[\alpha]$ of $\mathbb{Z}$. Namely, $\{1, \alpha, \ldots, \alpha^{n-1}\}$ is an integral basis of $\mathcal{O}_K$. We call the set $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ a power integral basis.*

Note that if the sets $\{\alpha_1, , \ldots, \alpha_n\}$ and $\{\alpha_1', , \ldots, \alpha_n'\}$ are two integral bases for K over $\mathbb{Q}$ then $D_{K/\mathbb{Q}}(\alpha_1, , \ldots, \alpha_n) = D_{K/\mathbb{Q}}(\alpha_1', , \ldots, \alpha_n')$ (see [6, Proposition 3.28]). We now define an important invariant attached to a number field K, which is independent from the choice of integral bases.

Definition 2.23. *Let K be a number field of degree n and $\{\alpha_1, \ldots, \alpha_n\}$ be an integral basis for K over $\mathbb{Q}$. The discriminant of K is the discriminant $D_{K/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n)$ of the integral basis. Hence, we denote it by D_K.*

The discriminant plays an integral role in determining whether a given number field K is monogenic.

Theorem 2.24. *[Discriminant Test] Let $K = \mathbb{Q}(\alpha)$ be a number field and let $f(x)$ denote the minimal polynomial of α over $\mathbb{Q}$ and $\mathrm{disc}(f)$ denote discriminant of the polynomial $f(x)$. If $\mathrm{disc}(f) = D_K$, then K is monogenic.*

Proof. We know that the discriminant of $f(x)$ is equal to $D_{K/\mathbb{Q}}(\alpha)$, where α is a root of $f(x)$. We also know that $\mathcal{O}_K$ contains α, and therefore contains $\mathbb{Z}[\alpha]$.

We now have that $D_{K/\mathbb{Q}}(\alpha) = D_K \cdot [\mathcal{O}_K : \mathbb{Z}[\alpha]]^2$. Since the discriminants are equal, we have $[\mathcal{O}_K : \mathbb{Z}[\alpha]] = 1$, and therefore the two rings are equal. It then follows that α generates the ring $\mathcal{O}_K$.

□

Example 2.25. *If follows from Example 2.21 that every quadratic field is a monogenic field; hence, there are infinitely many monogenic fields of degree 2.*

For a given integer $n \geq 1$, let $\zeta_n = e^{2\pi i/n} \in \mathbb{C}$; this is a primitive n-th root of unity. Then the n-th *cyclotomic field* is the extension $\mathbb{Q}(\zeta_n)$ of $\mathbb{Q}$ generated by ζ_n. The *degree* of $\mathbb{Q}(\zeta_n)$ is therefore $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \deg(\Phi_n) = \phi(n)$, where ϕ is Euler's totient function and

$$\Phi_n(x) = \prod_{1 \leq k \leq n} (x - \zeta_n^k) \ , \ \gcd(k, n) = 1. \tag{14}$$

The discriminant of $\mathbb{Q}(\zeta_n)$ is

$$(-1)^{\phi(n)/2}\frac{n^{\phi(n)}}{\prod_{p|n} p^{\frac{\phi(n)}{p-1}}}. \tag{15}$$

Here the product is taken over all primes p dividing n.

Theorem 2.26. *Let $K = \mathbb{Q}(\zeta_n)$ be a cyclotomic field, where ζ_n is a primitive n-th root of unity for some integer n. Then K is monogenic, more precisely $\mathcal{O}_K = \mathbb{Z}[\zeta_n]$.*

Proof. See [5, Page 26]. □

2.3. Index Form Equation

In this section, we will state discriminant forms, index forms and their relations. The main references for this section are [8] and [7].

Let K be an algebraic number field of degree n with the ring of integers $\mathcal{O}_K$. Let $\sigma_1, \ldots, \sigma_n$ denote the embeddings of K into $\overline{\mathbb{Q}}$. Recall that the discriminant test allows us to determine whether a given number field is monogenic or not. The following lemma will provide us another important tool.

Lemma 2.27 ([8], Chapter 1, Lemma 1.3)**.** *Let $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_K$ be linearly independent over $\mathbb{Q}$ and set $\mathcal{O} = \mathbb{Z}[\alpha_1, \ldots, \alpha_n]$. Let $\mathcal{O}_K^+$ and $\mathcal{O}^+$ be the additive groups of the corresponding modules and let D_K be the discriminant of the field K. Then*

$$D_{K/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n) = J^2 \cdot D_K, \tag{16}$$

where J denotes the group index

$$J = (\mathcal{O}_K^+ : \mathcal{O}^+). \tag{17}$$

Let $K = \mathbb{Q}(\alpha)$ for some $\alpha \in \mathcal{O}_K$ and let $\mathcal{O} = \mathbb{Z}[1, \alpha, \ldots, \alpha^{n-1}]$. Then we define *index* of α as the index

$$I(\alpha) := (\mathcal{O}_K^+ : \mathbb{Z}[\alpha]^+). \tag{18}$$

In general, if $\alpha \in \mathcal{O}_K$ such that $K = \mathbb{Q}(\alpha)$, then it follows from Lemma 2.27 that we have

$$D_{K/\mathbb{Q}}(\alpha) = I(\alpha)^2 \cdot D_K. \tag{19}$$

More precisely, we can write

$$I(\alpha) = \frac{\sqrt{D_{K/\mathbb{Q}}(\alpha)}}{\sqrt{D_K}} = \frac{1}{\sqrt{D_K}} \prod_{1 \le i < j \le n} |\alpha^{(i)} - \alpha^{(j)}|, \tag{20}$$

where $\alpha^{(i)} := \sigma_i(\alpha)$ denote the conjugates of α for $i \in \{1, \ldots, n\}$. It can easily be seen from (19) and the discriminant test that α generates a power integral basis in K if and only if $I(\alpha) = 1$. The *minimal index* of the field K is defined by

$$\mu(K) := \min I(\alpha), \tag{21}$$

where the minimum is taken over all $\alpha \in \mathcal{O}_K$ such that $K = \mathbb{Q}(\alpha)$. We call such $\alpha \in K$ a *primitive integer*. The *field index* of K is

$$m(K) := \gcd I(\alpha) \tag{22}$$

the greatest common divisor taken for all primitive integers of K as before. Monogenic fields have both $\mu(K) = 1$ and $m(K) = 1$, but $m(K) = 1$ is not sufficient for the monogenity.

Let us fix an integral basis of the form $\{1, \omega_2, \ldots, \omega_n\}$ for K. Let $\sigma_i : K \hookrightarrow \overline{\mathbb{Q}}$, where $i = 1, \ldots, n$ denote the embeddings. Set $X := (X_1, \ldots, X_n)$ and

$$L(X) := X_1 + \omega_2 X_2 + \cdots + \omega_n X_n \tag{23}$$

with conjugates $L^{(i)}(X) = X_1 + \omega_2^{(i)} X_2 + \cdots + \omega_n^{(i)} X_n$ with $i = 1, \ldots, n$. The form $L(X)$ is called the *Fundamentalform*.

Definition 2.28. *We define the discriminant form of K as*

$$D_{K/\mathbb{Q}}(L(X)) := \prod_{1 \le i < j \le n} (L^{(i)}(X) - L^{(j)}(X))^2, \tag{24}$$

which is a form of degree $n(n-1)$ with coefficients in K.

Lemma 2.29. *There exists a homogeneous form $I(X_2, \ldots, X_n)$ in $n-1$ variables of degree $n(n-1)/2$ with integer coefficients such that*

$$D_{K/\mathbb{Q}}(L(X)) = (I(X_2, \ldots, X_n))^2 \cdot D_K, \tag{25}$$

where D_K is the discriminant of the field K.

Proof. Let $L(X) = \omega_2 X_2 + \cdots + \omega_n X_n$ with conjugates $L^{(i)}(X) = \omega_2^{(i)} X_2 + \cdots + \omega_n^{(i)} X_n$. Obviously, there are homogeneous polynomials $F_{ji} \in \mathbb{Z}[X_2, \ldots X_n]$ where $1 \leq j \leq n$ of degree $i-1$ such that

$$(L(X))^{i-1} = F_{1i}(X) + F_{2i}(X)\omega_2 + \cdots + F_{ni}(X)\omega_n \tag{26}$$

holds for $1 \leq j \leq n$. Moreover,

$$\begin{aligned}
D_{K/\mathbb{Q}}(L(X)) &= \prod_{1 \leq i < j \leq n} (L^{(i)}(X) - L^{(j)}(X))^2 \\
&= \prod_{1 \leq i < j \leq n} (L^{(i)}(X) - L^{(j)}(X))^2 \\
&= \begin{vmatrix} 1 & L^{(1)}(X) & \ldots & (L^{(i)}(X))^{n-1} \\ \vdots & \vdots & & \vdots \\ 1 & L^{(in)}(X) & \ldots & (L^{(n)}(X))^{n-1} \end{vmatrix}^2 \\
&= \begin{vmatrix} 1 & \omega_2^{(1)} & \ldots & \omega_n^{(1)} \\ \vdots & \vdots & & \vdots \\ 1 & \omega_2^{(n)} & \ldots & \omega_n^{(n)} \end{vmatrix}^2 \cdot \begin{vmatrix} 1 & F_{11}(X) & \ldots & F_{1n}(X) \\ \vdots & \vdots & & \vdots \\ 1 & F_{n1}(X) & \ldots & F_{nn}(X) \end{vmatrix}^2 \\
&= D_K \cdot (I(X_2, \ldots, X_n))^2,
\end{aligned} \tag{27}$$

where the degree of the homogeneous polynomial

$$I(X_2, \ldots, X_n) = \begin{vmatrix} 1 & F_{11}(X) & \ldots & F_{1n}(X) \\ \vdots & \vdots & & \vdots \\ 1 & F_{n1}(X) & \ldots & F_{nn}(X) \end{vmatrix} \tag{28}$$

is $n(n-1)/2$ which can be calculated from the degrees of the polynomials $F_{ji}(X)$. $\square$

Example 2.30. *Let $K = \mathbb{Q}(\sqrt[3]{m})$ with some $m \in \mathbb{Z}$ which is not a perfect cube. It is easy to see that $\{1, \sqrt[3]{m}, \sqrt[3]{m^2}\}$ is a $\mathbb{Z}$-module basis of the ring $\mathbb{Z}[\sqrt[3]{m}]$,*

$$D_{K/\mathbb{Q}}(a_1 + a_2\sqrt[3]{m} + a_3\sqrt[3]{m^2}) = -27m^2 \cdot (a_2^3 - ma_3^3)^2 \tag{29}$$

and $D_{K/\mathbb{Q}}(1, \sqrt[3]{m}, \sqrt[3]{m^2}) = D_{K/\mathbb{Q}}(\sqrt[3]{m}) = -27m^2$.

The polynomial $I(X_2, \ldots, X_n)$ plays an important role for determining the monogenity of a given number field.

Definition 2.31. *The polynomial of $(n-1)$-variables $I(X_2, \ldots, X_n)$ appearing in Lemma 2.29 is called the index form corresponding to the integral basis $\{1, \omega_2, \ldots, \omega_n\}$.*

Let L be a number field with the integer ring $\mathcal{O}_L$ and K be a finite extension of L of degree $n \geq 2$. An *$\mathcal{O}_L$-order* of K is a subring $\mathcal{O} \subset \mathcal{O}_K$ which is also an $\mathcal{O}_L$-module of rank $n = [K : L]$. The following proposition provides us equivalent conditions for an order to be monogenic.

Proposition 2.32. *Let $\mathcal{O}$ be an $\mathcal{O}_L$-order of K and $\alpha \in \mathcal{O}$. If $\mathcal{O}$ has an $\mathcal{O}_L$-basis $\{1, \omega_2, \ldots, \omega_n\}$, $I \in \mathcal{O}_L[X_2, \ldots, X_n]$ is the index form relative to $1, \omega_2, \ldots, \omega_n$ and $\alpha = x_1 + x_2\omega_2 + \cdots + x_n\omega_n$ with $x_1, \ldots, x_n \in \mathcal{O}_L$. Then the following assertions are equivalent:*

(i) $\mathcal{O}_L[\alpha] = \mathcal{O}$,
(ii) $\{1, \alpha, \ldots, \alpha^{n-1}\}$ *is a $\mathcal{O}_L$-basis for $\mathcal{O}$,*
(iii) $D_{K/L}(\alpha) = u \cdot D_{K/L}(1, \omega_2, \ldots, \omega_n)$ *for some $u \in \mathcal{O}_L^\times$.*
(iv) $I(x_2, \ldots, x_n) \in \mathcal{O}_L^\times$

Proof. See [7, Proposition 5.3.1]. □

We will give the major property of the index form in the following lemma: the relation between the index of an element and the index form.

Lemma 2.33. *For any algebraic integer $\alpha = x_1 + \omega_2 x_2 + \cdots + \omega_n x_n$ with $K = \mathbb{Q}(\alpha)$, the equality*

$$I(\alpha) = |I(x_2, \ldots, x_n)| \tag{30}$$

holds true.

Proof. By Lemma 2.27, we get

$$\begin{aligned}(I(x_2, \ldots, x_n))^2 \cdot D_K =& D_{K/\mathbb{Q}}(L(x_1, \ldots, x_n)) \\ =& D_{K/\mathbb{Q}}(\alpha) \\ =& D_{K/\mathbb{Q}}(1, \alpha, \ldots, \alpha^{n-1}) \\ =& (I(\alpha))^2 \cdot D_K. \end{aligned} \tag{31}$$

□

It can be easily seen that if $\beta = \alpha + a$ where a is a integer and $\alpha, \beta \in \mathcal{O}_K$, then $\mathbb{Z}[\alpha] = \mathbb{Z}[\beta]$, so $I(\alpha) = I(\beta)$.

Let $\mathcal{O}$ be a $\mathbb{Z}$-order in K with a fixed $\mathbb{Z}$-basis $\{1, \omega_2, \ldots, \omega_n\}$ and $\alpha = x_1 + x_2\omega_2 + \cdots + x_n\omega_n$. It follows from Proposition 2.32 that $\alpha \in \mathcal{O}$ generates a power basis for $\mathcal{O}$ if and only if $(x_2, \ldots, x_n) \in \mathbb{Z}^{n-1}$ satisfies the index form equation

$$I(x_2, \ldots, x_n) = \pm 1 \text{ in } x_2, \ldots, x_n \in \mathbb{Z}. \tag{32}$$

Note that the index form is independent of the variable $x_1 \in \mathbb{Z}$. Hence, solving the equation (32) and determining all power integral bases in K are equivalent.

Definition 2.34. *Let K be a number field with ring of integers $\mathcal{O}_K$ and $\alpha, \beta \in \mathcal{O}_K$. If $\beta = a \pm \alpha$ for any $a \in \mathbb{Z}$, then α and β are called equivalent.*

Let K be a number field of degree n with ring of integers $\mathcal{O}_K$. If $\{1, \omega_2, \ldots, \omega_n\}$ is an integral basis of K and $\alpha \in \mathcal{O}_K$, by Lemma 2.31 the index $I(\alpha)$ is the absolute value of determinant of the matrix transforming the basis $\{1, \ldots, \omega_n\}$ to $\{1, \alpha, \ldots, \alpha^{n-1}\}$. We now compute the index form for some particular number fields.

Example 2.35. *Consider a number field K of degree 3. Then each element $\alpha \in \mathcal{O}_K$ is of the form*

$$\alpha = x_1 + x_2\omega_2 + x_3\omega_3 \quad \textit{with } x_i \in \mathbb{Z},\ (i = 1, 2, 3). \tag{33}$$

Hence, we want to compute

$$m(K) = \min_{x_i \in \mathbb{Z}}(\mathcal{O}_K : \mathbb{Z}[x_1 + x_2\omega_2 + x_3\omega_3]). \tag{34}$$

Since $\mathbb{Z}[x_1 + x_2\omega_2 + x_3\omega_3] = \mathbb{Z}[x_2\omega_2 + x_3\omega_3]$, it just suffices to consider elements of the form: $x_2\omega_2 + x_3\omega_3$. Let $M_{xy} \in \mathbb{Z}[x, y]^{3\times 3}$ denote the transformation matrix from the basis $\{1, \omega_2, \omega_3\}$ to $\{1, x_2\omega_2 + x_3\omega_3, (x_2\omega_2 + x_3\omega_3)^2\}$. Then the determinant of M_{xy} is a homogeneous cubic polynomial with rational integral coefficients. Hence, $I(x_2, x_3) := M_{xy}$ is the index form of α. There exists $I_0, I_1, I_2, I_3 \in \mathbb{Z}$ with

$$I(x_2, x_3) = I_0x_2^3 + I_1x_2^2x_3 + I_2x_2x_3^2 + I_3x_3^3. \tag{35}$$

Example 2.36. *Consider now the cubic field $K = \mathbb{Q}(\alpha)$ generated by $\alpha \in \mathcal{O}_K$, with minimal polynomial $f(x) = x^3 - x^2 - 6x + 1$ having discriminant $D_K = 361$. The index form equation corresponding to this integer basis is given by*

$$I(X, Y) = X^3 + 2X^2Y - 5XY^2 + Y^3. \tag{36}$$

To check whether this field is monogenic we need to find out if $I(X, Y) = \pm 1$ has any solution. Note that $(-7, 2)$, $(1, 1)$, $(9, 7)$, $(0, 1)$, $(2, 9)$, $(1, 0)$ are solutions to the equation, so this field has a power integral basis.

Example 2.37. *In case $m \equiv 2 \pmod 4$ and $n \equiv 3 \pmod 4$ an integer basis of $K = \mathbb{Q}(\sqrt{m}, \sqrt{n})$ is given by $\{1, \sqrt{m}, \sqrt{n}, \sqrt{m} + \sqrt{m_1 n_1}/2\}$, where $n_1 = n/d$ and $m_1 = m/d$ with $d = (m, n)$. The index form corresponding to this integer basis is*

$$I(x, y, z) = \Big(\frac{d}{2}(2x + z)^2 - \frac{n_1}{2}z^2\Big)\Big(2dy^2 - \frac{m_1}{2}z^2\Big)\Big(2n_1y^2 - \frac{m_1}{2}(2x + z)^2\Big), \tag{37}$$

where each factor is an element of $\mathbb{Z}[x, y, z]$.

In particular, for $m = 2$ and $n = 11$, the field $K = \mathbb{Q}(\sqrt{2}, \sqrt{11})$ has discriminant $D_K = 30976$ and only solutions to the equation $I(x, y, z) = \pm 1$ are $(-1, 0, 1)$, $(0, 0, 1)$.

For the computation of index forms in Example 2.36, 2.37 and 2.38 we refer to [9]. The next natural question is to know if there is any non-monogenic field.

Example 2.38. *Consider the totally real field $K = \mathbb{Q}(\alpha)$, generated by α, with minimal polynomial $f(x) = x^4 - x^3 - 16x^2 - 11x + 7$ and $D_K = 848241$. The index form corresponding to the integral basis $\{1, \alpha, \alpha^2, (1 + \alpha^2)/2\}$ is of the form*

$$\begin{aligned} I(x, y, z) = {} & -58x^4y^2 + 101x^4yz + 1347x^4z^2 - 126x^3y^3 - 1613x^3y^2z - 99x^3yz^2 + 10730x^3z^3 \\ & + 414x^2y^4 - 449x32y^3z - 13632x^2y^2z^2 - 9105x^2yz^3 + 42517x^2z^4 \\ & + 6157xy^4z + 10545xy^3z^2 - 34661xy^2z^3 - 45514xyz^4 + 1797y^4z^2 \\ & + 225112y^3z^3 - 5993y^2z^4. \end{aligned} \tag{38}$$

The minimal index of the field is $m(K) = 2$. The equation $I(x, y, z) = \pm 1$ does not have any solution in $\mathbb{Z}^3$, the field K does not have a power integral basis. For the method to find the solutions of the index form equation we refer to [9].

One can see that Lemma 2.27 can be used to show the existence of non-monogenic number fields. For instance, Dedekind discovered the following cubic non-monogenic field:

Example 2.39. *Let $K = \mathbb{Q}(a)$, where a is any root of the irreducible polynomial $f(x) = x^3 - x^2 - 2x - 8$. The number $b = \frac{(a^2+a)}{2}$ is a root of the polynomial $x^3 - 3x^2 - 10x - 8$, hence is integral. Notice that $\{1, a, b\}$ form an integral basis for K, since $D_{K/\mathbb{Q}}(1, a, b) = -503$ is prime, and by Lemma 2.27, $D_{K/\mathbb{Q}}(1, a, b) = D_K$. We claim that K is not monogenic. To show this, it suffices to prove that for all $\alpha \in \mathcal{O}_K$, we have $2|D_{K/\mathbb{Q}}(\alpha)$. Indeed, writing $\alpha = A + Ba + Cb$ with $A, B, C \in \mathbb{Z}$, we have $\alpha^2 = (A^2 + 6C^2 + 8BC) + (2C^2 - B^2 + 2AB)a + (2B^2 + 3C^2 + 2AC + 4BC)b$ and so*

$$D_{K/\mathbb{Q}}(\alpha) \equiv (BC)^2(B + C) \equiv 0 \pmod 2. \tag{39}$$

2.4. Thue Equations

The main focus of this section is to define the Thue equations and state some of their applications. The reference for this section is [8].

Definition 2.40. *Let $F \in \mathbb{Z}[X, Y]$ be an irreducible homogeneous form of degree $n \geq 3$ and let m be a nonzero integer. An equation of the form*

$$F(x, y) = m \text{ with } x, y \in \mathbb{Z}. \tag{40}$$

is called a Thue equation.

It is named after Axel Thue who proved in [10] that an equation of the form (40) has only finitely many solutions in integers (see also [8, Chapter 3, Theorem 3.2]).

There are different ways of finding solutions to the equation $F(x,y) = m$ with $x, y \in \mathbb{Z}$. One of them is to provide an upper bound $|y| \leq C$ for some constant C. However, finding an optimal upper bound is an issue; Thue's proof does not allow us to calculate the constant C. In [11], Baker gave the first effective bounds for the solutions of the equation (40) and Bugeaud and Győry have given the most optimal upper bound to date in [12].

The resolution of index form equations (2.32) for cubic and quartic number fields relies on solving Thue equations. Hence, one strategy to determine whether or not a given number field has a power integral basis is to solve the Thue equations.

For larger degree number fields, one might need to modify equation (40) to tackle the index form equation. Assume that $K = \mathbb{Q}(\alpha)$ where α is an algebraic integer of degree $n \geq 3$. Let $m \neq 0 \in \mathbb{Z}$ be given. Consider the following equation

$$N_{K/\mathbb{Q}}(x + \alpha y + \lambda) = m \text{ with } x, y \in \mathbb{Z} \text{ and } \lambda \in \mathcal{O}_K, \tag{41}$$

where $|\overline{\lambda}| < a^{1-\epsilon}$ with $a = \max\{x, y\}$ and $0 < \epsilon < 1$ (here $\overline{\lambda}$ denotes the complex conjugate of λ). In [13], Sprindźuk studied the equations of this type and used Baker's method to give effective bounds for the equation (41). Before ending the section, we give some examples that the solutions of the equation (41) allow us to tackle the index form equations of sextic or octic fields. For details we refer the reader to [8, Section 11.2.1, 11.2.2 and 14.2.5].

Example 2.41. *Let ξ be a root of the polynomial $f(x) = x^8 - x^7 + x^6 + 2x^5 - 2x^4 + 2x^2 - x - 1$. Consider the field $K = \mathbb{Q}(\xi)$ generated by ξ with discriminant $D_K = -4461875 = -5^4 11^2 59$. Note that the fiel K contains $M = \mathbb{Q}(\sqrt{5})$. Set $\omega := (1+\sqrt{5}/2)$. The relative defining polynomial of ξ over M is given by $f_M(x) = x^4 + (-1+\omega)x^3 + x^2 + (1+\omega)x + \omega$. It then follows from the calculations in [8, Section 14.2.5] that the following integers generate power integral bases in K:*

$$\xi, \quad \xi + (-1+\omega)\xi^2, \quad (1-\omega)\xi + (-1+\omega)\xi^2. \tag{42}$$

3. MONOGENITY OF CUBIC FIELDS

In this chapter, our main purpose is to give partial answers to the following questions: Which cubic fields are monogenic and if a cubic number field K is, for which α we have $\mathcal{O}_K = \mathbb{Z}[\alpha]$?

There is no unified theory to classify all the monogenic number fields. However, for some types of cubic fields such as cyclic cubic fields or pure cubic fields, there are some approaches to derive some results on monogenity. Moreover, some computational results exist for the fields whose discriminant lie in a fixed interval. This chapter is devoted to the collections of these approaches in cubic fields.

3.1. Arbitrary Cubic Fields

In this section, we will explain the correlation between the index form equations and arbitrary cubic fields which have power integral bases. The main references are [8] and [14].

Let K be a number field of degree 3. As we know the index form equation of K is just the cubic Thue equation

$$I(x, y) = a_0x^3 + a_1x^2y + a_2xy^2 + a_3y^3 = \pm 1, \tag{1}$$

where $a_i \in \mathbb{Z}$ for $i = 0, 1, 2, 3$. We will list all solutions of the index form equation (1) corresponding to monogenic cubic fields with discriminant lying in the interval $-300 \leq D_K \leq 3137$. There are 100 totally real and 30 complex monogenic cubic fields.

The following tables contain the data:

$$D_K \quad f(x) \quad (I_3, I_2, I_1, I_0) \quad (x_1, y_1), (x_2, y_2) \dots \tag{2}$$

where $f(x) = x^3 + a_2x^2 + a_1x + a_0 \in \mathbb{Z}[x]$ is the defining polynomial of K generated by α over $\mathbb{Q}$ and D_K denotes the discriminant of the field K. The index form is

$$I(X, Y) = I_3X^3 + I_2X^2Y + I_1XY^2 + I_0Y^3 \in \mathbb{Z}[X, Y], \tag{3}$$

and the solutions of $I(X,Y) = \pm 1$ are $(x_1, y_1), (x_2, y_2), \ldots$ One can see that, if (x, y) is a solution of $I(X,Y) = \pm 1$, then so is $(-x, -y)$; however, we will state only one of them in the tables. If the given integral basis is the form $\{1, \omega_2, \omega_3\}$ instead of $\{1, \alpha, \alpha^2\}$, we can write

$$\omega_2 = (p_0 + p_1\alpha + p_2\alpha^2)/p \text{ and } \omega_3 = (q_0 + q_1\alpha + q_2\alpha^2)/q \text{ with } p, p_i, q, q_j \in \mathbb{Z}. \quad (4)$$

Hence, the tables also contain the following data:

$$\omega_2 = (p_0, p_1, p_2)/p \text{ and } \omega_3 = (q_0, q_1, q_2)/q. \quad (5)$$

Table 3.1. Real monogenic cubic fields.

D_K	$f(x)$	$I(X,Y)$	Solution(s)
49	x^3-x^2-2x+1	(1,2,-1,-1)	(-2,1),(-9,4),(-1,1),(-1,-1),(-1,2), (-5,9),(0,1),(4,5),(1,0)
81	x^3-3x+1	(1,0,-3,1)	(-2,1),(1,1),(3,2),(0,1),(1,3),(1,0)
148	x^3-x^2-3x+1	(1,2,-2,-2)	(1,1),(1,-1),(-5,2),(-31,45),(1,0)
169	x^3-x^2-4x-1	(1,2,-3,-5)	(-2,1),(-1,1),(1,0)
229	x^3-4x+1	(1,0,-4,1)	(-2,1),(-2,-2),(508,273),(0,1),(1,4),(1,0)
257	x^3-x^2-4x+3	(1,2,-3,-1)	(1,1),(6,5),(-3,1),(0,1),(-2,7),(1,0)
316	x^3-x^2-4x+2	(1,2,-3,-2)	(-1,2),(1,0)
321	x^3-x^2-4x+1	(1,2,-3,-3)	(1,-1),(1,0)
361	x^3-x^2-6x+7	(1,2,-5,1)	(-7,2),(1,1),(9,7),(0,1),(2,9),(1,0)
404	x^3-x^2-5x-1	(1,2,-4,-6)	(1,-1),(1,0)
469	x^3-x^2-5x+4	(1,2,-4,-1)	(0,1),(1,0)
473	x^3-5x+1	(1,0,-5,1)	(-2,-1),(-7,3),(0,1),(1,5),(1,0)
564	x^3-x^2-5x+3	(1,2,-4,-2)	(3,2),(-3,1),(-3,7),(1,0)
568	x^3-x^2-6x-2	(1,2,-5,-8)	(17,8),(1,0)
621	x^3-6x+3	(1,0,-6,3)	(-8,3),(2,1),(1,2),(1,0)
697	x^3-7x+5	(1,0,-7,5)	(-3,1),(2,1),(13,6),(1,1),(1,0)
733	x^3-x^2-7x+8	(1,2,-6,1)	(3,2),(0,1),(1,0)
756	x^3-6x+2	(1,0,-6,2)	(1,3),(1,0)
761	x^3-x^2-6x-1	(1,2,-5,-7)	(2,1),(-3,1),(-1,1),(1,0)
785	x^3-x^2-6x+5	(1,2,-5,-1)	(0,1),(1,0)
788	x^3-x^2-7x-3	(1,2,-6,-10)	(-3,1),(-3,2),(1,0)
837	x^3-6x+1	(1,0,-6,1)	(0,1),(1,6),(1,0)
892	$x^3-x^2-8x+10$	(1,2,-7,2)	(1,0)
940	x^3-7x+4	(1,0,-7,4)	(1,0)

Table 3.1. Real monogenic cubic fields. (cont.)

D_K	$f(x)$	$I(X,Y)$	Solution(s)
961	$x^3 - x^2 - 10x + 8$	(2,5,-1,-2)	no solutions $\omega_2 = (0,1,0)/1$, $\omega_3 = (0,1,1)/2$
985	$x^3 - x^2 - 6x + 1$	(1,2,-5,-5)	(1,-1),(2,1),(-3,1),(1,0)
993	$x^3 - x^2 - 6x + 3$	(1,2,-5,-3)	(-1,2),(1,0)
1016	$x^3 - x^2 - 6x + 2$	(1,2,-5,-4)	(1,0)
1076	$x^3 - 8x + 6$	(1,0,-8,-6)	(7,3),(1,1),(1,0)
1101	$x^3 - x^2 - 9x + 12$	(1,2,-8,3)	(1,0)
1129	$x^3 - 7x + 3$	(1,0,-7,3)	(1,0)
1229	$x^3 - x^2 - 7x + 6$	(1,2,-6,-1)	(7,4),(0,1),(1,0)
1257	$x^3 - x^2 - 8x + 9$	(1,2,-7,1)	(-19,7),(18,7),(0,1),(1,7),(1,0)
1300	$x^3 - 10x + 10$	(1,0,-10,-10)	(1,1),(1,0)
1345	$x^3 - 7x + 1$	(1,0,-7,1)	(-19,7),(18,7),(0,1),(1,7),(1,0)
1369	$x^3 - x^2 - 12x - 11$	(1,2,-11,-23)	(3,-1),(-2,1),(1,0)
1373	$x^3 - 8x + 5$	(1,0,-8,5)	(2,3),(1,0)
1384	$x^3 - x^2 - 10x + 14$	(1,2,-9,4)	(25,14),(1,2),(1,0)
1396	$x^3 - x^2 - 7x + 5$	(1,2,-6,-2)	(1,0)
1425	$x^3 - x^2 - 8x - 3$	(1,2,-7,-11)	(3,-1),(1,0)
1436	$x^3 - 11x + 12$	(1,0,-11,12)	(5,2),(1,0)
1489	$x^3 - x^2 - 10x - 7$	(1,2,-9,-7)	(2,-1),(3,1),(3,-1),(-22,7),(1,0)
1492	$x^3 - x^2 - 9x - 5$	(1,2,-8,-14)	(3,-1),(1,0)
1509	$x^3 - x^2 - 7x + 4$	(1,2,-6,-3)	(2,1),(1,0)
1524	$x^3 - x^2 - 7x + 1$	(1,2,-6,-6)	(-1,1),(1,0)
1556	$x^3 - x^2 - 9x + 1$	(1,2,-8,2)	(1,0)
1573	$x^3 - x^2 - 7x + 2$	(1,2,-6,-5)	(2,1),(-13,18),(1,0)

Table 3.1. Real monogenic cubic fields. (cont.)

D_K	$f(x)$	$I(X,Y)$	Solution(s)
1593	x^3-9x+7	(1,0,-9,7)	(-10,3),(5,2),(1,1),(1,0)
1620	$x^3-12x+14$	(1,0,-12,14)	(1,0)
1708	x^3-x^2-8x-2	(1,2,-7,-10)	(1,0)
1765	$x^3-x^2-11x+16$	(1,2,-10,5)	(2,1),(1,0)
1772	$x^3-x^2-12x+8$	(2,5,-2,-3)	(-8,3),(-2,3) $\omega_2=(0,1,0)/1$, $\omega_3=(0,1,1)/2$
1825	x^3-x^2-8x+7	(1,2,-7,-1)	(2,1),(0,1),(1,0)
1849	$x^3-x^2-14x-8$	(2,5,-7,-1)	no solutions $\omega_2=(0,1,0)/1$, $\omega_3=(0,1,1)/2$
1901	x^3-x^2-9x-4	(1,2,-8,-13)	(-42,13),(-3,2),(1,0)
1929	$x^3-x^2-10x+13$	(1,2,-9,3)	(2,1),(1,0)
1937	x^3-x^2-8x-1	(1,2,-7,-9)	(-1,1),(1,0)
1940	x^3-8x+2	(1,0,-8,-2)	(-3,1),(1,4),(1,0)
1944	x^3-9x+6	(1,0,-9,6)	(1,0)
1957	$x^3-x^2-9x+10$	(1,2,-8,1)	(-4,1),(2,1),(0,1),(1,0)
2021	x^3-8x+1	(1,0,-8,1)	(-26,9),(0,1),(1,8),(1,0)
2024	$x^3-x^2-10x-6$	(1,2,-9,-16)	(1,0)
2057	$x^3-11x+11$	(1,0,-11,11)	(1,1),(1,0)
2089	$x^3-13x+4$	(2,3,-5,-2)	no solutions $\omega_2=(0,1,0)/1$, $\omega_3=(0,1,1)/2$
2101	$x^3-x^2-11x-8$	(1,2,-10,-19)	(-2,1),(1,0)
2177	x^3-x^2-8x+5	(1,2,-7,-3)	(2,1),(1,0)
2213	$x^3-x^2-13x-12$	(1,2,-12,-25)	(-2,1),(1,0)
2233	x^3-x^2-8x+1	(1,2,7,-7)	(-1,1),(1,0)
2241	x^3-9x+5	(1,0,-9,5)	(8,3),(1,0)
2296	$x^3-x^2-14x-14$	(1,2,-7,-7)	(-9,4),(1,0)

Table 3.1. Real monogenic cubic fields. (cont.)

D_K	$f(x)$	$I(X,Y)$	Solution(s)
2300	$x^3 - x^2 - 8x + 2$	(1,2,-7,-6)	(-7,2),(1,0)
2349	$x^3 - 12x + 13$	(1,0,-12,13)	(8,3),(1,0)
2505	$x^3 - x^2 - 10x - 5$	(1,2,-9,-15)	(1,0)
2557	$x^3 - x^2 - 9x - 2$	(1,2,-8,-11)	(1,0)
2589	$x^3 - x^2 - 14x + 12$	(2,5,-3,-3)	(1,1) $\omega_2 = (0,1,0)/1$, $\omega_3 = (0,1,1)/2$
2597	$x^3 - x^2 - 9x + 8$	(1,2,-8,-1)	(2,1),(-4,1),(0,1), (1,0)
2636	$x^3 - 14x + 4$	(2,0,-7,1)	(-2,1),(1,0) $\omega_2 = (0,1,0)/1$, $\omega_3 = (0,0,1)/2$
2673	$x^3 - 9x + 3$	(1,0,-9,3)	(1,3),(1,0)
2677	$x^3 - 10x + 7$	(1,0,-10,7)	(1,0)
2700	$x^3 - 15x + 20$	(1,0,-15,20)	(1,0)
2708	$x^3 - x^2 - 11x - 7$	(1,2,-10,-18)	(1,0)
2713	$x^3 - 13x + 15$	(1,0,-13,15)	(-49,12),(4,3),(1,0)
2777	$x^3 - x^2 - 14x + 23$	(1,2,-13,9)	(-5,1),(2,1),(17,8),(1,1),(1,0)
2804	$x^3 - x^2 - 9x - 1$	(1,2,-8,-10)	(-1,1),(1,0)
2808	$x^3 - 9x + 2$	(1,0,-9,2)	(1,0)
2836	$x^3 - x^2 - 9x + 7$	(1,2,-8,-2)	(1,0)
2857	$x^3 - x^2 - 10x + 11$	(1,2,-9,1)	(-21,5),(2,1),(0,1),(1,0)
2917	$x^3 - x^2 - 13x + 20$	(1,2,-12,7)	(2,1),(1,0)
2981	$x^3 - x^2 - 11x + 14$	(1,2,-10,3)	(2,1),(1,0)
2993	$x^3 - x^2 - 12x + 17$	(1,2,-11,5)	(2,1),(1,2),(1,0)
3021	$x^3 - x^2 - 9x + 6$	(1,2,-11,-3)	(1,0)
3028	$x^3 - 10x + 6$	(1,0,-10,6)	(1,0)
3137	$x^3 - 11x + 9$	(1,0,-11,9)	(-11,3),(1,1)

Table 3.2. Complex monogenic cubic fields.

D_K	$f(x)$	$I(X,Y)$	Solution(s)
-23	$x^3 - x + 1$	(1,0,-1,1)	(-1,1),(0,1),(1,1),(4,-3),(1,0)
-31	$x^3 + x + 1$	(1,0,1,1)	(-2,3),(1,-1),(0,1),(1,0)
-44	$x^3 + x^2 - x + 1$	(1,-2,0,2)	(-47,56),(1,-1),(1,0),(1,1)
-59	$x^3 + 2x + 1$	(1,0,2,1)	(0,1),(1,-2),(1,0)
-76	$x^3 - 2x + 2$	(1,0,-2,2)	(-23,13),(1,1),(1,0)
-83	$x^3 + x^2 + x + 2$	(1,-2,-2,1)	(0,1),(1,0)
-87	$x^3 + x^2 - 2x - 3$	(1,-2,-1,-1)	(0,-1),(1,0)
-104	$x^3 - x + 2$	(1,0,-1,2)	(-3,2),(1,0)
-107	$x^3 + x^2 + 3x + 2$	(1,-2,4,-1)	(0,-1),(2,7),(1,0)
-108	$x^3 + 2$	(1,0,0,2)	(-1,1),(1,0)
-116	$x^3 + x + 2$	(1,-2,1,2)	(1,0)
-135	$x^3 - 3x + 3$	(1,0,-3,3)	(-2,1),(1,1),(1,0)
-139	$x^3 + x^2 + x - 2$	(1,-2,2,-3)	(2,1),(1,0)
-140	$x^3 + 2x + 2$	(1,0,2,2)	(1,-1),(1,0)
-152	$x^3 + x^2 - 2x + 2$	(1,-2,-1,4)	(1,0)
-172	$x^3 + x^2 - x - 3$	(1,-2,0,-2)	(1,0)
-175	$x^3 + x^2 + 2x + 3$	(1,-2,3,1)	(0,1),(1,0)
-199	$x^3 + x^2 - 4x + 3$	(1,-2,-3,7)	(2,1),(1,0)
-200	$x^3 + x^2 + 2x - 2$	(1,-2,3,-4)	(1,0)
-204	$x^3 + x^2 + x + 3$	(1,-2,2,2)	(1,0)
-211	$x^3 - 2x + 3$	(1,0,-2,3)	(2,-1),(1,0)
-212	$x^3 + x^2 + 4x + 2$	(1,-2,5,-2)	(1,2),(1,0)
-216	$x^3 + 3x + 2$	(1,0,3,2)	(1,0)
-231	$x^3 + x^2 - 3$	(1,-2,1,-3)	(-2,-1),(1,0)

Table 3.2. Complex monogenic cubic fields. (cont.)

D_K	$f(x)$	$I(X,Y)$	Solution(s)
-239	$x^3 - x + 3$	(1,0,-1,3)	(-5,3),(1,0)
-243	$x^3 + 3$	(1,0,0,3)	(1,0)
-244	$x^3 + x^2 - 4x - 6$	(1,-2,-3,-2)	(1,0)
-239	$x^3 - x + 3$	(1,0,-1,3)	(-5,3),(1,0)
-243	$x^3 + 3$	(1,0,0,3)	(1,0)
-244	$x^3 + x^2 - 4x - 6$	(1,-2,-3,-2)	(1,0)
-247	$x^3 + x + 3$	(1,0,1,3)	(1,0)
-255	$x^3 + x^2 + 3$	(1,-2,1,3)	(-1,1),(1,0)
-268	$x^3 + x^2 - 3x - 5$	(1,-2,-2,-2)	(1,-1),(1,0)
-283	$x^3 + 4x + 1$	(1,0,4,1)	(0,1),(1,-4),(1,0)
-300	$x^3 + x^2 - 3x + 3$	(1,-2,-2,6)	(1,0)

The following polynomials illustrate some monogenic number fields with discriminant larger than 3137.

Example 3.1. *Consider the cubic fields $K = \mathbb{Q}(\alpha_i)$ generated by α_i where $i \in \{1, 2, 3\}$, with minimal polynomials f_1, f_2 and f_3 given below. These cubic fields have the same discriminant, $D_K = 22356$, and they are monogenic.*

- $f_1(x) = x^3 - 36x + 60$ *with the associated index form* $I(X, Y) = 2X^3 - 18XY^2 + 15Y^3$. *The only solutions of the index form equation* $I(X, Y) = \pm 1$ *are* $(1, 1)$ *and* $\omega_2 = (0, 1, 0)/1$, $\omega_3 = (0, 0, 1)/2$.
- $f_2(x) = x^3 - 16x + 6$ *with the associated index form* $I(X, Y) = X^3 - 18XY^2 + 6Y^3$. *The only solutions of the index form equation are* $(1, 3)$ *and* $(1, 0)$.
- $f_3(x) = x^3 - 36x + 78$ *with the associated index form* $I(X, Y) = X^3 - 36XY^2 + 78Y^3$. *The solutions are* $(485, 117)$ *and* $(1, 0)$.

Example 3.2. *Let α be a root of the polynomial $g(x) = x^3 + x^2 - 274x + 61$ and $K = \mathbb{Q}(\alpha)$ with discriminant $D_K = 677329$. The associated index form of K is given by $I(X, Y) = 11X^3 - 14X^2Y - 19XY^2 + 11Y^3$. There are no solutions to the index form equation $I(X, Y) = \pm 1$, so K is not monogenic. In (4) we get $\omega_2 = (0, 1, 0)/1$, $\omega_3 = (-1, -4, 1)/11$.*

3.2. Cyclic Cubic Fields

The number fields of degree 3 whose Galois groups are isomorphic to $\mathbb{Z}/3\mathbb{Z}$ are called *cyclic cubic fields*. Cyclic cubic fields are totally real fields, i.e. all three roots of the minimal polynomial are real.

In this section, we will give some equivalent conditions for the monogenity of the ring of integers of any cyclic cubic field. First, we will show that if a cyclic cubic field is monogenic then it is a simplest cubic field K_t defined by Shanks' cubic polynomial, which is defined below. Then we will give two equivalent conditions for when K_t is monogenic, which is explicitly written in terms of t.

Let $t \in \mathbb{Z}$ and the Shanks' cubic polynomials be defined as in [15]:

$$f_t(x) := x^3 - tx^2 - (t+3)x - 1, \tag{6}$$

with discriminant $D(f_t) = (t^2 + 3t + 9)^2$.

Definition 3.3. *The field $K_t := \mathbb{Q}(\theta_t)$ is called a simplest cubic field where θ_t is a root of $f_t(x) \in \mathbb{Z}[x]$.*

It can easily be seen that $K_t = K_{-(t+3)}$, so without loss of generality we may assume $-1 \leq t \in \mathbb{Z}$. Set $\Delta_t := t^2+3t+9$. Hence, if Δ_t is square-free, then $D(f_t) = D_K$ and $(1, \theta_t, \theta_t^2)$ is an integral basis of K_t. The index form equation corresponding to the integral basis $(1, \theta_t, \theta_t^2)$ is $I(x, y) = x^3 - tx^2y - (t+3)xy^2 - y^3 = \pm 1$. In [8], Gaál tried to solve this index form equation for some $t \in \mathbb{Z}$ and gave some partial examples of monogenic cyclic cubic fields. However, in [16], Kashio and Sekigawa gave a complete characterization of such cubic fields.

Note that by Rational Root test, the polynomial $f_t(x)$ is irreducible, since ± 1 are not roots of $f_t(x)$. Let θ_t denote a root of $f_t(x)$. Then the field $K_t = \mathbb{Q}(\theta_t)$ is a degree 3 extension of $\mathbb{Q}$. It can be seen that $\frac{-1}{1+\theta_t}$ and $-\frac{1+\theta_t}{\theta_t}$ are the other roots of $f_t(x)$. Hence, we deduce the following facts:

- $K_t/\mathbb{Q}$ is a cyclic cubic extension. Let us denote the Galois group by

$$G := \mathrm{Gal}(K_t/\mathbb{Q}) =< \sigma >= \{1, \sigma, \sigma^2\}. \tag{7}$$

- θ_t is a unit of $\mathcal{O}_{K_t}^{\times}$ satisfying

$$\sigma(\theta_t) = -\frac{1+\theta_t}{\theta_t},\ \sigma^2(\theta_t) = \frac{-1}{1+\theta_t},\ 1+\theta_t+\theta_t\sigma(\theta_t) = 0,\ N_{K/\mathbb{Q}}(\theta_t) = 1,\ \mathrm{Tr}_{K/\mathbb{Q}}(\theta_t) = t.$$

- Let c_K denote the conductor of K. By conductor-discriminant formula we have

$$c_K = \sqrt{D_K}. \tag{8}$$

Let $v_p(n)$ denote the order at a prime p of an integer n defined by $n = p^{v_p(n)}n_0$, $(p, n_0) = 1$. The proof of the following theorem will be given in Section 3.2.1.

Theorem 3.4. *Let K be a cyclic cubic field. The followings are equivalent:*

(i) K has a power integral basis.

(ii) There exists t satisfying $K = K_t$ and

$$\frac{\Delta_t}{c_K} \in \mathbb{N} := \{n^3 | n \in \mathbb{N}\}. \tag{9}$$

(iii) There exists t satisfying $K = K_t$ and

$$t \not\equiv 3, 21 \pmod{27}, \ \ v_p(\Delta_t) \not\equiv 2 \pmod{3} \text{ for all } p \neq 3. \tag{10}$$

In this case, a power integral basis $\alpha \in \mathcal{O}_K$ is a given by

$$\alpha := \frac{\theta_t - a}{\sqrt[3]{\frac{\Delta_t}{c_K}}} \text{ for } \alpha \in \mathbb{Z} \text{ with } a \equiv \frac{t}{3} \pmod{\sqrt[3]{\frac{\Delta_t}{c_K}}}. \tag{11}$$

The condition $a \equiv \frac{t}{3} \pmod{\sqrt[3]{\frac{\Delta_t}{c_K}}}$ means that we take an integer a satisfying

$$\begin{cases} a \equiv \frac{t}{3} \pmod{\sqrt[3]{\frac{\Delta_t}{c_K}}}, & \text{if } 3 | \sqrt[3]{\frac{\Delta_t}{c_K}}, \\ 3a \equiv t \pmod{\sqrt[3]{\frac{\Delta_t}{c_K}}}, & \text{if } 3 \not| \sqrt[3]{\frac{\Delta_t}{c_K}}. \end{cases} \tag{12}$$

Here, we have $3|t$ when $3|\sqrt[3]{\frac{\Delta_t}{c_t}}$ by Proposition 3.2 (i) in [17].

Remark 3.5.

- *The condition given in terms of t in Theorem 3.4(iii) allows us to study the monogenity without studying the number field K_t itself, see Corollary 3.10.*
- *For $\mathbb{Q}(\zeta_9 + \zeta_9^{-1})$ we have $c_{\mathbb{Q}(\zeta_9+\zeta_9^{-1})} = \Delta_0 = 9$. Hence, the assertions of Theorem 3.4 hold true in this case. Therefore, we focus our attention on case $K \neq \mathbb{Q}(\zeta_9 + \zeta_9^{-1})$.*

Let us set some notations. For a given number field K, we denote by I_K, P_K the group of all fractional ideals, all principal ideals, respectively. In addition, we put

$$I_K^G := \{\mathfrak{U} \in I_K | \mathfrak{U}^\sigma = \mathfrak{U}\},\ P_K^G := I_K^G \cap P_K \tag{13}$$

to be the group of all ambiguous ideals, all principal ambiguous ideals, respectively. Let $\mathfrak{C}_K$ be the unique integral ideal of K such that

$$N_{K/\mathbb{Q}}\mathfrak{C}_K = c_K, \tag{14}$$

whose existence is proven in Lemma 3.6. It can be seen easily that $\mathfrak{C}_K \in I_K^G$; in particular, if $\mathfrak{C}_K$ is principal, then $\mathfrak{C}_K \in P_K^G$.

Lemma 3.6. *Let K be a cyclic cubic field. There exists a unique integral ideal $\mathfrak{C}_K \subset \mathcal{O}_K$ satisfying $N_{K/\mathbb{Q}}\mathfrak{C}_K = c_K$.*

Proof. The followings are equivalent:

(i) $p | c_K$.
(ii) $p | D_K$.
(iii) a unique prime ideal $\mathfrak{B}_p$ satisfies $p = \mathfrak{B}_p^3$, $N_{K/\mathbb{Q}}\mathfrak{B}_p = p$.

Hence, the ideal

$$\mathfrak{C}_K := \prod_{p | c_K} \mathfrak{B}_p^{v_p(c_K)} \tag{15}$$

is the unique ideal satisfying $N_{K/\mathbb{Q}}\mathfrak{C}_K = c_K$. □

The following theorems, which establish equivalent conditions of having a power integral basis, will play an integral role in the proof Theorem 3.4.

Theorem 3.7. *Let K be a cyclic cubic field and $K \neq \mathbb{Q}(\zeta_9 + \zeta_9^{-1})$.*

(i) If K has a power integral basis, then we have
- *K is a simplest cubic field.*
- *$\mathfrak{C}_K$ is principal.*

(ii) Assume that K is a simplest cubic field and $\mathfrak{C}_K$ is principal, say $\mathfrak{C}_K = (\beta)$. The followings are equivalent.
(a) K has a power integral basis.
(b) There exists t satisfying $K = K_t$ and $\frac{\Delta_t}{c_K} \in \mathbb{N}^3$.

Proof. See [16, Theorem 1.3]. □

Theorem 3.8. *Assume that $K = K_t$, for some $-1 \leq t \in \mathbb{Z}$ and $K \neq \mathbb{Q}(\zeta_9 + \zeta_9^{-1})$. The following statements are equivalent.*

(i) $\mathfrak{C}_K$ is principal.
(ii) $\frac{\Delta_t}{c_K}$ or $\frac{\Delta_t^2}{c_K} \in \mathbb{N}^3$.

Proof. See [16, Theorem 1.4]. □

Remark 3.9. *One can derive the following expression regarding c_{K_t}:*

$$c_{K_t} = \begin{cases} \displaystyle\prod_{v_p(\Delta_t)\not\equiv 0 \pmod 3} p & (3 \nmid t \text{ or } t \equiv 12 \pmod{27}) \\ 3^2 \displaystyle\prod_{p\neq 3, v_p(\Delta_t)\not\equiv 0 \pmod 3} p & (\textit{otherwise}). \end{cases} \tag{16}$$

In [18], Hoshi shows that if $t \neq t'$ then $K_t \neq K_{t'}$ except for the cases

$$K_{-1} = K_5 = K_{12} = K_{1259},\ K_0 = K_3 = K_{54}(= \mathbb{Q}(\zeta_9 + \zeta_9^{-1})),\ K_1 = K_{66},\ K_2 = K_{2389}. \tag{17}$$

Therefore, if we assume that $t \neq -1,\ 0,\ 1,\ 2,\ 3,\ 5,\ 12,\ 54,\ 66,\ 1259,\ 2389$*, we can say that the integer* t *in Theorem 3.4 and 3.7 is unique. Note that it follows from Theorem 3.4 that* K_t *has a power integral basis for* $t = -1,0,1,2$*. Hence, we can deduce the following result.*

Corollary 3.10. *If a cyclic cubic field* K *has a power integral basis, then it is a simplest cubic field, that is, there exists* t *satisfying* $K = K_t$*. Moreover, the following statements are equivalent.*

(i) K_t *has a power integral basis.*

(ii) $t \in \{-1, 0, 1, 2, 3, 5, 12, 54, 66, 1259, 2389\}$ *or* t *satisfies that* $\frac{\Delta_t}{c_{K_t}} \in \mathbb{N}^3$.

(iii) $t \in \{-1, 0, 1, 2, 3, 5, 12, 54, 66, 1259, 2389\}$ *or* t *satisfies that* $t \not\equiv 3, 21 \pmod{27}$ *and that* $v_p(\Delta_t) \not\equiv 2 \pmod{3}$ *for all* $p \neq 3$.

Proof. The equivalence between (i) and (ii) follows from Theorem 3.8 and Remark 3.9. On the other hand, it follows from Theorem 3.4 that (ii) is equivalent to (iii). □

We now recall some properties of primes dividing c_K and Δ_t. The following propositions will be used frequently during the proof of Theorem 3.4.

Proposition 3.11. *Let* K *be a cyclic cubic field. The conductor* c_K *satisfies the following conditions. Let* p *denote a rational prime.*

(i) If $3|c_K$*, then* $v_3(c_K) = 2$.

(ii) If $p \equiv 1 \pmod{3}$*, then* $p|c_K$ *implies* $v_p(c_K) = 1$.

(iii) If $p \equiv 2 \pmod{3}$*, then* $p \not| c_K$.

Proof. See [16, Proposition 3.1]. □

Proposition 3.12. *Let $K = K_t$. Then $v_3(\Delta_t)$ can be only $0, 2, 3$. More precisely, we have the following*

(i) $v_3(\Delta_t) = 0$ *if and only if* $3 \nmid t$. *In this case,* $3 \nmid c_K$.
(ii) $v_3(\Delta_t) = 2$ *if and only if* $t \equiv 0, 6 \pmod 9$. *In this case,* $3 | c_K$.
(iii) $v_3(\Delta_t) = 3$ *if and only if* $t \equiv 3 \pmod 9$. *In this case,*

$$\begin{cases} t \equiv 12 \pmod{27} \text{ if and only if } 3 \nmid c_K, \\ t \equiv 3, 21 \pmod{27} \text{ if and only if } 3 | c_K. \end{cases} \tag{18}$$

Proof. See [16, Proposition 3.2]. □

In particular, we have that

$$\begin{cases} 3 \nmid c_K \text{ if and only if } 3 \nmid t \text{ or } t \equiv 12 \pmod{27}, \\ 3 | c_K \text{ if and only if } t \equiv 0, 6 \pmod 9 \text{ or } t \equiv 3, 21 \pmod{27}. \end{cases} \tag{19}$$

Proposition 3.13. *Let $K = K_t$ and $p \neq 3$ be a prime. The following statements are equivalent.*

(i) $v_p(\Delta_t) \equiv 0 \pmod 3$,
(ii) $p \nmid c_K$.

Proof. See [16, Proposition 3.3]. □

The following corollary is a consequence of the results of Proposition 3.11, 3.12 and 3.13.

Corollary 3.14. *Let $K = K_t \neq \mathbb{Q}(\zeta_9 + \zeta_9^{-1})$. The following statement are equivalent.*

(i) $\mathfrak{C}_K$ *is principal.*

(ii) $\begin{cases} v_p(\Delta_t) \equiv 1 \text{ or } 2 \pmod 3 \text{ for all } p|c_K \ (3 \nmid c_K) \\ v_3(\Delta_t) = 2 \text{ and } v_p(\Delta_t) \equiv 1 \pmod 3 \text{ for all } 3 \neq p|c_K \ (3|c_K). \end{cases}$

(iii) $\begin{cases} v_p(\Delta_t) \not\equiv 1 \text{ or } 2 \pmod 3 \text{ for all } p \ (3 \nmid t, \ t \equiv 12 \pmod{27}), \\ v_p(\Delta_t) \not\equiv 2 \pmod 3 \text{ for all } p \neq 3, \ (t \equiv 0, 3 \pmod 9). \end{cases}$

Proof. First, we prove that (i) is equivalent to (ii). By Proposition 3.11, 3.12 and 3.13, for primes $p \neq 3$, we have

$$v_p(c_K) = 0, 1 \text{ and } v_p(c_K) = 0 \text{ if and only if } v_p(\Delta_t) \equiv 0 \pmod 3. \tag{20}$$

For $p = 3$, we have

- $v_3(\Delta_t) \in \{0, 2, 3\}$. In particular, if $3 \nmid c_K$ then $v_3(\Delta_t) \in \{0, 3\}$;
- 3 divides c_K if and only if $v_3(c_K) = 2$, which implies that $v_3(\Delta_t) \in \{2, 3\}$.

By Theorem 3.8, the ideal $\mathfrak{C}_K$ is principal if and only if Δ_t/c_K or $\Delta_t^2/c_K \in \mathbb{N}^3$, which is equivalent to saying that

$$v_p(\Delta_t) \equiv e v_p(c_K) \pmod 3 \text{ with } e \in \{1, 2\} \text{ for all primes } p. \tag{21}$$

Case I. Assume that 3 does not divide c_K. In this case, since $v_p(c_K) = 0 \equiv e v_p(\Delta_t) \pmod 3$, the statement (21) is equivalent to

$$v_p(\Delta_t) \equiv e v_p(c_K) \pmod 3 \text{ with } e \in \{1, 2\} \text{ for all primes } p|c_K. \tag{22}$$

By Proposition 3.11, i.e. $v_p(c_K) = 1$ for all $3 \neq p|c_K$, we deduce that (21) is equivalent to saying that

$$v_p(\Delta_t) \equiv 1 \text{ or } 2 \pmod 3 \text{ for all primes } p|c_K. \tag{23}$$

Case II. Suppose now that 3 divides c_K. Since $v_3(c_K) = 2$ and $v_3(\Delta_t) \in \{2, 3\}$, the case $e = 2$ in (21) is not possible. Therefore, (21) holds true if and only if

$$v_p(\Delta_t) \equiv v_p(c_K) \pmod 3 \text{ for all primes } p|c_K,$$

which is equivalent to

$$v_3(\Delta_t) = 2 \text{ and } v_p(\Delta_t) \equiv 1 \pmod 3 \text{ for all primes } 3 \neq p|c_K. \tag{24}$$

We now want to show that (ii) is equal to (iii). Note that by Proposition 3.12 we have that $3|c_K$ if and only if $t \equiv 0, 6 \pmod 9$ or $t \equiv 3, 21 \pmod{27}$ and $3 \nmid c_K$ if and only if $3 \nmid t$ or $t \equiv 12 \pmod{27}$. Since $v_p(\Delta_t) \equiv 0 \pmod 3$ whenever $3 \neq p \nmid c_K$, we see that (24) is equivalent to $v_p(\Delta_t) \not\equiv 2 \pmod 3$ for all primes $3 \neq p$ and $t \equiv 0, 6 \pmod 9$. By using the similar arguments we can conclude the proof for the other cases.

□

3.2.1. Proof of Theorem 3.4

In this subsection, we will give the proof of Theorem 3.4. Let K be a cyclic cubic field and $K \neq \mathbb{Q}(\zeta_9 + \zeta_9^{-1})$. We aim to prove the equivalence of the following statements:

(i) K has a power integral basis.

(ii) There exists t satisfying $K = K_t$ and

$$\frac{\Delta_t}{c_K} \in \mathbb{N} := \{n^3 | n \in \mathbb{N}\}. \tag{25}$$

(iii) There exists t satisfying $K = K_t$ and

$$t \not\equiv 3, 21 \pmod{27}, \quad v_p(\Delta_t) \not\equiv 2 \pmod 3 \text{ for all } p \neq 3. \tag{26}$$

We first prove that (i) is equivalent to (ii). Assume that K has a power integral basis. By Theorem 3.7 (i), we have that K is a simplest cubic field and the ideal $\mathfrak{C}_K$ is principal. It follows from Theorem 3.7 (ii) that there exists t such that that $K = K_t$ and $\frac{\Delta_t}{c_K} \in \mathbb{N}^3$. So we deduce that (i) implies (ii).

Suppose now that there exists t such that $K = K_t$ and $\frac{\Delta_t}{c_K} \in \mathbb{N}^3$. By Theorem 3.8, we have that the ideal $\mathfrak{C}_K$ is principal. It then follows from Theorem 3.7 (ii) that the field K has a power integral basis.

We now show that (iii) implies (ii). Assume that we are under the condition of (iii). By Corollary 3.14, we have that the ideal $\mathfrak{C}_K$ is principal, which implies by Theorem 3.8 that Δ_t/c_K or $\Delta_t^2/c_K \in \mathbb{N}^3$. Note that since $K \neq \mathbb{Q}(\zeta_9 + \zeta_9^{-1})$, there exists a prime $p \neq 3$ dividing c_K. By Proposition 3.11, we have that

$$v_p(c_K) = 1. \tag{27}$$

Fix the prime p satisfying (27). Under the condition (iii), i.e. $v_p(\Delta_t) \not\equiv 2 \pmod 3$, we see that $\Delta_t^2/c_K \notin \mathbb{N}^3$. So we have $\Delta_t/c_K \in \mathbb{N}^3$ as desired.

To complete the proof we need to show that (ii) implies (iii). Note that by Proposition 3.12 we have that $3|c_K$ if and only if $t \equiv 0, 6 \pmod 9$ or $t \equiv 3, 21 \pmod{27}$ and $3 \nmid c_K$ if and only if $3 \nmid t$ or $t \equiv 12 \pmod{27}$. Since (ii) holds, we have

$$v_p(\Delta_t) \equiv v_p(c_K) \pmod 3 \text{ for all primes } p. \tag{28}$$

Recall that we have proved (i) is equivalent to (ii), which implies that the ideal $\mathfrak{C}_K$ is principal by Theorem 3.7. It then follows from Theorem 3.8 that $\mathfrak{C}_K$ is principal if and only if

$$v_p(\Delta_t) \equiv e v_p(c_K) \pmod 3 \text{ with } e \in \{1, 2\} \text{ for all primes } p. \tag{29}$$

Observe the following:

Case I. If $3 \nmid c_K$, then $3 \nmid t$ or $t \equiv 12 \pmod{27}$ and $\mathfrak{C}_K$ is principal if and only if $v_p(\Delta_t) \equiv 1$ or $2 \pmod 3$ for all p dividing c_K by Proposition 3.11 and (29).

Case II. If $3|c_K$, then $t \equiv 0, 6 \pmod 9$ or $t \equiv 3, 21 \pmod{27}$ and $\mathfrak{C}_K$ is principal if and only if $v_3(\Delta_t) = 2$ and $v_p(\Delta_t) \equiv 1 \pmod 3$ for all $p \neq 3$ dividing c_K by Propositions 3.11, 3.12, 3.13 and (29). Here we find $v_3(\Delta_t) = 2$ or 3 by Proposition 3.12. It then must be 2 by (29). Therefore, $e = 1$, by Proposition 3.11. Again, by Propositions 3.11, 3.13, we get the result.

Since we are assuming (ii), we can deduce from Case I and II the following cases:

a) $v_p(\Delta_t) \not\equiv 1 \pmod 3$ for all primes p and $3 \nmid t$ or $t \equiv 12 \pmod{27}$;
b) $v_p(\Delta_t) \not\equiv 2 \pmod 3$ for all primes p and $3 \nmid t$ or $t \equiv 12 \pmod{27}$.
c) $v_3(\Delta_t) = 2$, $v_p(\Delta_t) \equiv 1 \pmod 3$ for all $p \neq 3$ dividing c_K and $t \equiv 0, 6 \pmod 9$.

Since $K \neq \mathbb{Q}(\zeta_9 + \zeta_9^{-1})$, by Proposition 3.11 there exists a prime p such that $v_p(c_K) = 1$, which implies that a) cannot hold by (28). Observe that under these conditions, (iii) holds if b) or c) holds true, which completes the proof. □

3.3. Pure Cubic Fields

A *pure field* is an extension of $\mathbb{Q}$ of the form $\mathbb{Q}(\sqrt[n]{m})$ for some $n \in \mathbb{Z}$ and $m \in \mathbb{Z} - \{0, \pm 1\}$ such that $\sqrt[n]{m} \notin \mathbb{Q}$. In particular, if $n = 3$ the fields $K = \mathbb{Q}(\sqrt[3]{m})$ are called *pure cubic fields*. The main references for this section are [19] and [20].

In [21], Spearman and Williams gave an explicit formula for the integral basis of pure cubic fields. The conditions for the existence of power integral bases of pure cubic fields in terms of the index form equation are given by El Fadil in [20] (Theorem 3.15). However, in [19], Gaál and Remete calculated the index form equations $I(x, y) = \pm 1$ associated to pure cubic fields when m is square-free.

Theorem 3.15. *Let $m = ab^2$ be cube-free integer, a and b be square-free integers such that $(a, b) = 1$. Consider the field $K = \mathbb{Q}(\sqrt[3]{m})$.*

(i) If $m^2 \not\equiv 1 \pmod 9$, the field K is monogenic if and only if the index form equation $I(x, y) = bx^2 - ay^3 = \pm 1$. has a solution.

(ii) If $m^2 \equiv 1 \pmod 9$, the field K is monogenic if and only if the index form equation $I(x, y) = 4xy^2a^2b^3 + 3bx^3 - 6x^2yab^2 - \frac{1}{9}y^3a(8a^2b^4 + 1) = \pm 1$ has a solution.

Proof. See [20, Theorem 1.4]. □

Corollary 3.16. *Let m be a cubic free integer such that $m^2 \not\equiv 1 \pmod 9$. If $m = \pm n(n+1)^2$ or $m = \pm(n+1)n^2$ or m is square free or $m = \pm b^2$, then K is monogenic.*

The corollary is an easy result of Theorem 3.15 (see also [20, Corollary 1.5]). Assume that m is a square-free integer with $m \neq 0, \pm 1$ and $n > 2$. Consider the field $K = \mathbb{Q}(\sqrt[n]{m})$ with $v = \sqrt[n]{m}$. We first state a theorem regarding the prime divisors of the denominators of the integral basis elements:

Theorem 3.17. *If $\{1, v, \ldots, v^{n-1}\}$ is not an integral basis in K, then for any element*

$$\alpha = \frac{a_0 + a_1 v + \cdots + a_{n-1}v^{n-1}}{q} \tag{30}$$

of the integral basis where $a_0, \ldots, a_{n-1}$, $q \in \mathbb{Z}_{>0}$ the denominator q can only be divisible by primes dividing n, the prime factors of q do not divide m.

Proof. See [19, Theorem 1]. □

Note that Theorem 3.17 implies [22, Theorem 3.1], which we will state as a corollary.

Corollary 3.18. *If all the prime factors of n divide m then $\mathbb{Q}(\sqrt[n]{m})$ is monogenic. In particular, if $m \neq 0$ is a square-free integer such that $m \equiv 0 \pmod 3$, then the field $\mathbb{Q}(\sqrt[3]{m})$ is monogenic.*

We now show that the integral bases of are $\mathbb{Q}(\sqrt[n]{m})$ periodic, which will lead us to list explicit integral bases and associated index forms.

Theorem 3.19. *Let $n = p_1^{h_1} \dots p_k^{h_k}$ and $n_0 = p_1^{\lfloor nh_1/2 \rfloor} \dots p_k^{\lfloor nh_k/2 \rfloor}$ where $\lfloor \cdot \rfloor$ denotes the floor function. Let $v = \sqrt[n]{m}$ and $\gamma = \sqrt[n]{m + n_0^n}$. Then the structures of the integral bases of the fields $\mathbb{Q}(v)$ and $\mathbb{Q}(\gamma)$ are the same in terms of v and γ.*

Proof. See [19, Theorem 2]. □

What we mean by having the same structure is the following: if the integral basis of $\mathbb{Q}(v)$ is given by

$$\left\{1, \frac{a_{10} + a_{11}v}{q_1}, \dots, \frac{a_{n0} + a_{n1}v + \dots + a_{n(n-1)}v^{n-1}}{q_n}\right\},\ a_{ij}, q_i \in \mathbb{Z} \tag{31}$$

then the integral basis of $\mathbb{Q}(\gamma)$ is

$$\left\{1, \frac{a_{10} + a_{11}\gamma}{q_1}, \dots, \frac{a_{n0} + a_{n1}\gamma + \dots + a_{n(n-1)}\gamma^{n-1}}{q_n}\right\} \tag{32}$$

and vice versa.

It follows from Theorem 3.19 that the integral bases of $K = \mathbb{Q}(\sqrt[n]{m})$ are periodic modulo n_0^n. For $n \in \{3, \dots, 9\}$, we can be more precise.

Theorem 3.20. *For $3 \leq n \leq 9$ the integral bases of $\mathbb{Q}(\sqrt[n]{m})$ are periodic in m modulo n^2.*

Proof. See [19, Theorem 3]. □

Utilizing the periodicity we can find explicit integral bases of the field $\mathbb{Q}(\sqrt[n]{m})$ for $3 \leq n \leq 9$. Then we can calculate the associated index form to derive the monogenity of the field. Here we present examples only regarding the pure cubic fields. For the cases where $n \in \{1, \ldots, 9\}$ we refer to [19, Section 5] and [8, Section 12.2].

Let $K = \mathbb{Q}(\sqrt[3]{m})$ where $m \neq 0, \pm 1$ is square-free and set $m = r + 9k$ for some $k \in \mathbb{Z}$ and $1 < r < 9$. We have the following three cases:

Case I. $r = 2, 3, 4, 5, 6, 7$, $m = r + 9k$ is square-free

$$\begin{aligned} B = \{1, \alpha, \alpha^2\} \quad &, \; D_K = -27m^2 \\ I(x, y) \quad &= x^3 - my^3 \end{aligned} \tag{33}$$

Obviously, these fields are monogenic; $(1, 0)$ is a solution of the index form equation.

Case II. $r = 1$, $m = 1 + 9k$ is square-free

$$\begin{aligned} B = \{1, \alpha, \quad &\tfrac{1+\alpha+\alpha^2}{3}\}, \; D_K = -3m^2 \\ I(x, y) \quad &= 3x^3 + 3x^2y + xy^3 - ky^3 \end{aligned} \tag{34}$$

In this case the index form equation is solvable for example when $k = 27, 37$ but not solvable for example when $k = 10, 11, 12$.

Case III. $r = 8$, $m = 8 + 9k$ is square-free

$$\begin{aligned} B = \{1, \alpha, \quad &\tfrac{1+2\alpha+\alpha^2}{3}\}, \; D_K = -3m^2 \\ I(x, y) \quad &= 3x^3 + 6x^2y + 4xy^3 - ky^3 \end{aligned} \tag{35}$$

In this case the index form equation is solvable for example when $k = 1, 4, 12$ but not solvable for example when $k = 2, 3, 5, 6, 7$.

Observe that all the index form equations we computed in Cases I, II and III are relatively simpler than the ones given in Theorem 3.15.

3.4. Cubic Monogenic Fields with the Same Discriminant

In this section, we will study the monogenity of cubic fields that have the same discriminant. For number fields, monogenity is not always guaranteed, and we also know that having the same discriminant is an uncommon phenomena as well. First, we will prove that there exist infinitely many triples of polynomials defining distinct monogenic cubic fields with the same discriminant. After this, we will give some examples of these kind of fields. The main reference is [23] for this section. The proof of the following theorem will be given in Section 3.4.1.

Theorem 3.21. *There exist infinitely many pairs of relatively prime integers* (p, q) *that satisfy* $p \equiv \pm 1 \pmod 3$, $q \equiv \pm 1 \pmod 3$, *and*

$$p(3p^4 - 6p^2q^2 - q^4) \tag{36}$$

is squarefree. For each such pair (p, q), *the polynomials*

$$\begin{aligned} f_1(x) &= x^3 - 9p(p+q)x - 3p(3p^2 + 6pq + q^2), \\ f_2(x) &= x^3 - 9p^2x - 3p(3p^2 + q^2), \\ f_3(x) &= x^3 - 9p(p-q)x - 3p(3p^2 - 6pq + q^2) \end{aligned} \tag{37}$$

define distinct monogenic cubic fields with the same discriminant. Furthermore, the set of integers defined in (36) *is infinite.*

Let $p(3p^4 - 6p^2q^2 - q^4)$ be a squarefree integer with $p, q \equiv \pm 1 \pmod 3$ and the polynomials f_1, f_2, and f_3 be given in (37). Set $K_i = \mathbb{Q}(\theta_i)$, where θ_i is a root of f_i with $i \in \{1, 2, 3\}$.

Lemma 3.22. *The polynomials f_1, f_2, and f_3 are irreducible over $\mathbb{Q}$ and have the same polynomial discriminant.*

Proof. It is easy to see that 3 exactly divides all the coefficients of f_1, f_2, and f_3 but, 3^2 does not divide their constant terms since 3 does not divide p and q. Hence, by Eisenstein's criterion, they are irreducible. The discriminant of each f_i for $i \in \{1, 2, 3\}$ is equal to $D(f_i) = 3^5p^2(3p^4 - 6p^2q^2 - q^4)$. Hence, it can be seen that the fields K_i share the same discriminant. □

Lemma 3.23. *The fields K_1, K_2, and K_3 are monogenic.*

Proof. See [23, Lemma 2]. □

Lemma 3.24. *The fields K_1, K_2, and K_3 are distinct.*

Proof. See [23, Lemma 3]. □

Let k and n be integers. We say that n is *k-free* if n is not divisible by k-th power of a prime. Let

$$F(X, Y) = a_rX^r + a_{r-1}X^{r-1}Y + \cdots + a_0Y^r \tag{38}$$

be a binary form with integer coefficient and positive degree r. Let w be the largest positive integer such that w^k divides $F(A, B)$ for all integers a, b with $a \equiv A \pmod{M}$ and $b \equiv B \pmod{M}$.

For any real number x, let $R_k(x)$ denote the number of k-free integers t with $|t| \leq x$ for which there are integers a and b with $a \equiv A \pmod{M}$ and $b \equiv B \pmod{M}$ and $F(A, B) = tw^k$.

We will apply the following theorem to deduce that there are infinitely many pairs (p, q) such that $p \equiv \pm 1 \pmod 3$, $q \equiv \pm 1 \pmod 3$, and $p(3p^4 - 6p^2q^2 - q^4)$ is squarefree.

Theorem 3.25. *Let A, B, M and k be integers with $M \geq 1$ and $k \geq 2$. Let F, as in (38), be a binary form with integer coefficient, non-zero discriminant and degree $r \geq 3$. Let m be the largest degree of an irreducible factor of F over $\mathbb{Q}$ and suppose that $m \leq 2k + 1$ or that $k = 2$ and $m = 6$. There are positive numbers C_{15} and C_{16} which depend on M, k and F such that if x is a real number larger that C_{15}, then*

$$R_k(x) > C_{16}x^{\frac{2}{r}} \tag{39}$$

Proof. See [24, Theorem 1]. □

3.4.1. Proof of Theorem 3.21

Let the polynomials f_1, f_2 and f_3 be given as in (37). It follows from Lemma 3.22 that f_1, f_2 and f_3 are irreducible over $\mathbb{Q}$ and they have the same discriminant. We know that $K_1 = \mathbb{Q}(\theta_1)$, $K_2 = \mathbb{Q}(\theta_2)$ and $K_3 = \mathbb{Q}(\theta_3)$ where θ_i with $i \in \{1, 2, 3\}$ are monogenic fields by Lemma 3.23. We also get that the fields K_1, K_2 and K_3 are all distinct by Lemma 3.24. To complete the proof we need to show that there are infinitely many integer pairs (p, q) satisfy $p \equiv \pm 1 \pmod 3$, $q \equiv \pm 1 \pmod 3$, and the equation (36) is squarefree. We apply Theorem 3.25 with $A = \pm 1$, $B = \pm 1$, $M = 3$, $m = 4$, $w = 1$, $r = 5$, $k = 2$, $F(p, q) = p(3p^4 - 6p^2q^2 - q^4)$. As x approaches ∞, we deduce that there are infinitely many integers as in (36), which implies that there are infinitely many fields whose discriminants satisfy the assertion given in the Theorem 3.21.

3.4.2. Examples

Let θ_i denote a root of f_i for each $i \in \{1, 2, 3\}$. Table 3.3 illustrates some examples of polynomials f_1, f_2, f_3 which are distinct monogenic fields over $\mathbb{Q}$ with the same discriminant.

Table 3.3. Integral bases and discriminants for $K = \mathbb{Q}(\theta_i)$ defined by f_i for $i \in 1, 2, 3$.

(p, q)	f_i	$D(f_i)$	Integral Basis for $K_i = \mathbb{Q}(\theta_i)$
(2,1)	$f_1 = x^3 - 54x - 150$ $f_2 = x^3 - 36x - 78$ $f_3 = x^3 - 18x - 6$	$22356 = 2^2 \cdot 3^5 \cdot 23$	$\{1, \theta_i, \theta_i^2\}$
(1,2)	$f_1 = x^3 - 27x - 57$ $f_2 = x^3 - 9x - 21$ $f_3 = x^3 + 9x + 15$	$-8991 = -3^5 \cdot 37$	$\{1, \theta_i, \theta_i^2\}$
(1,5)	$f_1 = x^3 - 54x - 174$ $f_2 = x^3 - 9x - 84$ $f_3 = x^3 + 36x^2 + 6$	$-187596 = 2^2 \cdot 3^5 \cdot 193$	$\{1, \theta_i, \theta_i^2\}$
(2,7)	$f_1 = x^3 - 162x - 726$ $f_2 = x^3 - 36x - 366$ $f_3 = x^3 + 90x - 6$	$-3430188 = -2^2 \cdot 3^5 \cdot 3529$	$\{1, \theta_i, \theta_i^2\}$

Additionally, Table 3.4 gives us an example of four polynomials having the same discriminant and generating distinct monogenic fields. Note that this is the only example that is known so far. Let θ_i be a root of the polynomials f_i given in Table 3.4 and set $K_i = \mathbb{Q}(\theta_i)$ for $i \in \{1, 2, 3, 4\}$.

Table 3.4. Integral bases and discriminants for $K = \mathbb{Q}(\theta_i)$ defined by f_i for $i \in 1, 2, 3, 4$.

f_i	$D(f_i)$	Integral Basis for $K_i = \mathbb{Q}(\theta_i)$
$f_1 = x^3 - 990x^2 - 10830$ $f_2 = x^3 - 900x^2 - 9030$ $f_3 = x^3 - 810x^2 - 7230$ $f_4 = x^3 - 720x^2 + 5370$	$714395700 = 2^2 \cdot 3^5 \cdot 5^2 \cdot 29399$	$\{1, \theta_i, \theta_i^2\}$

Example 3.26. *For* $(p, q) = (2, 1)$ *consider the polynomials* f_1, f_2, f_3, *and from Example 3.1 we take the polynomials* f_4, f_5, f_6 *given in Table 3.5. The discriminant of those polynomials is* $22356 = 2^2 \cdot 3^5 \cdot 23$. *Set* $K = \mathbb{Q}(\theta_i)$, *where* θ_i *is a root of* f_i *with* $i = 1, 2, 3, 4, 5, 6$. *One can observe that the fields* K_i *are all distinct and monogenic.*

Table 3.5. Integral bases and discriminants for $K = \mathbb{Q}(\theta_i)$ defined by f_i for $i \in 1, 2, 3, 4, 5, 6$.

f_i	$D(f_i)$	Integral Basis for $K_i = \mathbb{Q}(\theta_i)$
$f_1 = x^3 - 54x - 150$		
$f_2 = x^3 - 36x - 78$		
$f_3 = x^3 - 18x - 6$	$22356 = 2^2 \cdot 3^5 \cdot 23$	$\{1, \theta_i, \theta_i^2\}$
$f_4 = x^3 - 36x + 60$		
$f_5 = x^3 - 16x + 6$		
$f_6 = x^3 - 36x + 78$		

4. LIFTING MONOGENIC CUBIC FIELDS TO SEXTIC FIELDS

Let C_n, S_n D_n and A_n denote the cyclic group $\mathbb{Z}/n\mathbb{Z}$, the symmetric group on n letters, the dihedral group of order $2n$ and the alternating subgroup of S_n, respectively. Let $K = \mathbb{Q}(\theta)$ be a number field of degree n, where $f(x)$ denotes the minimal polynomial of θ over $\mathbb{Q}$. Let $\mathrm{Gal}(f)$ denote the Galois group of the splitting field of f over $\mathbb{Q}$. It then follows from [25, Proposition 6.3.1] that $\mathrm{Gal}(f) \subset A_n$ if and only if the discriminant $D(f)$ is a square. So, following [25, Section 6.3], we will use the notation (+ sign) or (− sign) to express whether a subgroup of S_n is contained in A_n or not.

It follows from [25, Algorithm 6.3.10] that a sextic field contains a cubic subfield if and only if its Galois group is isomorphic to a transitive subgroup of $S_4 \times C_2$. These subgroups correspond to the groups $(C_6, -)$, $(S_3, -)$, $(D_6, -)$, $(A_4, +)$, $(S_4, +)$, $(S_4, -)$, $(A_4 \times C_2, -)$ and $(S_4 \times C_2, -)$. Note that the group S_4 occurs as two different conjugacy classes in S_6; the one which is in A_6, the other which is not. This is why we use the notation $(S_4, +)$ and $(S_4, -)$.

In this chapter, we will focus on the monogenity of sextic fields containing a cubic subfield. As mentioned above for such fields there are eight possible Galois groups classified by Cohen in [25, Section 6.3]: $(C_6, -)$, $(S_3, -)$, $(D_6, -)$, $(A_4, +)$, $(S_4, +)$, $(S_4, -)$, $(A_4 \times C_2, -)$ and $(S_4 \times C_2, -)$. For the groups $(A_4, +)$, $(A_4 \times C_2, -)$, $(S_4, +)$, $(S_4 \times C_2, -)$, $(D_6, -)$, we will construct infinitely many monogenic sextic fields such that the Galois group of the defining polynomial is isomorphic to one of these five groups. For the others, we will show that there are at most finitely many monogenic sextic fields. Moreover, we will introduce the notion of lifting a cubic number field to a sextic number field and state main theorem in this regard. The main references for this chapter are [25], [3] and [26].

Definition 4.1. *Suppose that we have a monogenic cubic field C defined by the polynomial $g(x) = x^3 + ax^2 + bx + c$ where $a, b, c \in \mathbb{Z}$. If the sextic number field K defined by the polynomial $f(x) = g(x^2) = x^6 + ax^4 + bx^2 + c$ defines a monogenic sextic field then we say that the field C lifts to K.*

Throughout the section, we will be interested in the case where $g(x) = x^3 + ax^2 + bx \pm 1$ for $a, b \in \mathbb{Z}$. The following theorem (see also [3, Theorem 1.1]) gives us the criteria for which a and b one can obtain a monogenic sextic number field lifted from a monogenic cubic number field. We will give the proof of this theorem below in Section 4.1.

Theorem 4.2. *Let d be an integer given in the first column of Table 4.1 and define $f_d(x)$ which is placed in the second column. Let $K_d = \mathbb{Q}(\theta_d)$ be a number field, where θ_d is a root of $f_d(x)$. Then there are infinitely many d such that*

(i) $[K_d : \mathbb{Q}] = 6$,

(ii) $\mathrm{Gal}(f_d)$ *is as given in the third column of Table 4.1,*

(iii) K_d *is monogenic with integral basis* $\{1, \theta_d, \theta_d^2, \theta_d^3, \theta_d^4, \theta_d^5\}$. *Moreover, the fields* K_d *are distinct.*

Table 4.1. The integers d that make K_d monogenic I.

$d \in \mathbb{Z}$	$f_d(x)$	$\mathrm{Gal}(f_d)$
$4d^2 + 2d + 7$ squarefree	$x^6 + (2d+2)x^4 + (2d-1)x^2 - 1$	A_4
$4d^2 + 2d + 7$ squarefree	$x^6 - (2d+2)x^4 + (2d-1)x^2 + 1$	$A_4 \times C_2$
$d > 3$ odd, $4d^3 - 27$ squarefree	$x^6 - dx^2 - 1$	$(S_4, +)$
$d > 3$ odd, $4d^3 - 27$ squarefree	$x^6 - dx^2 + 1$	$S_4 \times C_2$
$d > 3$ odd, $4d^3 - 27$ squarefree	$x^6 + 2dx^4 + d^2x^2 + 1$	D_6

Further, there exist only finitely many integers a and b such that

(iv) $g(x) = x^3 + ax^2 + bx \pm 1$ *defines a monogenic cubic field with an integral basis* $\{1, \alpha, \alpha^2\}$, *where* $\alpha \in C$ *is a root of* $g(x)$,

(v) $f(x) = g(x^2) = x^6 + ax^4 + bx \pm 1$ *defines a monogenic cubic field with an integral basis* $\{1, \theta, \theta^2, \theta^3, \theta^4, \theta^5\}$, *where* $\theta \in K$ *is a root of* $f(x)$,

(vi) $\mathrm{Gal}(f) \in \{C_6, S_3, (S_4, -)\}$.

We omit the proof and refer to [3].

Lemma 4.3. *Let $g(x) = x^3 + ax^2 + bx + 1 \in \mathbb{Z}[x]$ and let α be a root of $g(x)$. Suppose that $g(x)$ defines a monogenic cubic field C and that $\{1, \alpha, \alpha^2\}$ is a power basis of C. Let $f(x) = x^6 + ax^4 + bx^2 + 1$ and suppose that θ is a root of $f(x)$. Let $K = \mathbb{Q}(\theta)$ with $[K : \mathbb{Q}] = 6$. Then K is monogenic with power basis $\{1, \theta, \theta^2, \theta^3, \theta^4, \theta^5\}$ if and only if*

$$(a, b) \not\equiv (0, 2), (1, 1), (2, 0), (2, 2), (3, 3) \pmod 4. \tag{1}$$

Proof. See [3, Lemma 2.1]. □

Lemma 4.4. *Let $g(x) = x^3 + ax^2 + bx - 1 \in \mathbb{Z}[x]$ and let α be a root of $g(x)$. Suppose that $g(x)$ defines a monogenic cubic field C and that $\{1, \alpha, \alpha^2\}$ is a power basis of C. Let $f(x) = x^6 + ax^4 + bx^2 - 1$ and suppose that θ is a root of $f(x)$. Let $K = \mathbb{Q}(\theta)$ with $[K : \mathbb{Q}] = 6$. Then K is monogenic with power basis $\{1, \theta, \theta^2, \theta^3, \theta^4, \theta^5\}$ if and only if*

$$(a, b) \not\equiv (0, 0), (2, 1), (2, 2), (1, 3), (3, 1), (3, 2) \pmod 4. \tag{2}$$

Proof. See [3, Lemma 2.2]. □

Lemma 4.5. *There exist at most finitely many polynomials $f(x) = x^6 + ax^4 + bx^2 \pm 1$ irreducible over $\mathbb{Q}$ with $\mathrm{Gal}(f) = C_6, S_3$ or $(S_4, -)$; and such that a root of $f(x)$ is a monogenic generator of a sextic field and a root of $x^3 + ax^2 + bx \pm 1$ is a monogenic generator of a cubic field.*

Proof. See [3, Lemma 2.4]. □

Lemma 4.6. *Let d be an integer given in the first column of Table 4.2 and define $f_d(x)$ as in the second column. Then $f_d(x)$ is irreducible and the Galois group* $\mathrm{Gal}(f_d)$ *of $f_d(x)$ is isomorphic to the groups given in the third column.*

Table 4.2. The integers d that make K_d monogenic II.

d	$f_d(x)$	$\mathrm{Gal}(f_d)$
$d \in \mathbb{Z}$	$x^6 + (2d+2)x^4 + (2d-1)x^2 - 1$	A_4
$d \in \mathbb{Z}$	$x^6 - (2d+2)x^4 + (2d-1)x^2 + 1$	$A_4 \times C_2$
$d \in \mathbb{Z}$, $d > 3$ odd	$x^6 - dx^2 - 1$	$(S_4, +)$
$d \in \mathbb{Z}$, $d > 3$ odd	$x^6 - dx^2 + 1$	$S_4 \times C_2$
$d \in \mathbb{Z}$, $d \not\equiv 0, 2, 3,$	$x^6 + 2dx^4 + d^2x^2 + 1$	D_6

Proof. See [3, Lemma 2.3]. □

The lemmas we have stated so far were for the first three cases of Theorem 4.2. We need the following lemmas for the cases (iv), (v) and (vi) of Theorem 4.2.

Lemma 4.7. *Let $f(x) = x^3 - ax + b \in \mathbb{Z}[x]$ be an irreducible polynomial. Let $\Delta = 4a^3 - 27b^2 \neq 0$. For prime p set $s_p = v_p(\Delta)$ and $\Delta_p = \frac{\Delta}{p^{s_p}}$.*

Moreover, if p is a prime then $v_p(a) < 2$ or $v_p(b) < 3$. Set $K = \mathbb{Q}(\alpha)$ where α is a root of $f(x)$. Then

$$D_K = \mathrm{sgn}(\Delta) 2^{\alpha} 3^{\beta} \prod_{\substack{p>3, \\ s_p \text{ odd}}} p \prod_{\substack{p>3, \\ 1 \le v_p(b) \le v_p(a)}} p^2, \tag{3}$$

where

$$\alpha = \begin{cases} 3, & \text{if } s_2 \equiv 1 \pmod 2, \\ 2, & \text{if } 1 \le v_p(b) \le v_p(a) \text{ or } s_2 \equiv 0 \pmod 2 \text{ and } \Delta_2 \equiv 3 \pmod 4, \\ 0, & \text{otherwise}, \end{cases} \tag{4}$$

and

$$\beta = \begin{cases} 5, & \text{if } 1 \le v_3(b) \le v_3(a), \\ 4, & \text{if } v_3(a) = v_3(b) = 2 \text{ or} \\ & a \equiv 3 \pmod 9, b \not\equiv 0 \pmod 3, b^2 \not\equiv 4 \pmod 9 \\ 3, & \text{if } v_3(a) = v_3(b) = 1 \text{ or} \\ & a \equiv 0 \pmod 3, b \not\equiv 0 \pmod 3, a \not\equiv 3 \pmod 9, b^2 \not\equiv a+1 \pmod 9 \text{ or} \\ & a \equiv 3 \pmod 9, b^2 \equiv 4 \pmod 9, b^2 \equiv a+1 \pmod{27}, \\ 1, & \text{if } 1 = v_3(a) < v_3(b) \text{ or} \\ & a \equiv 0 \pmod 3, a \not\equiv 3 \pmod 9, b^2 \not\equiv a+1 \pmod 9 \text{ or} \\ & a \equiv 3 \pmod 9, b^2 \equiv a+1 \pmod{27}, s_3 \equiv 1 \pmod 2, \\ 0, & \text{if } 3 \not| a \text{ or} \\ & a \equiv 3 \pmod 9, b^2 \equiv a+1 \pmod{27}, s_3 \equiv 0 \pmod 2. \end{cases} \tag{5}$$

Proof. See [3, Lemma 3.1]. □

Lemma 4.8. *Let d be an integer given in the first column of Table 4.3 and define $g_d(x)$ as in the second column. Let $C_d := \mathbb{Q}(\alpha_d)$ denote the field generated by a root α_d of $g_d(x)$. Then field discriminant D_{C_d} is given in the third column.*

Table 4.3. The integers d that make D_{C_d} field discriminant.

$d \in \mathbb{Z}$	$g_d(x)$	D_{C_d}
$4d^2+2d+7$ squarefree	$x^3+(2d+2)x^2+(2d-1)x-1$	$(4d^2+2d+7)^2$
$4d^2+2d+7$ squarefree	$x^3-(2d+2)x^2+(2d-1)x+1$	$(4d^2+2d+7)^2$
$d>3$ odd, $4d^3-27$ squarefree	x^3-dx-1	$4d^3-27$
$d>3$ odd, $4d^3-27$ squarefree	x^3-dx+1	$4d^3-27$
$d>3$ odd, $4d^3-27$ squarefree	$x^3+2dx^2+d^2x+1$	$4d^3-27$

Proof. Assume for $d \in \mathbb{Z}$ we have $4d^2 + 2d + 7$ squarefree and define

$$g_d(x) = x^3 - (2d+2)x^2 + (2d-1)x + 1. \tag{6}$$

By Rational Root theorem, the polynomial $g_d(x)$ is irreducible over $\mathbb{Q}$ for $d \in \mathbb{Z}$ since ± 1 is not a root of $g_d(x)$. We now need to find the field discriminant of the cubic field defined by $g_d(x)$. First, let eliminate the x^2 term of the polynomial $g_d(x)$ by using the transformation

$$x \to x + \frac{2d+2}{3} \tag{7}$$

followed by the scaling transformation $x \to \frac{x}{3}$. We get the polynomial

$$h_d(x) = x^3 - 3(4d^2 + 2d + 7)x - (4d+1)(4d^2 + 2d + 7) \tag{8}$$

with the discriminant $\Delta = 3^6(4d^2 + 2d + 7)^2$.

By Lemma 4.7, one can see the discriminant D_K of the cubic field K generated by a root of the polynomial $h_d(x)$ is of the form,

$$D_K = \operatorname{sgn}(\Delta) 2^\alpha 3^\beta \prod_{\substack{p>3, \\ s_p \text{ odd}}} p \prod_{\substack{p>3, \\ 1 \le v_p(b) \le v_p(a)}} p^2. \tag{9}$$

It can be seen that 2 does not divide Δ, so $\alpha = 0$. Therefore, since $4d^2 + 2d + 7 = \frac{(4d+1)^2+27}{4}$ and $4d^2 + 2d + 7$ is squarefree, we can deduce that $3 \not| (4d^2 + 2d + 7)$ so that $d \equiv 0, 1 \pmod 3$. For the values of β in Lemma 4.7 with

$$a = 3(4d^2 + 2d + 7), \quad b = -(4d+1)(4d^2 + 2d + 7). \tag{10}$$

We note that $a \equiv 3 \pmod 9$, $b^2 \equiv a+1 \pmod 9$ for all $d \equiv 0, 1 \pmod 3$. Finally, $s_3 = 6$ so that $s_3 \equiv 0 \pmod 2$. So, $\beta = \alpha = 0$. Therefore, we have

$$\prod_{\substack{p>3, \\ 1 \le v_p(b) \le v_p(a)}} p^2 = (4d^2 + 2d + 7)^2, \tag{11}$$

which completes the proof.

□

4.1. Proof of Theorem 4.2

We will first prove (i), (ii) and (iii) of Theorem 4.2. Note that for the group $(A_4, +)$, the theorem is proven in [27] and the strategy is exactly the same as in the proof of $(A_4 \times C_2, -)$. So we omit this case.

It follows from [26, Theorem 6.1.10] (or see [28]) that there are infinitely many $d \in \mathbb{Z}$ such that the quadratic $4d^2 + 2d + 7$ is square-free. Define $g_d(x) := x^3 - (2d + 2)x^2 + (2d - 1)x + 1$ and let $C_d := \mathbb{Q}(\alpha_d)$ denote the field generated by a root α_d of $g_d(x)$. Since ± 1 is not a root of $g_d(x)$, by Rational Root theorem, the polynomial $g_d(x)$ is irreducible, which implies that C_d is a cubic field. Note that we have

$$D(g_d) = (4d^2 + 2d + 7)^2 = D_{C_d}, \tag{12}$$

so by Theorem 2.24 that $\{1, \alpha_d, \alpha_d^2\}$ is a power integral basis for the field C_d. Put

$$f_d(x) := x^6 - (2d + 2)x^4 + (2d - 1)x^2 + 1 \tag{13}$$

and let $K_d := \mathbb{Q}(\theta_d)$ denote the lift of C_d generated by a root θ_d of $f_d(x)$. It follows from Lemma 4.6 that the polynomial $f_d(x)$ is irreducible, so $[K_d : \mathbb{Q}] = 6$, the Galois group $\mathrm{Gal}(f_d)$ is isomorphic to $A_4 \times C_2$. Observe that the cubic fields C_d have distinct discriminants, so they are distinct. Therefore, the fields K_d are also distinct. It remains to show that K_d is monogenic. Recall that by Lemma 4.3 the field K_d is monogenic with power integral basis $\{1, \theta_d, \ldots, \theta_d^5\}$ if and only if

$$(a, b) = (-(2d + 2), (2d + 1)) \not\equiv (0, 2), (1, 1), (2, 0), (2, 2), (3, 3) \pmod 4. \tag{14}$$

Hence, there are infinitely many $d \in \mathbb{Z}$ such that $4d^2 + 2d + 7$ is square-free and K_d is monogenic with power integral basis $\{1, \theta_d, \ldots, \theta_d^5\}$.

The cases $S_4 \times C_2$, $(S_4, +)$ and D_6 will follow in a similar manner. Let $d > 3$ be an odd integer such that $4d^3 - 27$ is square-free.

In these cases, $g_d(x)$'s are $x^3 - dx - 1$, $x^3 - dx + 1$ and $x^3 + 2dx^2 + d^2x + 1$, respectively. Note that in all cases we have $D(g_d) = 4d^3 - 27 = D_{C_d}$. Hence, by Theorem 2.24 and the irreducibility of g_d, we deduce that the field $C_d = \mathbb{Q}(\alpha_d)$ generated by a root α_d of

$g_d(x)$ is a monogenic cubic field with power integral basis $\{1, \alpha_d, \alpha_d^2\}$. Observe that we have the followings

$$\begin{aligned}
(a,b) &= (0,-d) \not\equiv (0,0),(2,1),(2,2),(1,3),(3,1),(3,2) \pmod 4 \big(\text{ for } (S_4,+)\big)\\
(a,b) &= (0,-d) \not\equiv (0,2),(1,1),(2,0),(2,2),(3,3) \pmod 4 \big(\text{ for } S_4\times C_2\big)\\
(a,b) &= (2d,d^2) \not\equiv (0,2),(1,1),(2,0),(2,2),(3,3) \pmod 4 \big(\text{ for } D_6\big). \qquad (15)
\end{aligned}$$

Hence, by Lemma 4.3, 4.4 and 4.6, we deduce that the field $K_d = \mathbb{Q}(\theta_d)$ is monogenic with power integral basis $\{1, \theta_d, \ldots, \theta_d^5\}$, where θ_d is a root of $f_d(x) := g_d(x^2)$.

The assertions (iv), (v) and (vi) follow from Lemma 4.5, which completes the proof of Theorem 4.2. □

5. OUR RESULT

In this section, we will state our observation of the lifting of the monogenic cubic fields to monogenic sextic fields.

The following theorem is a combination of Theorem 3.4 and Lemma 4.4, which states that every monogenic cyclic cubic number field can be lifted to a monogenic number field of degree 6. In Theorem 4.2, they deal with only polynomials given in Table 1 and $g(x) = x^3 + ax^2 + bx \pm 1$ defined by finitely many integers a and b. Hence we have extended their result to all monogenic cyclic cubic number fields.

Lemma 5.1. *Let α_t be a root of the polynomial $g_t(x) = x^3 - tx^2 - (t+3)x - 1$ and set $C_t := \mathbb{Q}(\alpha_t)$. Let $f_t(x) = x^6 - tx^4 - (t+3)x^2 - 1$ with $t \in \mathbb{Z}$ and let θ_t be a root of $f_t(x)$ such that $\theta_t^2 = \alpha_t$. Set $K_t := \mathbb{Q}(\theta_t)$. Then $f_t(x)$ is irreducible, so that $[K_t : \mathbb{Q}] = 6$.*

Proof. Note that by Rational Root test, the polynomial does not have any root in $\mathbb{Q}$. Suppose that f_t is reducible. Since C_t is a subfield of degree 3, we have $3|[K_t : \mathbb{Q}]$, i.e. $[K_t : \mathbb{Q}] = 3$. Therefore, we deduce that θ_t is a root of a cubic irreducible polynomial in $\mathbb{Z}[x]$, say

$$h(x) = x^3 + ax^2 + bx + c. \tag{1}$$

It is easy to see that $-\theta_t$ is a root of $h(-x)$ and $h(-x) \neq -h(x)$. Since θ_t and $-\theta_t$ are both roots of $f_t(x)$, we see that

$$f_t(x) = -h(x)h(-x) = x^6 + (-a^2 + 2b)x^4 + (b^2 - 2ac)x^2 - c^2. \tag{2}$$

Comparing the coefficients we deduce that $c = \pm 1$ and

$$\begin{aligned} -t &= -a^2 + 2b \\ -(t+3) &= b^2 - 2ac. \end{aligned} \tag{3}$$

Eliminating $-t$, we see

$$(a-c)^2+(b-1)^2=-1, \tag{4}$$

which is a contradiction. Hence, $f_t(x)$ is irreducible. □

Theorem 5.2. *Let C be a cyclic cubic number field which is monogenic. Then there exists $-1 \leq t \in \mathbb{Z}$ such that $C=\mathbb{Q}(\alpha_t)$, where α_t is a root of $g_t(x)=x^3-tx^2-(t+3)x-1$. Further, let $f_t(x)=g_t(x^2)=x^6-tx^4-(t+3)x^2-1$ and suppose that θ_t is a root of $f_t(x)$ and $K_t:=\mathbb{Q}(\theta_t)$. Then K_t is monogenic with power basis $\{1,\theta_t,\theta_t^2,\theta_t^3,\theta_t^4,\theta_t^5\}$.*

Proof. Let C be a cyclic cubic number field having a power integral basis. It then follows from Theorem 3.4 that there exists $-1 \leq t \in \mathbb{Z}$ such that $C=\mathbb{Q}(\alpha_t)$, where α_t is a root of $g_t(x)=x^3-tx^2-(t+3)x-1$. Observe that

$$(-t,-(t+3)) \not\equiv (0,0),(2,1),(2,2),(1,3),(3,1),(3,2) \pmod 4 \tag{5}$$

since we can only have $(-t,-(t+3)) \equiv (0,1),(1,2),(2,3),(3,0) \pmod 4$. Hence, by Lemma 4.4 applied with $a=-t$ and $b=-(t+3)$, we deduce that $K_t=\mathbb{Q}(\theta_t)$ is monogenic with power integral basis $\{1,\theta_t,\theta_t^2,\theta_t^3,\theta_t^4,\theta_t^5\}$, since $f_t(x)$ is irreducible by Lemma 5.1.

□

6. CONCLUSION

In this thesis, we studied the monogenicity of cubic number fields and their lift to monogenic sextic number fields. The problem of describing the monogenity of cubic fields usually leads to solving some Diophantine equations, the so-called index form equations. One of the purposes of this thesis was to point out the structure of the index form equations for cubic fields and their relation to Thue equations.

Therefore, one can deduce that the study of monogenic number fields is directly related to other aspects of mathematics such as solving Diophantine equations.

The other aim of the thesis was to provide monogenic sextic fields which can be lifted from monogenic cubic fields. First, we listed all possible Galois groups for the Galois closure of a sextic field containing a cubic subfield, it turns out that there are eight such possible groups. We constructed infinitely many monogenic sextic fields such that the Galois group of the defining polynomial is isomorphic to one of these five groups. For the others, we proved that there are at most finitely many monogenic sextic fields.

The knowledge of power integral bases in a number field has important applications. The most straightforward benefit of a power integral basis is to have an easy way of performing arithmetic calculations in $\mathcal{O}_K$. This is one of the reasons why it is interesting to decide the monogenity of a number field. Hence, one may ask the following questions to improve our perspective:

- Can we determine the monogenity of higher degree number fields? The methods for solving the index form equations associated to such fields depend on describing the solutions of infinitely many Diophantine equations. Therefore, it is a source of motivation to work on these type of Diophantine equations.

- Can we describe efficient algorithms for determining the generators of power integral bases? If this is the case, to perform these algorithms, we need computer algebra systems like Maple and algebraic number theory packages like Kash, Magma, or Pari.
- Can we consider the problem of relative power integral bases? One needs relative analogues of the methods that have been used to determine the relative power integral bases.

Although there are some particular answers to the questions above, there is still room to expand our knowledge about number fields.

REFERENCES

1. Hasse, H., *Vorlesungen Über Zahlentheorie*, Die Grundlehren der mathematischen Wissenschaften, Band 59, Springer-Verlag, Berlin-New York, 1964.

2. Dedekind, R., "Uber den Zusammenhang zwischen der Theorie der Ideale und der Theorie der hoheren Kongruenzen", *Abhandlungen der Königlichen Gesellschaft der Wissenschaften zu Göttingen*, Vol. 23, pp. 1–23, 1878.

3. Lavallee, M. J., B. K. Spearman and K. S. Williams, "Lifting Monogenic Cubic Fields to Monogenic Sextic Fields", *Kodai Mathematical Journal*, Vol. 34, No. 3, pp. 410–425, 2011.

4. Dummit, D. S. and R. M. Foote, *Abstract Algebra*, John Wiley & Sons, Inc., Hoboken, NJ, third edn., 2004.

5. Marcus, D. A., *Number Fields*, Universitext, Springer, Cham, 2018.

6. Jarvis, F., *Algebraic Number Theory*, Springer Undergraduate Mathematics Series, Springer, Cham, 2014.

7. Evertse, J.-H. and K. Győry, *Discriminant Equations in Diophantine Number Theory*, Vol. 32, Cambridge University Press, Cambridge, 2017.

8. Gaál, I., *Diophantine Equations and Power Integral Bases*, Birkhäuser Boston, Inc., Boston, MA, 2002.

9. Gaál, I., "Power Integer Bases in Algebraic Number Fields", *Annales Universitatis Scientiarum Budapestinensis de Rolando Eötvös Nominatae. Sectio Computatorica*, Vol. 18, pp. 61–87, 1999.

10. Thue, A., "Über Annäherungswerte Algebraischer Zahlen.", *Journal für die reine*

und angewandte Mathematik, pp. 284 – 305, 1909.

11. Baker, A., *Transcendental Number Theory*, Cambridge Mathematical Library, Cambridge University Press, Cambridge, second edn., 1990.

12. Bugeaud, Y. and K. Győry, "Bounds for the Solutions of Thue-Mahler Equations and Norm Form Equations", *Acta Arithmetica*, Vol. 74, No. 3, pp. 273–292, 1996.

13. Sprindžuk, V. G., "Representation of Numbers by The Norm Forms with Two Dominating Variables", *Journal of Number Theory*, Vol. 6, pp. 481–486, 1974.

14. Gaál, I. and N. Schulte, "Computing All Power Integral Bases of Cubic Fields", *Mathematics of Computation*, Vol. 53, No. 188, pp. 689–696, 1989.

15. Shanks, D., "The Simplest Cubic Fields", *Mathematics of Computation*, Vol. 28, pp. 1137–1152, 1974.

16. Kashio, T. and R. Sekigawa, "The Characterization of Cyclic Cubic Fields with Power Integral Bases", *Kodai Mathematical Journal*, Vol. 44, No. 2, pp. 290–306, 2021.

17. Dummit, D. S. and H. Kisilevsky, "Indices in Cyclic Cubic Fields", *Number theory and algebra*, pp. 29–42, 1977.

18. Hoshi, A., "On Correspondence Between Solutions of a Family of Cubic Thue Equations and Isomorphism Classes of the Simplest Cubic Fields", *Journal of Number Theory*, Vol. 131, No. 11, pp. 2135–2150, 2011.

19. Gaál, I. and L. Remete, "Integral Bases and Monogenity of Pure Fields", *Journal of Number Theory*, Vol. 173, pp. 129–146, 2017.

20. El Fadil, L. h., "Computation of a Power Integral Basis of a Pure Cubic Number Field", *International Journal of Contemporary Mathematical Sciences*, Vol. 2, No. 13-16, pp. 601–606, 2007.

21. Spearman, B. K. and K. S. Williams, "An Explicit Integral Basis for a Pure Cubic Field", *Far East Journal of Mathematical Sciences*, Vol. 6, No. 1, pp. 1–14, 1998.

22. Hameed, A., T. Nakahara, S. M. Husnine and S. Ahmad, "On Existence of Canonical Number System in Certain Classes of Pure Algebraic Number Fields", *Journal of Prime Research in Mathematics*, Vol. 7, pp. 19–24, 2011.

23. Davis, C. T., B. K. Spearman and J. Yoo, "Cubic Polynomials Defining Monogenic Fields with the Same Discriminant", *Journal de Théorie des Nombres de Bordeaux*, Vol. 30, No. 3, pp. 991–996, 2018.

24. Stewart, C. L. and J. Top, "On Ranks of Twists of Elliptic Curves and Power-free Values of Binary Forms", *Journal of the American Mathematical Society*, Vol. 8, No. 4, pp. 943–973, 1995.

25. Cohen, H., *A Course in Computational Algebraic Number Theory*, Vol. 138, Springer-Verlag, Berlin, 1993.

26. Lavallee, M. J., *Parametric Families of Polynomials: Construction and Applications*, Ph.D. Thesis, University of British Columbia, 2013.

27. Eloff, D., B. K. Spearman and K. S. Williams, "A_4-Sextic Fields with a Power Basis", *Missouri Journal of Mathematical Sciences*, Vol. 19, No. 3, pp. 188–194, 2007.

28. Nagel, T., "Zur Arithmetik der Polynome", *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg*, Vol. 1, No. 1, pp. 178–193, 1922.