Minimal Indices of Pure Cubic Fields

by

Jeewon Yoo

B.Sc., The University of British Columbia, 2014

A THESIS SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF

Master of Science

in

THE COLLEGE OF GRADUATE STUDIES
(Mathematics)

The University of British Columbia
(Okanagan)

May 2016

The undersigned certify that they have read, and recommend to the College of Graduate Studies for acceptance, a thesis entitled:

Minimal Indices of Pure Cubic Fields

submitted by Jeewon Yoo in partial fulfilment of the requirements of the

degree of Master of Science in Mathematics.

Blair Spearman, Faculty of Mathematics, UBC
Supervisor, Professor (please print name and faculty/school above the line)

Qiduan Yang, Faculty of Mathematics, UBC
Supervisory Committee Member, Professor (please print name and faculty/school in the line above)

Edward Butz, Faculty of Mathematics, UBC
Supervisory Committee Member, Professor (please print name and faculty/school in the line above)

Jim Robinson, Faculty of Philosophy, UBC
University Examiner, Professor (please print name and faculty/school in the line above)

Bernard Bauer, Faculty of Earth and Environmental Sciences, UBC
External Examiner, Professor (please print name and university in the line above)

May 26, 2016
(Date Submitted to Grad Studies)

Abstract

Determining whether a number field admits a power integral basis is a classical problem in algebraic number theory. It is well known that every quadratic number field is monogenic, that is they admit power bases. However, when we talk about cubic or higher degree number fields we may discover fields without power integral bases. In 1878, Dedekind gave the first example of a cubic field without a power integral basis. It is known that a number field is monogenic if and only if the minimal index is one. In 1937, Hall proved that the minimal index of pure cubic fields can be arbitrarily large. We extend this result by showing that the minimal index of a family of infinitely many pure cubic fields have an element of index n but no element of index less than n for a positive integer n.

Preface

The main result in this thesis is written in the paper [16] accepted on August 30, 2015. All authors of [16] contributed equally.

Contents

List of Tables

List of Figures

List of Symbols

$\mathbb{N}$	Set of natural numbers
$\mathbb{Z}$	Set of integers
$\mathbb{Q}$	Field of rational numbers
$\mathbb{R}$	Field of real numbers
$\mathbb{C}$	Field of complex numbers
$\phi(n)$	Euler ϕ function
S_n	Symmetric group of order n
$\mathbb{Z}+\mathbb{Z}i$	Set of Gaussian integers
$\mathbb{Z}[x]$	Set of polynomials with integer coefficients
$\mathbb{Q}[x]$	Set of polynomials with rational coefficients
$\langle f(x)\rangle$	Ideal generated by the polynomial $f(x)$
$[K:\mathbb{Q}]$	Degree of K over $\mathbb{Q}$
$\mathrm{disc}(f(x))$	Discriminant of the polynomial $f(x)$
$D(\alpha)$	Discriminant of the element α in an algebraic number field
$d(K)$	Field discriminant
$N(\alpha)$	Norm of the element α in an algebraic number field K
$\mathrm{Tr}(\alpha)$	Trace of the element α in an algebraic number field K
$\mathrm{ind}\,\alpha$	The index of an element α
$i(K)$	Index of an algebraic number field K
$m(K)$	Minimal index of an algebraic number field K
$\mathrm{Gal}(K:\mathbb{Q})$	Galois group of K over $\mathbb{Q}$
$\mathrm{Gal}(f(x))$	Galois group of the polynomial $f(x)$

Acknowledgments

I am a blessed one to meet my supervisor Dr. Blair Spearman. Without his support, I would not be able to accomplish this work and complete my graduate studies as a Master's student. Thanks for replying to my email and arranged a meeting with me four years ago when I was afraid of taking first step towards a mathematics student. My life changed gradually since our very first meeting.

Thanks to Dr. Qiduan Yang for teaching me the core courses that are indispensable to this achievement. I really appreciate your valuable comments and advices throughout my studies.

Thanks to my colleagues Chad Davies, Lindsey Reinholz, and Paul Lee for helping me throughout my undergraduate and graduate life. Your advices and experiences became a valuable model to follow.

Thanks to Cindy Bourne, the manger in the Math and Science Centre, for giving me opportunities to work as a tutor and as a SL leader. I learned the responsibility as a member of an organization and as a leader of students. Thanks for proofreading this paper.

Also, I would like to thank Mr. and Mrs. Mitsouras for treating me as your real grandchild although I am from totally different nation. Your life experiences and advices helped me a lot when I was left all alone in Canada since when I was a young kid.

Lastly, I would like to give a special thanks to my parents and my sister for the endless support and love.

Chapter 1

Introduction and Historical Remarks

Three positive integers a, b, and c do not satisfy the equation $a^n + b^n = c^n$ for any integer value of n greater than two.
— Pierre de Fermat (1637)

Algebraic number theory has been widely studied since 500 BC when the Pythagorean theorem was first introduced. It was developed in two different ways. One for the Fermat equations, and the other for class field theory. In either way, we have the same purpose: solving Diophantine equations. A Diophantine equation (named after Diophantus of Alexandria) is a polynomial equation in two or more unknowns, such that only the integer solutions are studied. One of the easiest Diophantine equations we have is

$$X^2 + Y^2 = Z^2$$

which is related to the Pythagorean theorem. Infinitely many integral solutions have been found for this equation such as

$$(3,4,5), (5,12,13), (8,15,17), ...$$

which we call them Pythagorean triples. One of the most famous and interesting

Diophantine equations in the history of mathematics is

$$x^n + y^n = z^n$$

where n is a positive integer. Pierre de Fermat claimed that there are no integral solutions to the Diophantine equation above when $n \geq 3$. This is called the "Fermat's Last Theorem." This theorem was first conjectured in 1637. Fermat claimed that he had a proof, but he did not show it to the public. This problem was left unsolved for more than 350 years until the first successful proof was released in 1994 by Andrew Wiles. Hence Fermat's Last Theorem shows that solving a Diophantine equation can be extremely difficult. The best possible situation for solving Diophantine equations is when we work over a unique factorization domain. The complexity of calculation is simpler than the equations without unique factorization domains. However, this only means that the calculation is simpler than the other; it still can be extremely difficult.

We say an algebraic number field is a monogenic field if it posesses a power integral basis, denoted by $\{1, \theta, \theta^2, ..., \theta^{n-1}\}$, where θ is a root of a minimal polynomial of degree n. It is well known that every number field has an integral basis. The next question then might be "how can we decide whether a field is monogenic?" It is known that a field is monogenic if and only if the absolute value of the index $|I| = 1$ is solvable, where I denotes the index form of the field. Using this, one can get a measure of how far away from being monogenic the number field is. Also, it is proven that the values of $|I|$ can be arbitrarily large. In [1], Hall proved that the minimal index of pure cubic fields can be arbitrarily large. The main aim of this thesis is to develop Hall's result so that we may construct an infinite family of pure cubic fields with an element of index equal to a particular positive integer n and we show the impossibility of the index being equal to any positive integers less than n.

Chapter 2

Number Theory Preliminaries

In this chapter, we review some of the basic definitions and theorems in elementary number theory and abstract algebra courses. In particular, we focus on primes, congruences, and cubic residues that are building blocks to the main result in chapter 5.

2.1 Elementary Number Theory

Definition 2.1.1. *If a and b are integers with $a \neq 0$, we say that a divides b if there is an integer c such that $b = ac$, and we write $a \mid b$. If a does not divide b, we write $a \nmid b$.*

Definition 2.1.2. *(Greatest Common Divisor) The greatest common divisor of two integers a and b, which are not both 0, is the largest positive integer that divides both a and b. It is written as $\gcd(a,b)$.*

Definition 2.1.3. *(Relatively Prime) The integers a and b, with $a,b \neq 0$, are relatively prime if $\gcd(a,b) = 1$.*

Theorem 2.1.1. *(Euclid) There are infinitely many primes.*

Theorem 2.1.2. *(Dirichlet's Theorem on Primes in Arithmetic Progressions) Suppose that a and b are relatively prime positive integers. Then the arithmetic progression $an+b$, $n = 1,2,3.....$, contains infinitely many positive primes.*

Definition 2.1.4. *Let m be a positive integer. If a and b are integers, we say that a is congruent to b modulo m, denoted $a \equiv b \pmod{m}$ if $m \mid (a-b)$.*

Example 2.1.1. *We have $5 \equiv 2 \pmod{3}$, since $3 \mid (5-2)$. However, $8 \not\equiv 2 \pmod{5}$ since $5 \nmid (8-2)$.*

Theorem 2.1.3. *If $a, b, c,$ and m are integers, with $m > 0$, such that $a \equiv b \pmod{m}$, then*

(i) $a+c \equiv b+c \pmod{m}$,

(ii) $a-c \equiv b-c \pmod{m}$,

(iii) $ac \equiv bc \pmod{m}$.

Theorem 2.1.4. *If $a \equiv b \pmod{m_1}, a \equiv b \pmod{m_2}, ..., a \equiv b \pmod{m_k}$, where $a, b, m_1, m_2, ..., m_k$ are integers with $m_1, m_2, ..., m_k$ positive, then*

$$a \equiv b \pmod{[m_1, m_2, ..., m_k]},$$

where $[m_1, m_2, ...m_k]$ denotes the least common multiple of $m_1, m_2, ..., m_k$.

Theorem 2.1.5. *(The Chinese Remainder Theorem) Let $m_1, m_2, ..., m_r$ be pairwise relative prime positive integers. Then the system of congruences*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_r \pmod{m_r} \end{aligned}$$

has a unique solution modulo $M = m_1 m_2 \cdots m_r$.

Example 2.1.2. *We solve the following system of congruences.*

$$\begin{aligned} x &\equiv 1 \pmod{3} \\ x &\equiv 2 \pmod{5} \\ x &\equiv 3 \pmod{7} \end{aligned}$$

Let $M = 3\cdot 5\cdot 7 = 105$, *and* $M_1 = M/3 = 35, M_2 = M/5 = 21$, *and* $M_3 = M/7 = 15$. *Now, we find* y_1, y_2, *and* y_3 *such that*

$$x \equiv y_1M_1 + 2y_2M_2 + 3y_3M_3 \pmod{3\cdot 5\cdot 7}.$$

To do this, we set up a congruence like following. $M_1y_1 = 35y_1 \equiv 1 \pmod 3$. *Then we get* $2y_1 \equiv 1 \pmod 3$ *by the replacement principle. Then, it is easy to see that* $y_1 \equiv 2 \pmod 3$. *Similarly,* $y_2 \equiv 1 \pmod 5$, *and* $y_3 \equiv 1 \pmod 7$. *Hence,*

$$x \equiv 1\cdot 35\cdot 2 + 2\cdot 21\cdot 1 + 3\cdot 15\cdot 1 \equiv 157 \equiv 52 \pmod{3\cdot 5\cdot 7}.$$

Lastly, we check if 52 *satisfies the desired congruences. Indeed,* $52 \equiv 1 \pmod 3, 52 \equiv 2 \pmod 5$, *and* $52 \equiv 3 \pmod 7$. *Therefore, we found the desired solution to the system of congruences above.*

Definition 2.1.5. *(Euler* ϕ *function) Let* n *be a positive integer. The Euler phi-function* $\phi(n)$ *is defined to be the number of positive integers not exceeding* n *that are relatively prime to* n.

Example 2.1.3. *Consider* $\phi(n)$ *for* $1 \le n \le 12$.

Table 2.1: The values of $\phi(n)$ for $1 \le n \le 12$

n	1	2	3	4	5	6	7	8	9	10	11	12
$\phi(n)$	1	1	2	2	4	2	6	4	6	4	10	4

Theorem 2.1.6. *(Euler's Theorem) If* m *is a positive integer and* a *is an integer with* $(a,m) = 1$, *then*

$$a^{\phi(m)} \equiv 1 \pmod m.$$

We proceed to the notion of cubic residues since this concept will be needed to prove Hall's results [1].

Definition 2.1.6. *Let* p *be a prime and let* q *be an integer not divisible by* p. *If there is an integer* x *such that* $x^3 \equiv q \pmod p$, *then* q *is said to be a cubic residue modulo* p. *If not,* q *is said to be a cubic non residue modulo* p.

Definition 2.1.7. *Two integers a, b are equivalent mod p if*

$$ax^3 \equiv b \pmod{p} \Longleftrightarrow y^3 \equiv a^2 b \pmod{p}$$

is solvable.

Theorem 2.1.7. *Let p be a prime with $p \equiv 2 \pmod 3$. Then every integer is a cube modulo p.*

Proof. Suppose $p \equiv 2 \pmod 3$. Set $p = 3e+2$ for some $e \in \mathbb{Z}$. Clearly, $p \equiv 0 \pmod p$. Consider the integers x, where $x \in \{1, ..., p-1\}$.
By Theorem 2.1.6,

$$x^{p-1} = x^{3e+1} \equiv 1 \pmod p.$$

Thus,

$$x = 1 \cdot x \equiv x^{3e+1} x^{3e+2} \equiv x^{6e+3} \equiv \left(x^{2e+1}\right)^3 \pmod p$$

This shows that every integer is a cube mod p. □

The following example illustrates Theorem 2.1.7.

Example 2.1.4. *Consider $p = 11 \equiv 2 \pmod 3$.*

Table 2.2: The cubic residues mod 11

x	1	2	3	4	5	6	7	8	9	10
$x^3 \pmod{11}$	1	8	5	9	4	7	2	6	3	10

But, choosing $p \equiv 1 \pmod 3$ gives totally different result.

Example 2.1.5. *Consider $p = 13 \equiv 1 \pmod 3$.*

Table 2.3: The cubic residues mod 13

x	1	2	3	4	5	6	7	8	9	10	11	12
$x^3 \pmod{13}$	1	8	1	12	8	8	5	5	1	12	5	12

We only obtained four integers mod 13 that are cubes mod 13. Let C_1 be the set of integers mod 13 that are cubes mod 13. In this case,

$$C_1 = \{1,5,8,12\}$$

Define the set of integers cubic non residues mod 13 by

$$CNR = \{2,3,4,6,7,8,10,11\}.$$

CNR can be further divided into two sets C_2 and C_3. To do this, pick any element in *CNR*, say 2. Then, calculate $2x^3 \pmod{13}$.

Table 2.4: C_2 : a set of cubic non-residues mod 13

x	1	2	3	4	5	6	7	8	9	10	11	12
$2x^3 \pmod{13}$	2	3	2	11	3	3	10	10	2	11	10	11

Then set

$$C_2 = \{2,3,10,11\}$$

We define C_3, pick any element in *CNR* excluding C_1 and C_2, say 4. Then, calculate $4x^3 \pmod{13}$.

Table 2.5: C_3 : a set of cubic non-residues mod 13

x	1	2	3	4	5	6	7	8	9	10	11	12
$4x^3 \pmod{13}$	4	6	4	9	6	6	7	7	4	9	7	9

By Table 2.5, we find that

$$C_3 = \{4,6,7,9\}$$

Observe that $C_1 \cup C_2 \cup C_3$ gives every integer mod 13. By Definition 2.1.7, if we

pick elements a, b where $a \in C_i$ and $b \in C_j$ where $i \neq j$, then the modular equation

$$ax^3 \equiv b \pmod{p}$$

is insolvable. Hall uses this argument in his main result, which will be discussed in Chapter 6.

2.2 Abstract Algebra

In this section, we introduce basic definitions and theorems from abstract algebra.

2.2.1 Group Theory

Definition 2.2.1. *(Group) A group $\langle G, * \rangle$ is a set G, closed under a binary operation $*$, such that the following axioms are satisfied:*
For all $a, b, c \in G$, we have

1. $(a * b) * c = a * (b * c)$ — ***associativity of*** $*$
2. *there exists* $e \in G$, *such that for all* $x \in G$, $e * x = x * e = x$ — ***identity element*** e
3. *For each* $a \in G$, *there exists* $a' \in G$ *such that* $a * a' = a' * a = e$ — ***inverse*** a'

Example 2.2.1. *The integers modulo 3, denoted $\mathbb{Z}_3$ form a group under addition, which is readily verified. We can describe all the elements in this group via a group table as follows. Later, we see that more complicated groups admit more complicated group tables.*

Table 2.6: Group table for $\mathbb{Z}_3$ under addition

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Definition 2.2.2. *(Subgroup) A subset H of a group G, (denote $H \leq G$) is a subgroup of G if and only if*

1. *H is closed under the binary operation of G,*

2. *the identity element e of G is in H.*

3. *for all $a \in H$ it is true that $a^{-1} \in H$ also.*

Definition 2.2.3. *A group $(G,*)$ is called **abelian** (or commutative) if $a*b = b*a$ for all $a,b \in G$.*

Definition 2.2.4. *Let G be a group. The order of G is its cardinality. That is, the number of elements in G. The order of an element $a \in G$, is the smallest positive integer m such that $a^m = e$, where e denotes the identity element in G. If no such m exists, then a is said to have infinite order.*

Definition 2.2.5. *A permutation of a set X is a function $\phi : X \to X$ that is both one to one and onto.*

Definition 2.2.6. *Let X be a set. $S_X := \{f : X \mapsto X \mid f \text{ is a bijection}\}$. Multiplication is composition*

$$\begin{array}{rcl} S_X \times S_X & \mapsto & S_X \\ (f,g) & \mapsto & g \circ f. \end{array}$$

*In case $X = \{1,2,...,n\}$ for some $n \in \mathbb{N}$, write S_n for S_X (called a **symmetric group**). If $G \leq S_n$ for some $n \in \mathbb{N}$, G is a **permutation group** of degree n.*

Note that the order of S_n is $n! = n \cdot (n-1) \cdots 2 \cdot 1$.

Definition 2.2.7. *A given binary relation $\sim$ on a set X is said to be an equivalence relation if and only if it is reflexive, symmetric and transitive. That is, for all a,b and c in X,*

- *$a \sim b \Rightarrow b \sim a$. (Reflexivity)*
- *$a \sim b$. (Symmetry)*
- *If $a \sim b$ and $b \sim c$ then $a \sim c$. (Transitivity)*

Lemma 2.2.1. *Let σ be a permutation of a set A. For $a,b \in A$, we have $a \sim b$ if and only if $b = \sigma^n(a)$ for some integer n. Here, $\sim$ denotes an equivalence relation.*

Definition 2.2.8. *Let σ be a permutation of a set A. The equivalence classes in A determined by the equivalence relation in Definition 2.2.7 are the orbits of σ.*

Definition 2.2.9. *A permutation $\sigma \in S_n$ is a cycle if it has at most one orbit containing more than one element. The length of a cycle is the number of elements in its largest orbit.*

Theorem 2.2.2. *Every permutation σ of a finite set is a product of disjoing cycles.*

Definition 2.2.10. *A cycle of length 2 is a transposition.*

Example 2.2.2. *Consider the following permutation in S_8.*

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 8 & 6 & 7 & 4 & 1 & 5 & 2 \end{pmatrix}$$

First, we find the orbit containing 1. Applying σ repeatedly, we see that

$$1 \to 3 \to 6 \to 1 \to 3 \to 6 \to 1 \to \cdots.$$

This shows the orbit containing 1 is $\{1,3,6\}$. We now choose an integer from 1 to 8 not in the set $\{1,3,6\}$, say 2, and similarly find that the orbit containing 2 is $\{2,8\}$. Finally, we find that the orbit containing 4 is $\{4,7,5\}$. Since these three orbits include all integers from 1 to 8, we see that the complete list of orbits of σ is

$$\{1,3,6\}, \quad \{2,8\}, \quad \{4,5,7\}.$$

Notice that the permutations corresponding to these three sets are cycles since they contain more than one element and we write these cycles as $(1\ 3\ 6), (2\ 8)$ and $(4\ 5\ 7)$ respectively. Since σ is a permutation in the finite set S_8, Theorem 2.2.1 shows that it can be written as a product of disjoint cycles:

$$\sigma = (1\ 3\ 6)(2\ 8)(4\ 7\ 5).$$

Clearly, $\{1,3,6\} \cap \{2,8\} \cap \{4,7,5\} = \emptyset$. Moreover, $(2\ 8)$ is a transposition by Definition 2.2.10.

Note that the sign of a permutation σ can be defined its decomposition into the product of transpositions as

$$\operatorname{sgn}(\sigma) = (-1)^m,$$

where m is the number of transpositions in the decomposition. If $\text{sgn}(\sigma) = +1$, then σ is even. If $\text{sgn}(\sigma) = -1$, then σ is odd.

Example 2.2.3. *Consider the symmetric group on* 3 *letters,* S_3. *Note that* S_n *has* $n!$ *elements. That means* $S_3 = 3! = 6$ *elements. Table 2.7 shows all the elements in* S_3. *Note that the abbreviation "CCW" stands for counterclockwise.*

Table 2.7: Elements of S_3

Elements	Standard Notation	Mapping
ρ_0	$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$	Identity
ρ_1	$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$	Rotation by 120° CCW
ρ_2	$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$	Rotation by 240° CCW
μ_1	$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$	Reflection by fixing 1
μ_2	$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$	Reflection by fixing 2
μ_3	$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$	Reflection by fixing 3

Now, we calculate a few compositions of permutations in S_3.

$$\begin{aligned} \mu_1 \circ \rho_1 &= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \mu_2 \\ \rho_1 \circ \mu_1 &= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \mu_3 \end{aligned}$$

This reveals that S_3 *is not abelian. In other words, the elements in* S_3 *do not commute except for one special case, which will be discussed later. Continuing with the similar calculations for all other compositions in the group, we obtain the group table for* S_3 *given below.*

Table 2.8: Group table for S_3

$\circ$	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_0	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	ρ_0	μ_3	μ_1	μ_2
ρ_2	ρ_2	ρ_0	ρ_1	μ_2	μ_3	μ_1
μ_1	μ_1	μ_2	μ_3	ρ_0	ρ_1	ρ_2
μ_2	μ_2	μ_3	μ_1	ρ_2	ρ_0	ρ_1
μ_3	μ_3	μ_1	μ_2	ρ_1	ρ_2	ρ_0

Theorem 2.2.3. *If $n \geq 2$, then the collection of all even permutations of $\{1,2,3,...,n\}$ forms a subgroup of order $n!/2$ of the symmetric group S_n.*

Definition 2.2.11. *The subgroup of S_n consisting of the even permutations of n letters is the alternating group A_n on n letters.*

By Theorem 2.2.3, the order of A_n is $n!/2$, and we say A_n has index 2 in S_n because intuitively "half" of the elements of S_n lie in A_n.

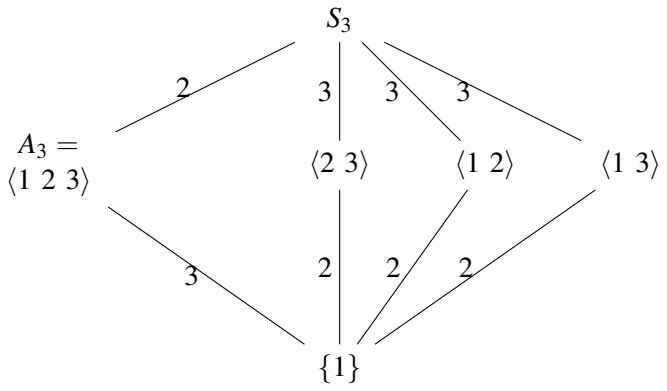
Example 2.2.4. *Going back to Table 2.7,*

$$\begin{aligned}
\rho_0 &= (1)(2)(3), \quad Even \\
\rho_1 &= (1\ 2\ 3), \quad Even \\
\rho_2 &= (1\ 3\ 2), \quad Even \\
\mu_1 &= (1)(2\ 3), \quad Odd \\
\mu_2 &= (1\ 3)(2), \quad Odd \\
\mu_3 &= (1\ 2)(3), \quad Odd
\end{aligned}$$

By Example 2.2.3, we showed that S_3 is not abelian except in one special case. That is, the elements ρ_0, ρ_1, ρ_2 are commutative and these elements have an even number of transpositions. Thus, by Definition 2.2.11, $A_3 = \{\rho_0, \rho_1, \rho_2\}$. The subgroup diagram for S_3 is constructed below in Figure 2.1. The number representing each lines joining each subgroups is the order of the corresponding subgroups. For example, the order of $(1\ 2\ 3)$ is 3, where as the index of A_3 in S_3 is 2.

.

Figure 2.1: The lattice of subgroups diagram of S_3



Definition 2.2.12. *In a group G, two elements g and h are called **conjugate** if*

$$h = xgx^{-1}$$

for some $x \in G$.

Definition 2.2.13. *For an element g of a group G, its **conjugacy class** is the set of elements*

$$C_g = \{xgx^{-1} \mid x \in G\}.$$

We know that

$$S_3 = \{(1), (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$$

Example 2.2.5. *It is easy to see that $g = (1)$ results in its own conjugacy class. Thus, we set the first trivial conjugacy class as*

$$C_1 = \{1\}.$$

σ	σ*(1 2)*σ^{-1}	*Cycle length*
(1)	(1 2)	*2*
(1 2)	(1 2)	*2*
(1 3)	(2 3)	*2*
(2 3)	(1 3)	*2*
(1 2 3)	(2 3)	*2*
(1 3 2)	(1 3)	*2*

Thus, the conjugates of $(1\ 2)$ *are* $(1\ 2), (1\ 3)$, *and* $(2\ 3)$. *We define the second conjugacy class of* S_3 *as*

$$C_2 = \{(1\ 2), (1\ 3), (2\ 3)\}.$$

Similarly,

σ	σ*(1 2 3)*σ^{-1}	*Cycle length*
(1)	(1 2 3)	*3*
(1 2)	(1 3 2)	*3*
(1 3)	(1 3 2)	*3*
(2 3)	(1 3 2)	*3*
(1 2 3)	(1 2 3)	*3*
(1 3 2)	(1 2 3)	*3*

and we define the final conjugacy class of C_3 *as*

$$C_3 = \{(1\ 2\ 3), (1\ 3\ 2)\}.$$

Definition 2.2.14. *(Cosets) Let* H *be a subgroup of a group* G *written multiplicatively. The subset* $aH = \{ah \mid h \in H\}$ *of* G *is the left coset of* H *containing* a, *while the subset* $Ha = \{ha \mid h \in H\}$ *is the right coset of* H *containing* a.

Theorem 2.2.4. *(Theorem of Lagrange) Let* H *be a subgroup of a finite group* G. *Then the order of* H *is a divisior of the order of* G.

Definition 2.2.15. *(Homomorphism) A map* $\phi : G \to G'$, *where* $(G, *)$ *and* $(G', *')$ *are groups is called a group homomorphism if*

$$\phi(a * b) = \phi(a) *' \phi(b)$$

for all $a, b \in G$.

Definition 2.2.16. *(Normal Subgroup) A subgroup H of a group G is normal if $gH = Hg$ for all $g \in G$.*

Theorem 2.2.5. *(Factor Group) Let $\phi : G \to G'$ be a group homomorphism with kernel H. Then the cosets of H form a group called the factor group and denoted G/H, where the group operation $*$ is given by $(aH) * (bH) = (ab)H$.*

2.2.2 Ring Theory and Fields

Definition 2.2.17. *(Rings) A ring $\langle R, +, \cdot \rangle$ is a set R together with two binary operations $+$ and $\cdot$, which we call addition and multiplication, defined on R such that the following axioms are satisfied:*

1. *$\langle R, + \rangle$ is an abelian group. That is, $a + b = b + a$ for all $a, b \in R$.*
2. *For all $a, b, c \in R$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.*
3. *For all $a, b, c \in R$, $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ and $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$ hold.*

If $a \cdot b = b \cdot a$ for all $a, b \in R$, we say R is commutative.

From here, we consider commutative rings with unity. That is, we only look at commutative rings with multiplicative identity, 1_R.

Example 2.2.6. *$\mathbb{Z}, n\mathbb{Z}, \mathbb{Z}_n, \mathbb{Z} + \mathbb{Z}\sqrt{d}$, where d is squarefree integer, and $\mathbb{Z} + \mathbb{Z}i$ are examples of rings.*

Definition 2.2.18. *(Zero Divisors and Units) Let R be a ring.*

1. *A element $a \neq 0$ in R is called a zero divisor in R, if there exists $b \neq 0$ in R, such that $ab = 0$.*
2. *Let R be a ring with the multiplicative identity 1. An element $u \in R$ is called a unit in R, if there exists $v \in R$ such that $uv = 1 = vu$.*

Definition 2.2.19. *(Integral Domain) An integral domain is a commutative ring that has a multiplicative identity 1, and has no divisors of zero.*

Example 2.2.7. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{Z}+\mathbb{Z}i, \mathbb{Z}+\mathbb{Z}\omega$, *where* $\omega = \frac{-1+\sqrt{-3}}{2}$, *and* $\mathbb{Z}+\mathbb{Z}\sqrt{m}$, *where m is a square free integer are examples of integral domain.*

Definition 2.2.20. *(Irreducible) A nonzero, nonunit element a of an integral domain D is called an irreducible, or said to be irreducible, if* $a = bc$, *where* $b, c \in D$, *implies that either b or c is a unit.*

Definition 2.2.21. *(Prime) A nonzero, nonunit element p of an integral domain D is called a prime if* $p \mid ab$, *where* $a, b \in D$, *implies that* $p \mid a$ *or* $p \mid b$.

Definition 2.2.22. *(Fields) Let R be a ring with unity* $1 \neq 0$. *If every nonzero element of R is a unit, then R is a division ring. A field is a commutative division ring.*

Example 2.2.8. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ *and* $\mathbb{Z}_p$, *p is a prime are examples of fields.*

Example 2.2.9. *The ring* $\mathbb{Z}_n$ *is of characteristic n, while* $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$, *and* $\mathbb{C}$ *all have characteristic 0.*

Definition 2.2.23. *(Unique Factorization Domain) Let D be a factorization domain. Suppose that every nonzero, nonunit element a of D has a unique factorization as a product of irreducible elements of D. Then D is called a unique factorization domain.*

Chapter 3

Algebraic Number Theory

In this chapter, we start by introducing algebraic elements and algebraic integers. Then we define the ring of algebraic integers in an algebraic number field. In Section 3.2 and 3.4, we study integral bases of cubic fields. Further, we find expressions for the index forms of cubic fields in Section 3.5. Using the index form of a number field, we are able to determine whether the field is monogenic or not.

3.1 Algebraic Number Fields

Definition 3.1.1. *(Algebraic Numbers) An element $\alpha \in \mathbb{C}$ is an algebraic number if $f(\alpha) = 0$ for some polynomial $f(x)$ with rational coefficients.*

Definition 3.1.2. *(Algebraic Integers) An element $\alpha \in \mathbb{C}$ is an algebraic integer if $f(\alpha) = 0$ for some monic polynomial $f(x)$ with integer coefficients. A monic polynomial is a polynomial in which the leading coefficient (the nonzero coefficient of highest degree) is equal to 1.*

Consider the following example.

Example 3.1.1. *$\alpha = \sqrt{3-\sqrt{5}}$ is an algebraic number as α is a root of the polynomial $f(x) = x^4 - 6x^2 + 4 \in \mathbb{Q}[x]$. Moreover, α is also an algebraic integer since $f(x) \in \mathbb{Z}[x]$ is a monic polynomial.*

Example 3.1.2. *Let $f(x) = x^3 - p^2x - 2p^2$, where p is an odd prime. We show that*

if θ is a root of $f(x)$, $\frac{\theta^2}{p}$ is an algebraic integer. Since θ is a root of $f(x)$,

$$f(\theta) = \theta^3 - p^2\theta - 2p^2 = 0,$$

$$\theta^3 = p^2\theta + 2p^2. \tag{3.1}$$

Let $\alpha = \frac{\theta^2}{p}$. We show that

$$\alpha^3 + A\alpha^2 + B\alpha + C = 0,$$

where $A, B, C \in \mathbb{Z}$. By (3.1), we can simplify the following expressions for α^3, α^2.

$$\alpha^3 = \left(\frac{\theta^2}{p}\right)^3 = \frac{\theta^6}{p^3} = \frac{\theta^3\theta^3}{p^3} = \frac{(p^2\theta + 2p^2)(p^2\theta + 2p^2)}{p^3} = p(\theta^2 + 4\theta + 4),$$

and

$$\alpha^2 = \left(\frac{\theta^2}{p}\right)^2 = \frac{\theta^3}{p^2} = \frac{\theta\theta^3}{p^2} = \frac{\theta(p^2\theta + 2p^2)}{p^2} = \frac{p^2(\theta^2 + 2\theta)}{p^2} = \theta^2 + 2\theta.$$

Thus,

$$\alpha^3 + A\alpha^2 + B\alpha + C = 0$$

is equivalent to

$$p(\theta^2 + 4\theta + 4) + A(\theta^2 + 2\theta) + B\left(\frac{\theta^2}{p}\right) + C = 0.$$

Rearranging terms,

$$\left(A + \frac{B}{p} + p\right)\theta^2 + (2A + 4p)\theta + (4p + C) = 0.$$

Since $\{1, \theta, \theta^2\}$ is linearly independent over $\mathbb{Q}$, each coefficient must vanish. Thus

$$\begin{aligned} A + \tfrac{B}{p} + p &= 0 \\ 2A + 4p &= 0 \\ 4p + C &= 0 \end{aligned}$$

Three equations give $C = -4p \in \mathbb{Z}, A = -2p \in \mathbb{Z}, B = p^2 \in \mathbb{Z}$. Thus, we have a polynomial $g(x) = x^3 - 2px^2 + p^2x - 4p$ such that $g(\alpha) = 0$. Since $g(x)$ is a monic polynomial with integer coefficients, Definition 3.1.2 tells us that α is an algebraic integer.

We claim that $\mathbb{C}$ is a field. It is enough to say that for all $z \in \mathbb{C}$, there exists $z^{-1} = \bar{z}/|z|^2 \in \mathbb{C}$ such that $zz^{-1} = 1 = z^{-1}z \in \mathbb{C}$. We now define field extensions and algebraic number fields that are stated on pages 98 and 109, [2].

Definition 3.1.3. *(Field Extension) Let K be a subfield of $\mathbb{C}$ and let $\alpha \in \mathbb{C}$. Let*

$$K(\alpha) = \bigcap_{\substack{F \\ \alpha \in F \\ K \subseteq F \subseteq \mathbb{C}}} F,$$

where the intersection is taken over all subfields F of $\mathbb{C}$, which contain both K and α. The intersection is nonempty as $\mathbb{C}$ is such a field. Since the intersection of subfields of $\mathbb{C}$ is again a subfield of $\mathbb{C}$, $K(\alpha)$ is the smallest field containing both K and α. We say that $K(\alpha)$ is formed from K by adjoining a single element α. $K(\alpha)$ is called a simple extension of K. If $\alpha_1, ..., \alpha_k \in \mathbb{C}$ for $k \geq 2$, $K(\alpha_1, ..., \alpha_k)$ is the smallest subfield of $\mathbb{C}$ that contains both K and $\alpha_1, ..., \alpha_k$, and is called a multiple extension of K.

Definition 3.1.4. *(Algebraic Number Field) An algebraic number field is a subfield of $\mathbb{C}$ of the form $\mathbb{Q}(\alpha_1, ..., \alpha_n)$, where $\alpha_1, ..., \alpha_n$ are algebraic numbers.*

Definition 3.1.5. *(Irreducible Polynomials) Let K be a subfield of $\mathbb{C}$. A nonconstant polynomial $f(x) \in K[x]$ is irreducible over K if it cannot be factored into the product of two nonconstant polynomials $g(x) \in K[x]$ and $h(x) \in K[x]$, where $deg(g(x)), deg(h(x)) < deg(f(x))$.*

Theorem 3.1.1. *(Eisenstein's Irreducibility Criterion) Let*

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x].$$

If there exists a prime number p such that

1. $p \mid a_i,\ i = 0, 1, ..., n-1$

2. $p \nmid a_n$,

3. $p^2 \nmid a_0$

then $f(x)$ is irreducible over the rational numbers.

Example 3.1.3. *Continue with Example 3.1.2. We show that the polynomial $f(x) = x^3 - p^2x - 2p^2$ is irreducible over $\mathbb{Q}$. We begin by finding the reverse polynomial $g(x)$ of $f(x)$. Consider*

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

Then, multiply both sides by x^3. We get

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

Then, the reverse polynomial of $f(x)$ is

$$g(x) = 1 - p^2x^2 - 2p^2x^3.$$

Now, set $y = xp$. Then,

$$\begin{aligned} g\left(\tfrac{y}{p}\right) &= -2p^2\left(\tfrac{y}{p}\right)^3 - p^2\left(\tfrac{y}{p}\right)^2 + 1 \\ &= \frac{-2y^3}{p} - y^2 + 1. \end{aligned}$$

Finally, multiplying both sides by p gives

$$h(y) = -2y^3 - py^2 + p.$$

Since p does not divide -2, and $p^2 \nmid p$ by Theorem 3.1.1, $h(y)$ is irreducible over $\mathbb{Q}$. Because $h(y)$ is related to $g(x)$ by a linear change of variables, $h(y)$ is irreducible over $\mathbb{Q}$ implies that $g(x)$ is also irreducible over $\mathbb{Q}$. Note that if $f(x)$ has a nonzero constant coefficient, then $f(x)$ is irreducible if and only if its reverse polynomial is irreducible. This statement shows that $f(x)$ is irreducible over $\mathbb{Q}$.

Theorem 3.1.2. *(Minimal polynomial of θ over K) Let θ be an algebraic integer. Then there exists a monic polynomial $f(x) \in \mathbb{Z}[x]$ of least degree such that $f(\theta) = 0$. $f(x)$ is called the minimal polynomial of θ with the following properties:*

1. *If $g(x) \in \mathbb{Q}[x]$, then $g(\theta) = 0$ if and only if $f(x)$ divides $g(x)$.*
2. *$f(x)$ is the unique monic irreducible polynomial such that $f(\theta) = 0$.*

Note that the degree of K is equal to the degree of $f(x)$, and denoted by

$$[K : \mathbb{Q}] = \deg(f(x)).$$

Definition 3.1.6. *(Conjugates of α over K) Let $\alpha \in \mathbb{C}$ be algebraic over a subfield K of $\mathbb{C}$. The conjugates of α over K are the roots in $\mathbb{C}$ of the minimal polynomial of α over K.*

3.2 The Set O_K

Definition 3.2.1. *(The set O_K) The set of all algebraic integers that lie in an algebraic number field K is denoted by O_K, that is,*

$$O_K = \Omega \cap K$$

where Ω is the set of all algebraic integers in $\mathbb{C}$. O_K is called the ring of integers of the algebraic number field K.

Theorem 3.2.1. *Let K be an algebraic number field. Then O_K is an integral domain.*

Theorem 3.2.2. *Let K be a quadratic field. Then there exists a unique squarefree integer m such that $K = \mathbb{Q}(\sqrt{m})$.*

Theorem 3.2.3. *Let K be a quadratic field. Let m be the unique squarefree integer such that $K = \mathbb{Q}(\sqrt{m})$. Then the set O_K of algebraic integers is given by*

$$O_K = \begin{cases} \mathbb{Z} + \mathbb{Z}\sqrt{m}, & \text{if } m \not\equiv 1 \pmod 4 \\ \mathbb{Z} + \mathbb{Z}\left(\dfrac{1+\sqrt{m}}{2}\right), & \text{if } m \equiv 1 \pmod 4. \end{cases}$$

Example 3.2.1. *Consider $\alpha = \sqrt[3]{5} \in \mathbb{C}$. Let $K = \mathbb{Q}(\sqrt[3]{5})$. Then K is an algebraic number field. Note that α is a root of the irreducible polynomial $x^3 - 5$, hence, it is an algebraic integer. The set O_K for K contains elements of the form:*

$$a + b\alpha + c\alpha^2,$$

where $a, b, c \in \mathbb{Z}$. We will show this in Section 3.4.

3.3 Discriminants

From high school, we know that the discriminant of a quadratic equation $ax^2 + bx + c$ is $b^2 - 4ac$. The discriminant of a polynomial of degree n is defined in the following way.

Definition 3.3.1. *(Discriminant of a polynomial)*
Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{C}[x]$, where $n \in \mathbb{N}$ and $a_n \neq 0$. Let $\theta_1, ..., \theta_n \in \mathbb{C}$ be the roots of $f(x)$. The discriminant of $f(x)$ is the quantity

$$\operatorname{disc}(f(x)) = a_n^{2n-2} \prod_{1 \leq i < j \leq n} (\theta_i - \theta_j)^2.$$

Example 3.3.1. *Consider $f(x) = x^2 + bx + c$, where $b, c \in \mathbb{Z}$. Let $\theta_1, \theta_2 \in \mathbb{C}$ be the roots of $f(x)$. Then, $f(x) = (x - \theta_1)(x - \theta_2) = x^2 - (\theta_1 + \theta_2)x + \theta_1\theta_2$. Set $b = -(\theta_1 + \theta_2)$, and $c = \theta_1\theta_2$. By Definition 3.3.1, $(\theta_1 - \theta_2)^2 = \theta_1^2 - 2\theta_1\theta_2 + \theta_2^2 = \theta_1^2 + 2\theta_1\theta_2 + \theta_2^2 - 4\theta_1\theta_2 = (\theta_1 + \theta_2)^2 - 4\theta_1\theta_2 = b^2 - 4c$, which confirms the discriminant of a quadratic equation.*

Definition 3.3.2. *Let K be an algebraic number field of degree n. Let $\omega_1, ..., \omega_n$ be n elements of K. Let σ_k $(k = 1, 2, ..., n)$ denote the n distinct monomorphisms of K in $\mathbb{C}$. For $i = 1, ..., n$, let*

$$\omega_i^{(1)} = \sigma_1(\omega_i) = \omega_i, \omega_i^{(2)} = \sigma_2(\omega_i), \cdots, \omega_i^{(n)} = \sigma_n(\omega_i)$$

denote the conjugates of ω_i. Then the discriminant of $\{\omega_1,...,\omega_n\}$ is

$$D(\omega_1,...,\omega_n) = \begin{vmatrix} \omega_1^{(1)} & \omega_2^{(1)} & \cdots & \omega_n^{(1)} \\ \omega_1^{(2)} & \omega_2^{(2)} & \cdots & \omega_n^{(2)} \\ \vdots & \vdots & \cdots & \vdots \\ \omega_1^{(n)} & \omega_2^{(n)} & \cdots & \omega_n^{(n)} \end{vmatrix}^2.$$

It is known that if $\omega_1,...,\omega_n$ are all algebraic integers then $D(\omega_1,...,\omega_n)$ is a rational integer.

Definition 3.3.3. *(Discriminant of an element α) Let K be an algebraic number field of degree n. Let $\alpha \in K$. Then we define the discriminant $D(\alpha)$ of α by*

$$D(\alpha) = \prod_{1\le i<j\le n} (\alpha^{(i)} - \alpha^{(j)})^2,$$

where $\alpha^{(1)} = \alpha, \alpha^{(2)}, ..., \alpha^{(n)}$ are the conjugates of α. Note that if α is an algebraic integer in K, then the discriminant of α is the discriminant of the minimal polynomial of α over K.

Example 3.3.2. *Let $K = \mathbb{Q}(\sqrt{2})$. The minimal polynomial of $\sqrt{2}$ over $\mathbb{Q}$ is given by*

$$f(x) = x^2 - 2.$$

It is easy to check that the discriminant of $f(x)$ is 8. We may also confirm this using Definition 3.3.3. Since $\pm\sqrt{2}$ are the roots of $f(x)$,

$$\begin{aligned} D(\sqrt{2}) &= (\sqrt{2}+\sqrt{2})^2 \\ &= (2\sqrt{2})^2 \\ &= 8. \end{aligned}$$

3.4 Integral Basis

In section 3.2, we fully generalized the elements in the set O_K for quadratic fields. Recall Theorem 3.2.3, if K is a quadratic field, and m is a squarefree integer such that $K = \mathbb{Q}(\sqrt{m})$, then the set O_K is described by

$$O_K = \begin{cases} \mathbb{Z} + \mathbb{Z}\sqrt{m}, & \text{if } m \not\equiv 1 \pmod 4 \\ \mathbb{Z} + \mathbb{Z}\left(\dfrac{1+\sqrt{m}}{2}\right), & \text{if } m \equiv 1 \pmod 4. \end{cases}$$

That is, every element in O_K is an integer linear combination of the elements in the following two sets.

$$\begin{cases} \{1, \sqrt{m}\}, & \text{if } m \not\equiv 1 \pmod 4 \\ \left\{1, \left(\dfrac{1+\sqrt{m}}{2}\right)\right\}, & \text{if } m \equiv 1 \pmod 4. \end{cases}$$

For $K = \mathbb{Q}(\sqrt{2})$, since $2 \not\equiv 1 \pmod 4$, the above observation implies that O_K can be generated by integral linear combinations of $\{1, \sqrt{2}\}$. For $L = \mathbb{Q}(\sqrt[3]{5})$ in Example 3.2.1, we claimed that the elements in O_L can be expressed as integer linear combinations of $\{1, \sqrt[3]{5}, (\sqrt[3]{5})^2\}$. This phenomenon leads us to the notion of an integral basis.

Definition 3.4.1. *(Integral Basis) Let K be an algebraic number field of degree n with ring of integers O_K. An integral basis for O_K is a set of n elements $\{\eta_1, \eta_2, ..., \eta_n\}$ of O_K such that for any algebraic integer $\alpha \in O_K$,*

$$\alpha = C_1\eta_1 + C_2\eta_2 + \cdots + C_n\eta_n$$

where $C_1, C_2, ..., C_n \in \mathbb{Z}$.

Theorem 3.4.1. *Every number field K has an integral basis.*

Theorem 3.4.2. *Suppose $\{\alpha_1, \alpha_2, ..., \alpha_n\}$ is a $\mathbb{Q}-$basis for a number field K. If $D(\alpha_1, ..., \alpha_n)$ is squarefree, then $\{\alpha_1, ..., \alpha_n\}$ is an integral basis.*

Definition 3.4.2. *Let K be a number field, with degree n and the ring of integers O_K. If $O_K = \mathbb{Z}[\alpha]$ for some $\alpha \in O_K$, the set $\{1, \alpha, ..., \alpha^{n-1}\}$ is called a power basis.*

Theorem 3.4.2 provides a sufficient condition for a set to be an integral basis. But, the problem is this situation does not come up very often. It is also known that every integral basis has the same discriminant. Maple will calculate an integral

basis for a number field, but we will present an algorithm one can carry out by hand that will give an integral basis. First, we need to define the norm and trace of an element.

Definition 3.4.3. *Let K be a number field of degree n. The norm of an element $\alpha \in K$ is given by*

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

and the trace is given by

$$\mathrm{Tr}(\alpha) = \sum_{i=1}^{n} \alpha^{(i)},$$

where $\alpha = \alpha^{(1)}, \alpha^{(2)}, ..., \alpha^{(n)}$ are the conjugates of α. Note that $N(\alpha), \mathrm{Tr}(\alpha) \in \mathbb{Z}$ for any algebraic integer α.

Theorem 3.4.3. *Let K be an algebraic number field of degree n. Let $\alpha, \beta \in K$. Then*

$$\mathrm{Tr}(\alpha+\beta) = \mathrm{Tr}(\alpha) + \mathrm{Tr}(\beta) \text{ and } N(\alpha\beta) = N(\alpha)N(\beta).$$

Theorem 3.4.4. *Suppose that $\{\alpha_1, ..., \alpha_n\}$ is a $\mathbb{Q}-$basis for K consisting of algebraic integers, and let p be a prime such that p^2 divides $D(\alpha_1, ..., \alpha_n)$. Then there is an algebraic integer of the form*

$$\frac{1}{p}(\lambda_1\alpha_1 + \cdots + \lambda_n\alpha_n),$$

where $0 \leq \lambda_i \leq p-1,\ \lambda_i \in \mathbb{Z}$.

Now, we adapt the algorithm from Cook [18] to compute integral bases.
Let $K = \mathbb{Q}(\alpha)$ be an algebraic number field.

Table 3.1: Computing Integral Bases

Steps	Description	Mathematical Description
1	Set up a $\mathbb{Q}-$basis for K.	$\{\alpha_1, \alpha_2, ..., \alpha_n\}$.
2	Calculate the discriminant of the set in Step 1. If it is squarefree, then by Theorem 3.4.2, process complete.	$D(\alpha_1, \alpha_2, ..., \alpha_n)$.
3	Find all primes p such that p^2 divides the discriminant in Step 2.	$p^2 \mid D(\alpha_1, \alpha_2, ..., \alpha_n)$.
4	Select one of the primes found in Step 3. Define a new algebraic integer in the form described in Theorem 3.4.4. Then compute the trace of the element.	$\alpha^* = \frac{1}{p}(\lambda_1\alpha_1 + \cdots + \lambda_n\alpha_n)$, Find $\mathrm{Tr}(\alpha^*)$.
5	Find the norm of α^*.	$N(\alpha^*)$.
6	Using the fact that the norm of an algebraic integer is a rational integer, check all the cases of λ_i to see if α^* is the algebraic integer for the given prime.	See the examples below.
7	If all λ_is do not satisfy the conditions in Step 6, then α^* is not an algebraic integer. Return to Step 3 and repeat the same process by selecting the other primes. Otherwise, proceed to Step 8.	See the examples below.
8	At this stage, α^* is tested to be an algebraic integer in K. Adjoin the new algebraic integer to the basis in step 1.	$\{\alpha_1, \alpha_2, ..., \alpha_n, \alpha^*\} \to \{\beta_1, \beta_2, ..., \beta_n\}$.
9	Calculate the discriminant of the new basis in Step 8. If it is not squarefree, repeat the same process from Step 3 until no new algebraic integers are found.	$D(\beta_1, \beta_2, ..., \beta_n)$.

Example 3.4.1. *Let* $K = \mathbb{Q}(\sqrt[3]{5})$.

Step 1. A natural guess for a $\mathbb{Q}-$*basis for* K*. That is,* $\{1, \sqrt[3]{5}, (\sqrt[3]{5})^2\}$.

Step 2. Calculate the discriminant of the set in Step 1.

$$D(1, \sqrt[3]{5}, (\sqrt[3]{5})^2) = -3^3 5^2.$$

Step 3. Find all primes p *such that* p^2 *divides the discriminant in Step 2. Hence,* $p = 3, 5$.

Step 4. Select one of the primes found in Step 3. Define a new algebraic integer in the form described in Theorem 3.4.4. Then compute the trace of the element. As

$$\alpha^* = \frac{1}{5}(\lambda_1 + \lambda_2 \sqrt[3]{5} + \lambda_3 (\sqrt[3]{5})^2),$$

$$\mathrm{Tr}(\alpha^*) = \left(\frac{1}{5}\right) \sum_{i=1}^{3} \alpha^{(i)} = \frac{3\lambda_1}{5},$$

where $0 \leq \lambda_i \leq 4$, *and since* $\frac{3\lambda_1}{5} \in \mathbb{Z}$, *it follows that* $\lambda_1 = 0$.

Step 5. Find the norm of α^*.

$$N(\alpha^*) = \prod_{i=1}^{3} \alpha^{(i)} = \frac{\lambda_2^3 + 5\lambda_3^3}{25}.$$

Step 6. Using the fact that the norm of an algebraic integer is a rational integer, check all the cases of λ_i *to see if* α^* *is the algebraic integer for the given prime. See Table 3.2.*

Step 7. The algebraic integer α^* *in Step 6 is not in* O_K*. Return to Step 3.*

Step 8. Choose the other prime, which is $p = 3$*. Repeating Steps 4 - 6, there is no algebraic integers to be added in the basis described in Step 1. The integral basis is*

$$\{1, \sqrt[3]{5}, (\sqrt[3]{5})^2\}.$$

Table 3.2: Examining $\alpha^* \in O_K$

λ_2	λ_3	Divisible by 25?	YES/NO
0	1	5	NO
0	2	40	NO
0	3	135	NO
0	4	320	NO
1	0	1	NO
1	1	6	NO
1	2	41	NO
1	3	136	NO
1	4	321	NO
2	0	8	NO
2	1	13	NO
2	2	48	NO
2	3	143	NO
2	4	328	NO
3	0	27	NO
3	1	32	NO
3	2	67	NO
3	3	162	NO
3	4	347	NO
4	0	64	NO
4	1	69	NO
4	2	104	NO
4	3	199	NO
4	4	384	NO

Example 3.4.1 is one where our natural guess of the integral basis turns out to be the correct one. We now give an example due to Dedekind which is not as simple as the previous one.

Example 3.4.2. *Let $K = \mathbb{Q}(\theta)$ where θ is a root of the polynomial $f(x) = x^3 - x^2 - 2x - 8 \in \mathbb{Q}[x]$. We find the integral basis for K.*

Step 1. A natural guess for a $\mathbb{Q}-$basis for K. That is, $\{1, \theta, \theta^2\}$.

Step 2. Calculate the discriminant of the set in Step 1.

$$D(1, \theta, \theta^2) = -(2)^2(503).$$

Step 3. *Find all primes p such that p^2 divides the discriminant in Step 2. Hence, $p = 2$.*

Step 4. *Select one of the primes found in Step 3. Define a new algebraic integer in the form described in Theorem 3.4.4. Then compute the trace of the element. As*

$$\theta^* = \frac{1}{2}(\lambda_1 + \lambda_2\theta + \lambda_3\theta^2),$$

$$\mathrm{Tr}(\theta^*) = \left(\frac{1}{2}\right)\sum_{i=1}^{3}\alpha^{(i)} = \frac{3\lambda_1 + \lambda_2 + 5\lambda_3}{2},$$

where $0 \leq \lambda_i \leq 1$.

Table 3.3: Examining $\theta^* \in O_K$

λ_1	λ_2	λ_3	$3\lambda_1+\lambda_2+5\lambda_3$	Divisible by 2?
0	0	1	5	NO
0	1	0	1	NO
0	1	1	6	YES
1	0	0	3	NO
1	0	1	8	YES
1	1	0	4	YES
1	1	1	9	NO

The table above shows that we only need to test

$$(\lambda_1, \lambda_2, \lambda_3) = (0,1,1), (1,0,1) \text{ and } (1,1,0).$$

Step 5. *Find the norm of θ^**

$$\begin{aligned} N(\theta^*) &= \frac{1}{8}\prod_{i=1}^{3}\alpha^{(i)} \\ &= \frac{\lambda_1^3 + 8\lambda_2^3 + 64\lambda_3^3 - 2\lambda_1\lambda_2^2 - 12\lambda_1\lambda_3^2 - 16\lambda_2\lambda_3^2 + \lambda_1^2\lambda_2 + 5\lambda_1^2\lambda_3 + 8\lambda_2^2\lambda_3 - 26\lambda_1\lambda_2\lambda_3}{8}. \end{aligned}$$

Step 6. *Check all the cases of λ_i to see if θ^* is the algebraic integer for the given prime.*

Table 3.4: Examining $\theta^* \in O_K$

λ_1	λ_2	λ_3	$\lambda_1^3+8\lambda_2^3+64\lambda_3^3-2\lambda_1\lambda_2^2-12\lambda_1\lambda_3^2-16\lambda_2\lambda_3^2+\lambda_1^2\lambda_2+5\lambda_1^2\lambda_3+8\lambda_2^2\lambda_3-26\lambda_1\lambda_2\lambda_3$	Divisible by 8?
0	1	1	64	YES
1	0	1	58	NO
1	1	0	8	YES

Step 7. Two algebraic elements are survived.

$$\frac{1+\theta}{2}, \frac{\theta+\theta^2}{2}.$$

The minimal polynomial of each elements are $4x^3-8x^2+3x-4$ *and* $x^3-3x^2-10x-8$ *respectively. Since the first one is not a monic polynomial,* $(1+\theta)/2$ *is not an integer in* K.

Step 8. Adjoin any new algebraic integers to the original basis in Step 1.

$$\left\{1, \theta, \theta^2, \frac{\theta+\theta^2}{2}\right\}.$$

Observe that

$$\theta^2 = 2\left(\frac{\theta+\theta^2}{2}\right) - \theta,$$

hence the $\mathbb{Z}-$*linearly independent basis is*

$$\left\{1, \theta, \frac{\theta+\theta^2}{2}\right\}.$$

Step 9. Calculate the discriminant of the new basis.

$$D\left(1, \theta, \frac{\theta+\theta^2}{2}\right) = 503.$$

Since the discriminant $D\left(1, \theta, (\theta+\theta^2)/2\right)$ *is square free, we have found an integral basis for* K. *Therefore, we terminate this algorithm. The integral basis for* K *is*

$$\left\{1, \theta, \frac{\theta+\theta^2}{2}\right\}.$$

In Section 3.3, we discussed various kinds of discriminants. However, there was one type of discriminant we didn't mention, which we now define.

Definition 3.4.4. *(Field Discriminant) Let K be an algebraic number field of degree n. Let $\{\eta_1, ..., \eta_n\}$ be an integral basis for K. Then $D(\eta_1, ..., \eta_n)$ is called the discriminant of K and is denoted by $d(K)$.*

The field discriminant is used to derive index forms. To compute the field discriminant $d(K)$ for a number field K, we obtain a integral basis for K first. Then, use the determinant equation expressed in Definition 3.3.2.

The number field in Example 3.4.1 possesses a power basis, whereas the one in Example 3.4.2 does not. Determining whether a number field admits a power integral basis is a classical problem in algebraic number theory. Example 3.4.2 was the first example given of an algebraic number field without a power integral basis. If number fields admit power bases, we call them monogenic fields. Number theorists discovered a tool to measure how far a number field can be away from being monogenic. We use indices of number fields to determine whether they are monogenic or not. These will be discussed in the next section.

3.5 Index Forms and Minimal Indices

The minimal index of a number field measures how close it is to being monogenic. If the minimal index is 1, then the corresponding number field is monogenic. We will discuss how to find minimal indices in this section, but first we need a definition.

Definition 3.5.1. *(Index of α) Let K be an algebraic number field. Let $\alpha \in O_K$ be such that $K = \mathbb{Q}(\alpha)$. Then the index of α, written $\operatorname{ind}\alpha$, is the positive integer given by*

$$D(\alpha) = (\operatorname{ind}\alpha)^2 d(K),$$

where $D(\alpha)$ is the discriminant of α defined in Definition 3.3.3, and $d(K)$ is the field discriminant defined in Definition 3.4.4. Equivalently, we may use the following expression for the index of an element in K.

$$\operatorname{ind}\alpha = \sqrt{\frac{D(\alpha)}{d(K)}}.$$

Now we will calculate indices in some number fields, beginning with an arbitrary quadratic field. In Theorem 3.2.3, we stated that the general elements in the ring of integers of a quadratic field can be described by $\mathbb{Z}+\mathbb{Z}\sqrt{m}$ if $m \not\equiv 1 \pmod 4$, or $\mathbb{Z}+\mathbb{Z}(1+\sqrt{m})/2$ if $m \equiv 1 \pmod 4$. By Alaca [2], we state another important result about the field discriminant of a quadratic field.

Theorem 3.5.1. *Let K be a quadratic field. Let m be the unique squarefree integer such that $K = \mathbb{Q}(\sqrt{m})$. Then the field discriminant $d(K)$ of K is given by*

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

Using this result, we are ready to compute the index of $\alpha \in O_K$ for some quadratic field K.

Example 3.5.1. *Let K be a quadratic field. Then by Theorem 3.2.2, there exists a unique squarefree integer m such that $K = \mathbb{Q}(\sqrt{m})$. First, we assume that $m \equiv 1 \pmod 4$. Then, the corresponding integral basis is $\left\{1, \frac{1+\sqrt{m}}{2}\right\}$, with $d(K) = m$. Pick $\alpha \in O_K$. Then*

$$\alpha = a + b\left(\frac{1+\sqrt{m}}{2}\right),\ a,b \in \mathbb{Z}.$$

Now, by Definition 3.3.2, we get

$$D(\alpha) = \begin{vmatrix} 1 & a+b\left(\frac{1+\sqrt{m}}{2}\right) \\ 1 & a+b\left(\frac{1-\sqrt{m}}{2}\right) \end{vmatrix}^2 = (-b\sqrt{m})^2 = b^2 m.$$

Thus,

$$\operatorname{ind}\alpha = \sqrt{\frac{D(\alpha)}{d(K)}} = \sqrt{\frac{b^2 m}{m}} = |b|.$$

Now, if $m \not\equiv 1 \pmod 4$, then the integral basis is $\{1, \sqrt{m}\}$ and $d(K) = 4m$. Following a similar process as the first case, we pick $\alpha \in O_K$. Then $\alpha = a + b\sqrt{m}$,

where $a, b \in \mathbb{Z}$. Then,

$$D(\alpha) = \begin{vmatrix} 1 & a+b\sqrt{m} \\ 1 & a-b\sqrt{m} \end{vmatrix}^2 = (-2b\sqrt{m})^2 = 4b^2m.$$

Thus,

$$\operatorname{ind}\alpha = \sqrt{\frac{D(\alpha)}{d(K)}} = \sqrt{\frac{4b^2m}{4m}} = |b|.$$

Here, the equation $I(a,b) = \operatorname{ind}\alpha = |b|$ is called the index form of the quadratic field K in the previous example. This is the simplest index form we get for an algebraic number field. The results in Example 3.5.1 show that the index form of any quadratic field can be described by the positive integer $|b|$. Therefore, the minimum of $\operatorname{ind}(\alpha)$ is 1 for some $\alpha \in O_K$. Now, we consider finding the index form of a cubic polynomial.

Example 3.5.2. *Consider $K = \mathbb{Q}(\theta)$, where θ is a root of $f(x) = x^3 - 3x + 9$. We compute the index form, field index, and the minimal index of the field K.*
An integral basis for K is $\left\{1, \theta, \frac{\theta^2}{3}\right\}$. Then,

$$O_K = \left\{ a + b\theta + c\left(\frac{\theta^2}{3}\right) \mid a,b,c \in \mathbb{Z} \right\}.$$

Let $\alpha \in O_K$. Then $\alpha = a + b\theta + c\left(\frac{\theta^2}{3}\right)$, where $a,b,c \in \mathbb{Z}$. The conjugates of α over K are described below:

$$\alpha' = a + b\theta' + c\left(\frac{\theta'^2}{3}\right),$$

$$\alpha'' = a + b\theta'' + c\left(\frac{\theta''^2}{3}\right).$$

Obeserve that $f(x) = x^3 - 3x + 9 = (x-\theta)(x-\theta')(x-\theta'')$, where, θ' and θ'' are the other roots of $f(x)$. Expanding and simplifying gives $x^3 - (\theta+\theta'+\theta'')x^2 + (\theta\theta' + \theta\theta'' + \theta'\theta'')x - \theta\theta'\theta''$ Since the coefficient of x^2 is zero, we have $\theta + \theta' + \theta'' = 0$, and so we obtain $\alpha - \alpha'$, $\alpha - \alpha''$, and $\alpha' - \alpha''$ as follws:

$$\alpha - \alpha' = (\theta - \theta')\left(b + \frac{c}{3}(\theta + \theta')\right) = (\theta - \theta')\left(b - \frac{c}{3}\theta''\right),$$

$$\alpha-\alpha''=(\theta-\theta')\left(b+\frac{c}{3}(\theta+\theta'')\right)=(\theta-\theta'')\left(b-\frac{c}{3}\theta'\right),$$
$$\alpha'-\alpha''=(\theta'-\theta'')\left(b+\frac{c}{3}(\theta'+\theta'')\right)=(\theta'-\theta'')\left(b-\frac{c}{3}\theta\right).$$

Hence, by Definition 3.3.3,

$$\begin{aligned}
D(\alpha) &= (\alpha-\alpha')^2(\alpha-\alpha'')^2(\alpha'-\alpha'')^2 \\
&= (\theta-\theta')^2(\theta-\theta'')^2(\theta'-\theta'')^2\left(b-\tfrac{c}{3}\theta\right)^2\left(b-\tfrac{c}{3}\theta'\right)^2\left(b-\tfrac{c}{3}\theta''\right)^2 \\
&= D(\theta)\left\{\left(\frac{c}{3}\right)^3 f\left(\frac{3b}{c}\right)\right\}^2 \\
&= -3^3\cdot 7\cdot 11\left(b^3-\frac{bc^2}{3}+\frac{c^3}{3}\right)^2 \\
&= -3\cdot 7\cdot 11(3b^3-bc^2+c^3)^2.
\end{aligned}$$

Therefore, the index form of the field K is

$$\operatorname{ind}\alpha=\sqrt{\frac{D(\alpha)}{d(K)}}=\sqrt{\frac{-3\cdot 7\cdot 11(3b^3-bc^2+c^3)^2}{-3\cdot 7\cdot 11}}=|3b^3-bc^2+c^3|.$$

Now, we are ready to give two new definitions about the index forms.
Let K be an algebraic number field of degree n.

Definition 3.5.2. *(Index of a field) The index of the field K is*

$$i(K)=\gcd\{\operatorname{ind}\alpha \mid \alpha\in O_K\}.$$

Definition 3.5.3. *(Minimal index of a field) The minimal index of K is*

$$m(K)=\min\{\operatorname{ind}\alpha \mid \alpha\in O_K\}.$$

It is well known that the field index of a cubic field is either 1 or 2 (see [5]). Referring back to Example 3.5.2, the field index of K is 1 as we have $\operatorname{ind}\alpha = |3b^3-bc^2+c^3|=1$ if $(b,c)=(1,-1)$. Hence, $m(K)=1$. Similarly, we found that the index form of any quadratic field can be expressed by $|b|, b\in\mathbb{Z}\backslash\{0\}$. Thus, the field and minimal index of any quadratic field is equal to 1. There is a close relationship between the minimal index and the integral basis.

Theorem 3.5.2. *Let K be an algebraic number field, Then $m(K) = 1$ if and only if K possesses a power basis.*

Proof. ($\Rightarrow$) Suppose $m(K) = 1$. Then there exists a generator α of K such that ind $\alpha = 1$. Hence, $D(1, \alpha, ..., \alpha^{n-1}) = D(\alpha) = (\text{ind } \alpha)^2 d(K) = d(K)$ so that $\{1, \alpha, ..., \alpha^{n-1}\}$ is an integral basis for K. Hence, K possesses a power basis.
($\Leftarrow$) Conversely, suppose K possesses a power basis, say $\{1, \alpha, ..., \alpha^{n-1}\}$. Then $\{1, \alpha, ..., \alpha^{n-1}\}$ is an integral basis for K and so $D(1, \alpha, ..., \alpha^{n-1}) = d(K)$. But,

$$D(1, \alpha, ..., \alpha^{n-1}) = D(\alpha) = (\text{ind } \alpha)^2 d(K),$$

which forces ind $\alpha = 1$ and hence $m(K) = 1$. □

Chapter 4

Galois Groups and Chebotarev Density Theorem

For our discussion on Galois theory, we will restrict our attention to cubic polynomials.

4.1 Galois Groups of Cubics

In Theorem 3.1.1, we introduced Eisenstein's Irreducibility Criterion to test if a polynomial is irreducible. There are more techniques for testing irreducibility of polynomials. We begin this section by providing a few other techniques for irreducibility.

Theorem 4.1.1. *(Rational Root Theorem) Let*

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = 0 \in \mathbb{Z}[x],$$

where $a_n, a_0 \neq 0$. *Then, each rational solution* x, *when written as a fraction* $x = p/q$ *with* $\gcd(p,q) = 1$, *satisfies*

- p *is an integer factor of the constant term* a_0, *and*
- q *is an integer factor of the leading coefficient* a_n.

Theorem 4.1.2. *(Gauss) Let f be a polynomial over $\mathbb{Z}$ which is irreducible over $\mathbb{Z}$. Then f, considered as a polynomial over $\mathbb{Q}$, is also irreducible over $\mathbb{Q}$.*

We demonstrate Gauss's Lemma in the following example.

Example 4.1.1. *Consider*

$$f(x) = x^2 + x + 1 \in \mathbb{Z}[x].$$

Since $f(\pm 1) \neq 0$, $f(x)$ is irreducible by the Rational Root Theorem. Hence, by Theorem 4.1.2, $f(x)$ is irreducible over $\mathbb{Q}$.

Another type of irreducibility test is called the **modulo p test**. Let p be a prime and suppose that $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ with the degree of $f(x)$, $n \geq 1$, and $p \nmid a_n$. Let $\overline{f}(x)$ be the polynomial in $\mathbb{Z}_p[x]$ obtained by reducing the coefficients of f modulo p.

Theorem 4.1.3. *If $\overline{f}$ is irreducible over $\mathbb{Z}_p$ and the degree of $f(x)$ equals the degree of $\overline{f}(x)$, then $f(x)$ is irreducible over $\mathbb{Q}$.*

Proof. By way of contradiction, suppose $f(x) = g(x)h(x)$, where $g, h \in \mathbb{Z}[x]$, with $1 \leq \deg(g) \leq \deg(f)$ and $1 \leq \deg(h) \leq \deg(f)$. Define

$$\Phi_p : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$$

by

$$f(x) = \sum_{k=0}^{n} a_k x^k \longmapsto \sum_{k=0}^{n} \overline{a}_k x^k = \overline{f}(x),$$

where $\overline{a}_k = a_k + p\mathbb{Z}$. Note that Φ_p is a ring homomorphism. Apply Φ_p to both sides of the equation $f(x) = g(x)h(x)$. Then we obtain

$$\overline{f}(x) = \overline{g}(x)\overline{h}(x)$$

By the assumption, $\deg(f) = \deg(\overline{f})$ which means $p \nmid a_n$. Let

$$\begin{aligned} g(x) &= b_r x^r + (\text{lowest terms}) \\ h(x) &= c_s x^s + (\text{lowest terms}) \end{aligned}$$

Then, $a_n = b_r c_s$. Since p is a prime such that $p \nmid b_r c_s$, by Euclid's Lemma, $p \nmid b_r$ and $p \nmid c_s$. This means $\deg(g) = \deg(\overline{g})$, and $\deg(h) = \deg(\overline{h})$. Hence, $\overline{f}(x)$ is reducible over $\mathbb{Z}_p$. This is a contradiction to the assumption on $\overline{f}$ irreducible over $\mathbb{Z}_p$. The irreducibility over $\mathbb{Z}_p$ implies irreducibility over $\mathbb{Z}$. By Gauss' Lemma, $f(x)$ is irreducible over $\mathbb{Q}$. □

Symmetries of roots of polynomials is the main idea behind Galois theory. We consider the following general cubic polynomial:

$$f(x) = x^3 + a_2x^2 + a_1x + a_0.$$

Suppose that θ_1, θ_2, and θ_3 are the roots of $f(x)$. Then,

$$\begin{aligned} f(x) &= (x-\theta_1)(x-\theta_2)(x-\theta_3) \\ &= x^3 - (\theta_1+\theta_2+\theta_3)x^2 + (\theta_1\theta_2+\theta_2\theta_3+\theta_1\theta_3)x - \theta_1\theta_2\theta_3. \end{aligned}$$

For $i = 1,2,3$, define $s_i(x_1,x_2,x_3)$ as follows:

$$\begin{aligned} s_1 &= x_1+x_2+x_3 \\ s_2 &= x_1x_2+x_1x_3+x_2x_3 \\ s_3 &= x_1x_2x_3. \end{aligned}$$

Then we see that evaluating each s_i at each of the roots of f gives us exactly the three coefficients of f. Consider the symmetric group on 3 letters

$$S_3 = \{1, (1,2), (1,3), (2,3), (1,2,3), (1,3,2)\}.$$

Let $\sigma \in S_3$. Then, we can easily compute that $\sigma(s_i) = s_i$ for all $i = 1,2,3$. For example, if $\sigma = (1\ 2\ 3)$,

$$\begin{aligned} \sigma(s_1) &= s_1(x_3,x_1,x_2) &&= x_3+x_1+x_2 &&= s_1 \\ \sigma(s_2) &= s_2(x_3,x_1,x_2) &&= x_3x_1+x_3x_2+x_1x_2 &&= s_2 \\ \sigma(s_3) &= s_3(x_3,x_1,x_2) &&= x_3x_1x_2 &&= s_3 \end{aligned}$$

Thus, $\sigma(s_i) = s_i$ for all $i = 1,2,3$. Repeating the similar process for all $\sigma \in S_3$, we find that $\sigma(s_i) = s_i$ for $i = 1,2,3$.

Definition 4.1.1. *$h(x_1,x_2,..,x_n) \in K[x_1,x_2,...,x_n]$ is called a symmetric polynomial for $x_1,x_2,..,x_n$ if for any σ in the symmetric group $S_n, \sigma(h) = h$.*

Definition 4.1.2. *The elementary symmetric polynomials in n variables $x_1,...,x_n$, written $e_k(x_1,...,x_n)$ for $k = 0,...,n$, are defined by*

$$\begin{aligned} e_0(x_1,x_2,...,x_n) &= 1, \\ e_1(x_1,x_2,...,x_n) &= \textstyle\sum_{1\le j\le n} x_j, \\ e_2(x_1,x_2,...,x_n) &= \textstyle\sum_{1\le j<k\le n} x_j x_k, \\ e_3(x_1,x_2,...,x_n) &= \textstyle\sum_{1\le j<k<l\le n} x_j x_k x_l, \\ &\vdots \\ e_n(x_1,x_2,...,x_n) &= x_1 x_2 \cdots x_n \end{aligned}$$

so that $e_k(x_1,...,x_n) = 0$ if $k > n$.

Theorem 4.1.4. *(Fundamental Theorem of Symmetric Polynomials) Every symmetric polynomial $f(x_1,x_2,...,x_n) \in K[x_1,...,x_n]$ is a polynomial of elementary symmetric polynomials.*

In section 5.1, we will use a symmetric polynomial to derive the discriminant of a cubic polynomial.

Next, we state a series of definitions and theorems regarding field extensions, automorphisms, splitting fields, separability, and normality.

In Theorem 3.1.2, we mentioned that the degree of the field K over the ground field $\mathbb{Q}$ can be expressed as $[K:\mathbb{Q}]$. In general, if K is a subfield of a field L, the degree of L over K can be written as $[L:K]$.

Theorem 4.1.5. *(Tower Law) Let $K \le L \le M$ be field extensions. Then*

$$[M:K] = [M:L][L:K].$$

Definition 4.1.3. *$L:K$ is called finite extension, if $[L:K] < \infty$.*

Definition 4.1.4. *$L:K$ is called an algebraic extension if for all $\lambda \in L, \lambda$ is a root of some nonzero polynomial in $K[x]$.*

Definition 4.1.5. *An isomorphism σ is both one-to-one and onto map of a field K with itself is called an automorphism of K. The collection of automorphisms of K is denoted by*

$$Aut(K) = \{\sigma : K \to K \mid \sigma \text{ is an automorphism}\}.$$

Definition 4.1.6. *An automorphism $\sigma \in Aut(K)$ is said to fix an element $\alpha \in K$ if $\sigma(\alpha) = \alpha$. If $F \subseteq K$ then an automorphism σ is said to fix F if it fixes all the elements in F. That is, $\sigma(\alpha) = \alpha$ for all $\alpha \in F$.*

Observe that $Aut(L)$ is a group under composition. It is easy to see that if $\sigma, \tau \in Aut(L), \tau \circ \sigma \in Aut(L)$. Since σ is both one-to-one and onto, its inverse σ^{-1} is in $Aut(L)$.

Definition 4.1.7. *If K is a field and f is a polynomial over K, then f splits in K if it can be expressed as a product of linear factors*

$$f(x) = k(x - \alpha_1) \cdots (x - \alpha_n),$$

where $k, \alpha_1, \alpha_2, ..., \alpha_n \in K$.

Definition 4.1.8. *(Splitting Fields) The field Σ is a splitting field for the polynomial f over the field K if $K \subseteq \Sigma$ and*

1. *f splits over Σ,*
2. *$\Sigma = K(\alpha_1, \alpha_2, ..., \alpha_n)$, where $\alpha_1, \alpha_2, ..., \alpha_n$ are the roots of f.*

Definition 4.1.9. *(Normality) An algebraic extension $L : K$ is normal if every irreducible polynomial f over K which has at least one zero in L splits in L.*

Definition 4.1.10. *(Separability) An irreducible polynomial f over a field K is separable over K if it has no multiple zeros in a splitting field for K.*

Definition 4.1.11. *Let K be a field and let $f(x), g(x) \in K[x]$. A common divisor of $f(x)$ and $g(x)$ is a polynomial $c(x) \in K[x]$ such that $c(x) \mid f(x)$ and $c(x) \mid g(x)$. The greatest common divisor* (gcd) *is a monic common divisor of the highest degree.*

Corollary 4.1.6. *If L is the splitting field over $\mathbb{Q}$ of a separable polynomial $f(x)$, then L is normal.*

Note that a Galois extension is an algebraic field extension $K \leq L$ that is normal and separable. If $K \leq L$ is a Galois extension, then $Aut(L/K)$ is called the Galois group of L over K, and write $\text{Gal}(L:K)$.

Let $K \leq L$ be a finite Galois extension with Galois group G, which consists of all K-automorphisms of L. Let $\mathscr{F}$ be the set of intermediate fields, that is, subfields M such that $K \subseteq M \subseteq L$, and let $\mathscr{G}$ be the set of all subgroups H of G. We have defined two maps:

$$\begin{aligned} * &: \mathscr{F} \to \mathscr{G} \\ \ddagger &: \mathscr{G} \to \mathscr{F} \end{aligned}$$

as follows: if $M \in \mathscr{F}$, then M^* is the group of all M-automorphisms of L. If $H \in \mathscr{G}$, then $H^\ddagger$ is the fixed field of H. We have observed that the maps $*$ and $\ddagger$ reverse inclusions, that is, $M \subseteq M^{*\ddagger}$ and $H \subseteq H^{\ddagger *}$. Now, we are ready to state the Fundamental Theorem of Galois Theory from [6].

Theorem 4.1.7. *(Fundamental Theorem of Galois Theory) If $L:K$ is a finite normal field extension inside $\mathbb{C}$, with Galois group G, and if $\mathscr{F}, \mathscr{G}, *, \ddagger$ are defined as above, then:*

1. *The Galois group G has order $[L:K]$.*
2. *The maps $*$ and $\ddagger$ are mutual inverses, and set up an order-reversing one-to-one correspondence between $\mathscr{F}$ and $\mathscr{G}$.*
3. *If M is an intermediate field, then*

$$[L:M] = |M^*| \quad [M:K] = |G|/|M^*|$$

4. *An intermediate field M is a normal extension of K if and only if M^* is a normal subgroup of G.*
5. *If an intermediate field M is a normal extension of K, then the Galois group of $M:K$ is isomorphic to the quotient group G/M^*.*

Theorem 4.1.8. *Let $K \leq L$ be a field extension, where L is the splitting field of a separable polynomial $f \in K[x]$. Then* $\mathrm{Gal}(L:K)$ *has order* $[L:K]$.

It is well-known that the Galois group $\mathrm{Gal}(L:\mathbb{Q})$ is a subgroup of the symmetric group S_n where n is the degree of an irreducible polynomial over $\mathbb{Q}$. By the Lagrange Theorem,

$$|\mathrm{Gal}(L:\mathbb{Q})| \mid |S_n|$$

We now calculate the Galois group of some algebraic extensions. We consider two examples in this section.

Example 4.1.2. *Let $\alpha = \sqrt[3]{2}$. The minimal polynomial $m(x)$ of α is*

$$m(x) = x^3 - 2 \in \mathbb{Q}[x].$$

The roots of $m(x)$ are $\alpha, \omega\alpha, \omega^2\alpha$, where $\omega = \cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3}$, and $\omega^2 = \cos\frac{4\pi}{3} + i\sin\frac{4\pi}{3}$. The splitting field of $m(x)$ is $\mathbb{Q}(\alpha,\omega)$. Now, we investigate the number of elements in the Galois group $\mathrm{Gal}(\mathbb{Q}(\alpha,\omega):\mathbb{Q})$. *Observe that the field $\mathbb{Q}(\alpha,\omega)$ is normal by Corollary 4.1.6. Also, since $m(x)$ is an irreducible polynomial over $\mathbb{Q}$, we have $[\mathbb{Q}(\alpha):\mathbb{Q}] = 3$. Similarly, since ω is a root of the irreducible polynomial x^2+x+1 over $\mathbb{Q}(\alpha)$, we have $[\mathbb{Q}(\alpha,\omega):\mathbb{Q}(\alpha)] = 2$. By the Tower law described in Theorem 4.1.5, we obtain the following*

$$[\mathbb{Q}(\alpha,\omega):\mathbb{Q}] = [\mathbb{Q}(\alpha,\omega):\mathbb{Q}(\alpha)] \cdot [\mathbb{Q}(\alpha):\mathbb{Q}] = 6.$$

Since the field $\mathbb{Q}(\alpha,\omega)$ is the splitting field of a separable polynomial $m(x) \in \mathbb{Q}[x]$, $\mathbb{Q}(\alpha,\omega)$ is normal. Thus,

$$|\mathrm{Gal}(\mathbb{Q}(\alpha,\omega):\mathbb{Q})| = 6$$

Hence, $\mathrm{Gal}(\mathbb{Q}(\alpha,\omega):\mathbb{Q}) \simeq S_3$. *Now, we explore the elements in* $\mathrm{Gal}(\mathbb{Q}(\alpha,\omega):\mathbb{Q})$.

Define

$$\begin{array}{rcccc} \sigma & : & \mathbb{Q}(\alpha,\omega) & \longrightarrow & \mathbb{Q}(\alpha,\omega) \\ & & \alpha & \longmapsto & \omega\alpha \\ & & \omega & \longmapsto & \omega \\ \tau & : & \mathbb{Q}(\alpha,\omega) & \longrightarrow & \mathbb{Q}(\alpha,\omega) \\ & & \omega\alpha & \longmapsto & \omega^2\alpha \\ & & \alpha & \longmapsto & \alpha \end{array}$$

Now, consider the following table.

Table 4.1: The elements in the Galois group of S_3

Elements	α	$\omega\alpha$	$\omega^2\alpha$	order
1	α	$\omega\alpha$	$\omega^2\alpha$	1
σ	$\omega\alpha$	$\omega^2\alpha$	α	3
σ^2	$\omega^2\alpha$	α	$\omega\alpha$	3
τ	α	$\omega^2\alpha$	$\omega\alpha$	2
$\sigma\tau$	$\omega\alpha$	α	$\omega^2\alpha$	2
$\sigma^2\tau$	$\omega^2\alpha$	$\omega\alpha$	α	2

Hence, $\mathrm{Gal}(\mathbb{Q}(\alpha,\omega):\mathbb{Q}) = \{1,\sigma,\sigma^2,\tau,\sigma\tau,\sigma^2\tau\}$. *Lastly, we relate the subgroup diagram in Figure 2.2 as follows:*

Figure 4.1: The lattice of subfields diagram of $\mathbb{Q}(\alpha,\omega):\mathbb{Q}$

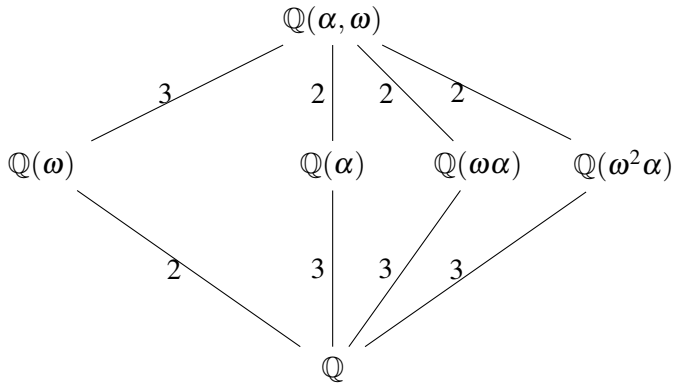
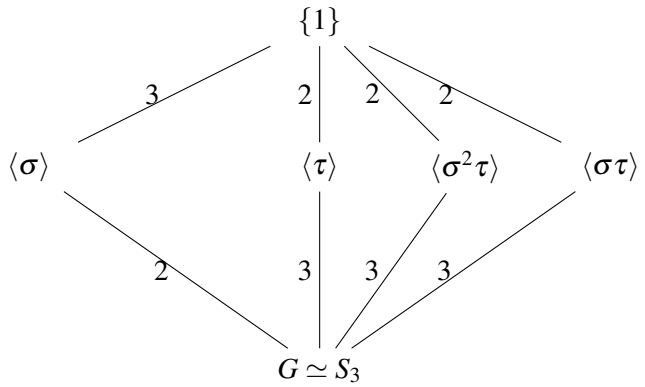


Figure 4.2: The lattice of subgroups diagram of $\mathrm{Gal}(\mathbb{Q}(\alpha,\omega):\mathbb{Q})$



Example 4.1.3. *Consider the following polynomial*

$$f(x)=x^3-6717x-203749.$$

By Theorem 3.1.1, $f(x)$ irreducible over $\mathbb{Q}$ as $f(x)$ is 2239-Eisenstein. Let α_1 be a

root of $f(x)$. The discriminant of $f(x)$ is

$$\Delta[1,\alpha,\alpha^2] = (3)^6(5)^2(2239)^2 > 0,$$

which means all the roots α_1,α_2, and α_3 of $f(x)$ are real and distinct. Then, the splitting field $K = \mathbb{Q}(\alpha_1,\alpha_2,\alpha_3)$ is normal. By Theorem 4.1.8,

$$|\operatorname{Gal}(K:\mathbb{Q})| = [K:\mathbb{Q}] = 3.$$

This implies that the Galois group is isomorphic to $\mathbb{Z}_3$.

4.2 The Chebotarev Density Theorem

Let $f(x)$ be monic and irreducible polynomial over $\mathbb{Q}$. Let p be a prime such that p does not divide the discriminant of $f(x)$. Using Galois theory, we investigate the factorization of polynomials in finite fields $\mathbb{F}_p$ that is related to the elements of the Galois group. Again, we restrict ourselves to the cubic and quartic polynomials in this section. Consider the following example.

Example 4.2.1. *Let $f(x) = x^3 - 5$. Note that $f(x)$ is irreducible over $\mathbb{Q}$ because it is 5-Eisenstein. Let $\theta = \sqrt[3]{5}$ be a root of $f(x)$. The discriminant*

$$\Delta[1,\theta,\theta^2] = -675 = -(3)^3(5)^2.$$

The splitting field of $f(x)$ is

$$L = \mathbb{Q}(\theta,\omega),$$

where ω is a root of the polynomial $x^2 + x + 1 = 0$. We know that $\operatorname{Gal}(L:\mathbb{Q})$ is isomorphic to a subgroup of S_3. In fact,

$$\operatorname{Gal}(L:\mathbb{Q}) \simeq S_3$$

as $[L:\mathbb{Q}] = 6$. We categorize the subgroups of $\operatorname{Gal}(L:\mathbb{Q})$ as follows.

Table 4.2: Cycle types in S_3

Cycle Type #	Elements
Type 1	(1 2 3), (1 3 2)
Type 2	(1 2)(3), (1 3)(2), (1)(2 3)
Type 3	(1)(2)(3)

Now, choose primes p such that $p \nmid \Delta[1,\theta,\theta^2] = -(3)^3(5)^2$. *We choose* $p = 2,7,11,13,17,19$, *and check the factorization over the finite fields* $\mathbb{F}_p$ *with Maple.*

Table 4.3: Polynomial factorization over $\mathbb{F}_p$

p	Factorization over $\mathbb{F}_p$	Cycle Type	Type #
2	$(x+1)(x^2+x+1)$	(1)(2 3)	2
7	x^3+2	(1 2 3)	1
11	$(x^2+3x+9)(x+8)$	(1 2)(3)	2
13	$(x+2)(x+5)(x+6)$	(1)(2)(3)	3
17	$(x^2+11x+2)(x+6)$	(1 2)(3)	2
19	x^3+14	(1 2 3)	1

We notice that there are three types of factorizations of x^3-5 *over* $\mathbb{F}_p$ *for the first 6 primes that do not divide the discriminant of* f. *If we associate each type of factorization to a certain cycle type in* S_3, *we see that the number of each factorization type is equal to the number of each cycle type in* S_3.

Maybe this observation was merely a fluke. Let's see what happens when we try another polynomial, which gives Galois group of D_4. The dihedral group D_n is the symmetry group of an n-sided regular polygon for $n > 1$. The group order of D_n is $2n$. Dihedral groups D_n are non-abelian permutation groups for $n > 2$. The elements in D_4 can be expressed as follows.

$$D_4 = \{1, \sigma, \sigma^2, \sigma^3, \tau, \sigma\tau, \sigma^2\tau, \sigma^3\tau\}, \quad |D_4| = 8,$$

satisfying the following property:

$$\sigma^4 = \tau^2 = 1, \tau\sigma = \sigma^{-1}\tau.$$

Example 4.2.2. *Let $f(x) = x^4 - 5$. Clearly, $f(x)$ is irreducible over $\mathbb{Q}$. Let $\theta = \sqrt[4]{5}$ be a root of $f(x)$. The discriminant*

$$\Delta[1, \theta, \theta^2, \theta^3] = -32000 = -(2)^8(5)^3.$$

The roots of $f(x)$ are $\theta = \sqrt[4]{5}, -\sqrt[4]{5}, i\sqrt[4]{5}, -i\sqrt[4]{5}$. The splitting field of $f(x)$ is $L = \mathbb{Q}(\theta, i)$. By Theorem 4.1.8, L is Galois, and so

$$|\operatorname{Gal}(L : \mathbb{Q})| = [L : \mathbb{Q}] = 8.$$

Define

$$\begin{array}{rcccc} \sigma & : & \mathbb{Q}(\theta,i) & \longrightarrow & \mathbb{Q}(\theta,i) \\ & & \theta & \longmapsto & i\theta \\ & & i & \longmapsto & i \\ \tau & : & \mathbb{Q}(\theta,i) & \longrightarrow & \mathbb{Q}(\theta,i) \\ & & i\theta & \longmapsto & -i\theta \\ & & \theta & \longmapsto & \theta \end{array}$$

It is easy to verify that $\sigma^3\tau = \tau\sigma, \tau\sigma^2 = \sigma^2\tau$, and $\tau\sigma^3 = \sigma\tau$. Hence,

$$\operatorname{Gal}(L : \mathbb{Q}) \simeq D_4.$$

We obtain the following cycle notations that are categorized in four different types shown in Table 4.4.

Table 4.4: Cycle types in D_4

Cycle Type #	Elements
1	$(1\ 2\ 3\ 4),\ (1\ 4\ 3\ 2)$
2	$(1\ 2)(3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4)(2\ 3)$
3	$(1)(2\ 4)(3),\ (1\ 3)(2)(4)$
4	$(1)(2)(3)(4)$

Now, choose primes that do not divide both 2 *and* 5. *Say,*

$$p = 3, 7, 11, 13, 17, 19, 23, \text{ and } 29.$$

Table 4.5: Polynomial factorization over $\mathbb{Q}_p$

p	Factorization over $\mathbb{Q}_p$	Cycle Type	Type #
3	$(x^2+2x+2)(x^2+x+2)$	$(1\ 2)(3\ 4)$	2
7	$(x^2+6x+4)(x^2+x+4)$	$(1\ 2)(3\ 4)$	2
11	$(x+2)(x^2+4)(x+9)$	$(1)(2\ 4)(3)$	3
13	x^4+8	$(1\ 2\ 3\ 4)$	1
17	x^4+12	$(1\ 2\ 3\ 4)$	1
19	$(x+3)(x^2+9)(x+16)$	$(1)(2\ 4)(3)$	3
23	$(x^2+4x+8)(x^2+19x+8)$	$(1\ 2)(3\ 4)$	2
29	$(x^2+18)(x^2+11)$	$(1\ 2)(3\ 4)$	2

We obtain $2/|D_4|$ *chances of the type 1,* $4/|D_4|$ *chances of the type 2,* $2/|D_4|$ *chances of the type 3, and no chance of the type 4. To verify this phenomenon, we used MAPLE to calculate the factorizations for a large number of primes p and we achieved the following results.*

Cycle Pattern	*# of occurrences*
(1 2 3 4)	$\approx 2/8$
(1 2)(3 4)	$\approx 3/8$
(1)(2 4)(3)	$\approx 2/8$
(1)(2)(3)(4)	$\approx 1/8$

Thus, there seems to be a close relationship between the factorization of polynomials in finite fields and elements in their corresponding Galois groups. In [9], Lenstra computes this behaviour for polynomials $f_1(X) = X^4 - X^2 - 1 \in \mathbb{Z}[x]$, and $f_2(X) = X^4 - X - 1 \in \mathbb{Z}[x]$. He finds 1000 primes that do not divide the discriminant of each polynomials f_1 and f_2. The details of this is shown below.

$f_i(X)$	p_0	$\Delta(f_i)$	# of $p \leq p_0$ s.t. $p \nmid \Delta(f_i)$
$X^4 - X^2 - 1$	7933	$-2^4 \cdot 5^2$	1000
$X^2 - X - 1$	7927	-283	1000

Then, he finds how often each factorization occurs among all primes up to p_0.

$f_i(X)$	4	1,3	2,2	1,1,2	1,1,1,1
$X^4 - X^2 - 1$	254	0	379	251	116
$X^4 - X - 1$	258	337	117	253	35

The numbers in the header of the table above represent the factorization pattern. For example, there are 254 primes p up to 7933 such that $f = X^4 - X^2 - 1$ remains irreducible modulo p. The pattern 1, 1, 2 represents that f splits into two linear and one quadratic factors for 251 primes.

Note that $\mathrm{Gal}(f_1(X)) \simeq D_4$ and $\mathrm{Gal}(f_2(X)) \simeq S_4$. Thus, the probability of getting each factorization matches with our results in the previous two examples. It turns out that the elements in each type of cycle notation are related to one another via conjugation in S_n. In Example 2.2.5, we showed that the elements in S_3 can be categorized in different conjugacy classes. We will make this result more precise by considering the conjugacy classes of S_3 and show that these exactly match with the cycle types from Example 4.2.1.

Before we provide the Chebotarev Density Theorem, we summarize the previous result. Let f be a monic polynomial with integer coefficients with degree n.

Write $K = \mathbb{Q}(\alpha_1, \alpha_2, ..., \alpha_n)$, where $\alpha_1, ..., \alpha_n$ are the roots of f. The Galois group G of f is the group of field automorphisms of K. We know that G is a subgroup of S_n. Writing an element $\sigma \in G$ as a product of disjoint cycles (including cycles of length 1), we obtain the cycle pattern of σ, which is a partition $n_1, n_2, ..., n_t$ of n. If p is a prime number not dividing $\Delta(f)$, then we can write f modulo p as a product of distinct irreducible factors over $\mathbb{F}_p$. The degrees of these irreducible factors form the decomposition type of f modulo p. The following theorem tells us that the number of primes with a given decomposition type is proportional to the number of $\sigma \in G$ with the same cycle pattern.

Theorem 4.2.1. *The density of the set of primes p for which f has a given decomposition type $n_1, n_2, ..., n_t$ exists, and it is equal to $1/\#G$ times the number of $\sigma \in G$ with cycle pattern $n_1, n_2, ..., n_t$.*

We verify Theorem 4.2.1 by looking at the following example.

Example 4.2.3. *Recall Example 4.2.1. We showed that the Galois group G of the polynomial $f(x) = x^3 - 5$ is isomorphic to S_3. The order of G is 6. Each of the following subsets*

$$\begin{aligned} C_1 &= \{(1)(2)(3)\} \\ C_2 &= \{(1\ 2)(3),\ (1\ 3)(2),\ (1)(2\ 3)\} \\ C_3 &= \{(1\ 2\ 3),\ (1\ 3\ 2)\} \end{aligned}$$

form a different conjugacy classes. First, consider the cycle pattern with $n_i = 1$ for $i = 1, 2, 3$. Only the identity permutation has this cycle pattern, which is in C_1. Hence, by Theorem 4.2.1, the set of primes p for which f modulo p splits completely into three distinct linear factors has density $1/\#G = 1/6$. Similarly, the cycle pattern with $n_1 = 2, n_2 = 1$ or $n_1 = 1, n_2 = 2$ corresponds to the elements in C_2. Again, using Theorem 4.2.1, the set of primes p for which f modulo p splits into linear-quadratic factors has density $(1/\#G) \times \#C_2 = 3/6$. Similarly the set of primes p for which f remains irreducible modulo p has density $2/6$. These statistics are also confirmed with our experiment in Table 4.3.

Theorem 4.2.2. *(Chebotarev Density Theorem) Let K be an algebraic number field of degree n over $\mathbb{Q}$. Let $C \subset G = \mathrm{Gal}(K : \mathbb{Q})$ be a conjugacy class. Then, the set of*

primes not dividing $\Delta(K:\mathbb{Q})$ has density $\#C/\#G$.

As a consequence of Chebotarev density theorem, for some polynomials, there exist infinitely many primes p so that the polynomial does not factor over the finite fields $\mathbb{F}_p$.

Theorem 4.2.3. *If n is an integer which is not a cube, then for $f(x) = x^3 - n$,*

1. *$f(x)$ is irreducible over $\mathbb{Q}$.*
2. $\mathrm{Gal}(f) \simeq S_3$

Theorem 4.2.4. *(Cauchy's Theorem) Let p be a prime. Let G be a finite group and let p divide $|G|$. Then G has an element of order p and, consequently, a subgroup of order p.*

Theorem 4.2.5. *Let $f(x) \in \mathbb{Z}[x]$ be a monic polynomial, irreducible over $\mathbb{Q}$, and having prime degree p. Then there exists a prime q such that $f(x)$ is irreducible mod q*

Proof. Let $\deg(f(x)) = p$, where p is a prime. Let L be a splitting field of $f(x)$. It is clear that

$$p \mid |\mathrm{Gal}(L:\mathbb{Q})|$$

By Theorem 4.2.4, $\mathrm{Gal}(L:\mathbb{Q})$ has an element $(a_1, a_2, ..., a_p)$ of order p and consequently, a subgroup of order p. This shows that there exists a prime q such that $f(x)$ is irreducible modulo q. □

We immediately obtain the following corollary.

Corollary 4.2.6. *Let n be an integer which is not a cube in $\mathbb{Z}$. Then there exists infinitely many primes q such that*

$$f(x) = x^3 - n$$

is irreducible mod q.

Chapter 5

Minimal Indices in Pure Cubic Fields

In this Chapter, we will focus on analyzing pure cubic fields. In the first three sections, we define pure cubic fields, and calculate an integral basis for them with index forms. Then using the index form we prove the unboundedness of its minimal index via Hall[1]. Furthermore, we construct infinitely many families of pure cubic fields whose index equals a particular positive integer.

5.1 Pure Cubic Fields

We begin with the definition of pure cubic fields.

Definition 5.1.1. *(Pure cubic field) A field K is said to be pure cubic field if there exists a rational integer d, which is not a perfect cube, such that $K = \mathbb{Q}(\sqrt[3]{d})$.*

Generally, we write pure cubic fields as $K = \mathbb{Q}(\sqrt[3]{ab^2})$, where a, b are square-free, and $\gcd(a,b) = 1$. It is easy to see ab^2 is cubefree, and that the minimal polynomial of $\sqrt[3]{ab^2}$ is $m(x) = x^3 - ab^2 \in \mathbb{Z}[x]$ so that $\sqrt[3]{ab^2}$ is an algebraic integer. Let $a = 2$, and $b = 1$. Then, we have the pure cubic field $K = \mathbb{Q}(\sqrt[3]{2})$. Let $\alpha = \sqrt[3]{2}$. Then, its minimal polynomial $m(x)$ is

$$m(x) = x^3 - 2 \in \mathbb{Z}[x].$$

Alaca (pg. 175, [2]) shows that $K = \mathbb{Q}(\alpha) = \mathbb{Q}(\theta)$, where $\theta \in \mathbb{R}$ is a root of the irreducible polynomial given by

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

This shows the existence of pure cubic fields of the form $K = \mathbb{Q}(\theta)$, where $\theta^3 + a\theta + b = 0,\ a,b \in \mathbb{Z}$. We end this section by showing that the discriminant of any polynomial of the form $f(x) = x^3 + px + q$ is $-4p^3 - 27q^2$, where $p,q \in \mathbb{Z}$. Furthermore, we show that if $K = \mathbb{Q}(\theta)$, where θ is a root of $f(x)$, is a pure cubic field, then the discriminant of $f(x)$ equals $-3c^2$ for some positive integer c.

Example 5.1.1. *We show that the discriminant of $f(x) = x^3 + px + q$ is*

$$-4p^3 - 27q^2.$$

Let α, β, γ be the three roots of $f(x)$. Then,

$$f(x) = (x-\alpha)(x-\beta)(x-\gamma),$$

where,

$$\begin{aligned} \alpha+\beta+\gamma &= 0 \\ \alpha\beta+\beta\gamma+\alpha\gamma &= p \\ \alpha\beta\gamma &= -q \end{aligned} .$$

This is equivalent to

$$f(x) = x^3 - (\alpha+\beta+\gamma)x^2 + (\alpha\beta+\beta\gamma+\alpha\gamma)x - \alpha\beta\gamma.$$

By Definition 3.3.1, the discriminant of the polynomial is

$$\begin{aligned} \Delta(f) &= (\alpha-\beta)^2(\beta-\gamma)^2(\alpha-\gamma)^2 \\ \sqrt{\Delta(f)} &= (\alpha-\beta)(\beta-\gamma)(\alpha-\gamma). \end{aligned}$$

Note that $\sqrt{\Delta(f)}$ can be computed by using the determinant of the following Van-

dermonde matrix:

$$M = \begin{bmatrix} 1 & 1 & 1 \\ \alpha & \beta & \gamma \\ \alpha^2 & \beta^2 & \gamma^2 \end{bmatrix}.$$

Thus, $\Delta(f)$ is equal to the determinant of MM^T, where M^T is the transpose of M. That is,

$$\det(MM^T) = \begin{vmatrix} 1 & 1 & 1 \\ \alpha & \beta & \gamma \\ \alpha^2 & \beta^2 & \gamma^2 \end{vmatrix} \begin{vmatrix} 1 & \alpha & \alpha^2 \\ 1 & \beta & \beta^2 \\ 1 & \gamma & \gamma^2 \end{vmatrix}.$$

In Section 4.1, we discussed symmetric polynomials of a cubic polynomial. We define

$$\begin{aligned} s_1 &= \alpha+\beta+\gamma \\ s_2 &= \alpha\beta+\alpha\gamma+\beta\gamma \\ s_3 &= \alpha\beta\gamma. \end{aligned}$$

We already mentioned that $\alpha+\beta+\gamma = 0$ in the previous page. Thus, $s_1 = 0$. Similarly, we have $s_2 = p$ and $s_3 = -q$. Using Newton's identities, MM^T can be expressed as follows

$$MM^T = \begin{bmatrix} 3 & a & b \\ a & b & c \\ b & c & d \end{bmatrix},$$

where

$$\begin{aligned} a &= s_1 = 0 \\ b &= s_1^2 - 2s_2 = -2p \\ c &= s_1 b - s_2 a + 3s_3 = -3q \\ d &= s_1 c - s_2 b + s_3 a = 2p^2. \end{aligned}$$

Therefore, the determinant of MM^T is

$$\det(MM^T) = \begin{vmatrix} 3 & 0 & -2p \\ 0 & -2p & -3q \\ -2p & -3q & 2p^2 \end{vmatrix} = -4p^3 - 27q^2.$$

Now, we prove that if θ is a root of $f(t)$, and $K = \mathbb{Q}(\theta)$ is a pure cubic field, then its discriminant is $-3c^2$ for some positive integer c.

Proof. Assume $L = \mathbb{Q}(\theta)$ is a pure cubic field. Then there exist relatively prime integers h, k such that $K = \mathbb{Q}(\sqrt[3]{hk^2})$. By Definition 3.5.1, we get the following two expressions for $d(K)$.

$$\begin{aligned} d(K) &= \frac{-4p^3 - 27q^2}{(\text{ind}(\theta))^2}, \\ d(L) &= \frac{-27(hk^2)^2}{(\text{ind}(\sqrt[3]{hk^2}))^2}. \end{aligned}$$

Since the two fields are equal, we obtain the following equality.

$$\frac{-4p^3 - 27q^2}{(\text{ind}(\theta))^2} = \frac{-27(hk^2)^2}{(\text{ind}(\sqrt[3]{hk^2}))^2},$$

it follows that

$$\begin{aligned} -4p^3 - 27q^2 &= \frac{-27(hk^2)^2(\text{ind}(\theta))^2}{(\text{ind}(\sqrt[3]{hk^2}))^2} \\ &= -3\left(\frac{3\,\text{ind}(\theta)(hk^2)}{\text{ind}(\sqrt[3]{hk^2})}\right)^2. \end{aligned}$$

Using a result of Dedekind (see [10]), the index of $\sqrt[3]{hk^2}$ is either $1, k$, or $3k$. In any case, we take

$$c = \frac{3\,\text{ind}(\theta)(hk^2)}{\text{ind}(\sqrt[3]{hk^2})} \in \mathbb{Z},$$

which completes the proof. □

5.2 Computing Index Forms

In 1900, Dedekind [10] was the first one to generalize the integral basis for the pure cubic field $K = \mathbb{Q}(\sqrt[3]{ab^2})$.

Theorem 5.2.1. *Let d be a cubefree integer. Set $d = ab^2$, where a, b are squarefree integers and $\gcd(a,b) = 1$. Let $\theta = \sqrt[3]{d}$ and $K = \mathbb{Q}(\theta)$. Then an integral basis for*

K is

$$\begin{cases} \left\{1, \theta, \dfrac{\theta^2}{b}\right\}, & \text{if } d^2 \not\equiv 1 \pmod 9 \\ \left\{1, \theta, \dfrac{b^2 \pm b^2\theta + \theta^2}{3b}\right\}, & \text{if } d \equiv \pm 1 \pmod 9. \end{cases}$$

The field discriminant $d(K)$ of K is given by

$$d(K) = \begin{cases} -27a^2b^2, & \text{if } d^2 \not\equiv 1 \pmod 9 \\ -3a^2b^2, & \text{if } d \equiv \pm 1 \pmod 9. \end{cases}$$

Using this result, we derive the index form of pure cubic fields due to Hall. Note that θ is a root of an irreducible monic polynomial $x^3 - ab^2 \in \mathbb{Z}[x]$. Also, by Theorem 2.1.6 (Euler's Theorem), $a^2 \not\equiv b^2 \pmod 9$ corresponds to $d^2 \not\equiv 1 \pmod 9$. We obtain the following equations.

$$\begin{aligned} \theta + \theta' + \theta'' &= 0 \\ \theta\theta' + \theta\theta'' + \theta'\theta'' &= 0 \\ \theta\theta'\theta'' &= ab^2. \end{aligned} \qquad (*)$$

Consider the case $a^2 \not\equiv b^2 \pmod 9$. Let $\alpha \in O_K$ be such that

$$\begin{aligned} \alpha &= x + y\theta + z\frac{\theta^2}{b} \\ \alpha' &= x + y\theta' + z\frac{\theta'^2}{b} \\ \alpha'' &= x + y\theta'' + z\frac{\theta''^2}{b}, \end{aligned}$$

where $x, y, z \in \mathbb{Z}$, and $\alpha, \alpha', \alpha''$ are the conjugates of α with respect to K. Note that

$$\begin{aligned} \alpha - \alpha' &= (\theta - \theta')\left(y - z\frac{\theta''}{b}\right) \\ \alpha - \alpha'' &= (\theta - \theta')\left(y - z\frac{\theta'}{b}\right) \\ \alpha' - \alpha'' &= (\theta - \theta')\left(y - z\frac{\theta}{b}\right). \end{aligned}$$

By Definition 3.3.3, the discriminant of α is given by

$$\begin{aligned}
D(\alpha) &= (\alpha-\alpha')^2(\alpha-\alpha'')^2(\alpha'-\alpha'')^2 \\
&= \left[(\theta-\theta')\left(y-z\frac{\theta''}{b}\right)(\theta-\theta')\left(y-z\frac{\theta'}{b}\right)(\theta-\theta')\left(y-z\frac{\theta}{b}\right)\right]^2 \\
&= D(\theta)\left[\left(y-z\frac{\theta''}{b}\right)\left(y-z\frac{\theta'}{b}\right)\left(y-z\frac{\theta}{b}\right)\right]^2 \\
&= D(\theta)\left[y^3-\frac{y^2z}{b}(\theta+\theta'+\theta'')+\frac{yz^2}{b}(\theta\theta'+\theta\theta''+\theta'\theta'')-z^3\frac{\theta\theta'\theta''}{b}\right]^2 \\
&= D(\theta)\left[y^3-z^3\frac{ab^2}{b^3}\right]^2 \\
&= \frac{D(\theta)}{b^2}(by^3-az^3)^2.
\end{aligned}$$

From Definition 3.5.1, we know that

$$\operatorname{ind}\alpha = \sqrt{\frac{D(\alpha)}{d(K)}}.$$

The field discriminant $d(K)$ is $-27a^2k^2$. The index of α is

$$\begin{aligned}
\operatorname{ind}\alpha &= \sqrt{\frac{-27a^2b^4}{-27a^2b^4}(by^3-az^3)^2} \\
&= \left|az^3-by^3\right|.
\end{aligned}$$

We may denote the index form of the field K as $I(x,y)$

$$I(x,y) = \left|ax^3-by^3\right|$$

for $x,y\in\mathbb{Z}$. Repeating the similar process for the case $a^2 \equiv b^2 \pmod 9$, we obtain the corresponding index form as follows.

$$I(x,y) = \left|\frac{ax^3-by^3}{9}\right|.$$

5.3 Hall's Theorem

We begin by considering a few examples.

Example 5.3.1. *Let $K = \mathbb{Q}(\sqrt[3]{ab^2})$ be a pure cubic field. Let $a = 5, b = 1$. Since $5^2 \not\equiv 1^2 \pmod 9$, the index form of this field is*

$$I(x,y) = |2x^3 - y^3|.$$

Choose $x = 0, y = \pm 1$. The minimal index $m(K) = 1$. Then by Theorem 3.5.2, K possesses a power basis, $\{1, \sqrt[3]{5}, (\sqrt[3]{5})^2\}$, which verifies the result in Example 3.4.1.

The next example shows that the minimal index can be greater than 1.

Example 5.3.2. *Let $K = \mathbb{Q}(\sqrt[3]{3 \cdot 11^2})$. Since $3^2 \not\equiv 11^2 \pmod 9$, the corresponding index form of K is*

$$I(x,y) = |3x^3 - 11y^3|.$$

Clearly, the minimal index $m(K) = 3 \neq 1$.

In fact, the minimal index of a pure cubic field can be arbitrarily large. The following is a theorem due to Hall (see [1]).

Theorem 5.3.1. *Given a large positive integer n, it is possible to find a cubic field $K = \mathbb{Q}(\sqrt[3]{ab^2})$ in which every integer has an index greater than n.*

Proof. Let $\theta = \sqrt[3]{ab^2}$, where a, b are relatively prime and squarefree. By Theorem 5.2.1, an integral basis for K is

$$\left\{1, \theta, \frac{\theta^2}{b}\right\}, \quad \text{if } a^2 \not\equiv b^2 \pmod 9$$

$$\left\{1, \theta, \frac{b^2 \pm b^2\theta + \theta^2}{3b}\right\}, \quad \text{if } a^2 \equiv b^2 \pmod 9.$$

The corresponding index forms are

$$I(x,y) = \begin{cases} \left|ax^3 - by^3\right|, & \text{if } a^2 \not\equiv b^2 \pmod 9 \\ \dfrac{|ax^3 - by^3|}{9}, & \text{if } a^2 \equiv b^2 \pmod 9. \end{cases}$$

It is sufficient to show that $I(x,y) > 9n$. Consider

$$a \equiv 2 \pmod 7 \text{ and } b \equiv 0 \pmod 7.$$

Then

$$I \equiv 2x^3 \equiv 0, \pm 2 \pmod 7.$$

This shows that $I(x,y) \neq \pm 1$. We eliminate the possibility of $I(x,y) = \pm 2$ by choosing

$$a \equiv 1 \pmod{13} \text{ and } b \equiv 0 \pmod{13}.$$

Then

$$I(x,y) \equiv x^3 \equiv 0, \pm 1, \pm 5 \pmod{13}.$$

This shows that $I(x,y) \neq \pm 2, \pm 3, \pm 4$. We eliminate the possibility of $I(x,y) = \pm 5$ by choosing

$$a \equiv 1 \pmod{19} \text{ and } b \equiv 0 \pmod{19}.$$

Then

$$I(x,y) \equiv x^3 \equiv 0, \pm 1, \pm 7, \pm 8 \pmod{19}.$$

This shows that $I(x,y) \neq \pm 5, \pm 6$. Continuing this process, the index is unbounded. Take a sequence of primes

$$p_1, p_2, ..., p_{9n}$$

of the form $3k+1$, where $k \in \mathbb{Z}$. Due to the choice of these primes, we choose integers $a_1, ..., a_{9n}$ so that a_i and n are not equivalent modulo p_i as described in Definition 2.1.7. That is,

$$\begin{array}{ccc} a_1x^3 & \not\equiv & n \pmod{p_1} \\ a_2x^3 & \not\equiv & n \pmod{p_2} \\ \vdots & \vdots & \vdots \\ a_{9n}x^3 & \not\equiv & n \pmod{p_{9n}}. \end{array}$$

Define

$$b = p_1 p_2 \cdots p_{9n}.$$

We may find a by solving the following system of modular equations using the Chinese Remainder Theorem.

$$\begin{aligned} a &\equiv a_1 \pmod{p_1} \\ a &\equiv a_2 \pmod{p_2} \\ &\vdots \\ a &\equiv a_{9n} \pmod{p_{9N}}. \end{aligned}$$

Then, $I(x,y) \neq \pm N$ for all $1 \leq n \leq 9N$. Thus, the minimal index of a pure cubic field can be arbitrarily large. □

5.4 Main Result

Motivated by Hall, we evaluate the minimal index for infinitely many pure cubic fields. Before we state the main result, we may borrow a theorem from Erdös[11]. Let $f(x)$ be a polynomial having integer coefficients with greatest common divisor 1. We assume that the coefficient of the leading term in $f(x)$ is positive.

Theorem 5.4.1. *If $n \geq 3$ and $f(x)$ satisfies the conditions stated above, then there are infinitely many positive integers x for which $f(x)$ is $(n-1)$-th power free.*

Example 5.4.1. *Let p be a prime of the form $3k+1$, where k is an integer and n be an integer not divisible by p. We show that*

$$f(x) = 27px^3 + 27px^2 + 9px + (p+9n)$$

is squarefree for infinitely many positive integers x.

Since $\gcd(27p, 27p, 9p, p+9n) = 1$, *and $27p$ is positive, we conclude that there are infinitely many positive integers x for which $f(x)$ is squarefree by Theorem 5.4.1.*

We use the result from Section 5.2 about integral bases and the index form of pure cubic fields except we give a small restriction on a, b. When we consider the case $a^2 \equiv b^2 \pmod{9}$, we choose the signs of a and b so that $a \equiv b \equiv 1 \pmod{3}$.

Then the corresponding integral basis is:

$$\left\{1, \theta, \frac{\theta^2 + ab^2\theta + b^2}{3b}\right\}.$$

Consequently, the index form in this case is:

$$I(x,y) = \frac{a(3x+y)^3 - by^3}{9}.$$

We are now ready to state and prove the main result.

Theorem 5.4.2. *Let n be a cubefree positive integer. Then there exist infinitely many pure cubic fields with minimal index equal to n.*

Proof. Let $K = \mathbb{Q}(\sqrt[3]{ab^2})$ be a pure cubic field, where a, and b are squarefree and such that $\gcd(a,b) = 1$. Let $\theta = \sqrt[3]{ab^2}$. Recall the index form $I(x,y)$ for K. If $a^2 \not\equiv b^2 \pmod 9$, then

$$I(x,y) = ax^3 - by^3. \tag{5.1}$$

If $a^2 \equiv b^2 \pmod 9$, then

$$I(x,y) = \frac{a(3x+y)^3 - by^3}{9}. \tag{5.2}$$

Suppose that $n = 1$. Choose $a = 3p$ for any prime $p > 3$. Then the family of pure cubic fields

$$K = \mathbb{Q}(\sqrt[3]{3p})$$

has minimal index $m(K) = 1$ since the index form of K is

$$I(x,y) = 3px^3 - y^3,$$

so that

$$I(0,-1) = 1.$$

Now, suppose that $n > 1$ and cubefree. It is easy to see that the sequence

$$n^2k \text{ for } k = 1,2,...,n-1,$$

does not contain a perfect cube. Thus the cubic polynomials

$$f_k(x) = x^3 - n^2k, \quad k = 1,2,...,n-1,$$

are irreducible over $\mathbb{Q}$. The Galois groups of the cubic polynomials $f_k(x)$ contain an element of order 3 so that by the Chebotarev Density Theorem [9] and Theorem 4.2.5, we may select prime numbers $p_k,\ k = 1,2,...,n-1$ such that $f_k(x)$ is irreducible modulo p_k. Suppose $p_k = 3$. Then, $f_k(x)$ is clearly reducible over $\mathbb{F}_3$. Now suppose, p_k are of the form $3e+2$, where e is an integer. Then

$$X^3 \ \equiv \ n^2k \pmod{p_k}$$

is solvable by Theorem 2.1.7, which contradicts our choice of p_k. Thus, p_k are of the form $3e+1$. Define the positive integer b to be the product of the distinct primes in the sequence

$$p_1, p_2, ..., p_{n-1}.$$

By the choice of p_k, $\gcd(n,b) = 1$, and b is squarefree. Further, we have

$$b \ \equiv \ 1 \pmod{3}.$$

Let z be an integer. We define the integer $a = a(z)$ by

$$a(z) = b(3z+1)^3 + 9n. \tag{5.3}$$

We have shown that there are infinitely many integers z for which a is squarefree in Example 5.4.1. We now have a family of pure cubic fields

$$K = \mathbb{Q}(\sqrt[3]{ab^2}).$$

We will show that these fields have the property that $m(K) = n$. By (5.3), it is easy to see that

$$a \ \equiv \ b \pmod{9},$$

from which we deduce that we are using the index form given by equation (5.2).

As $b \equiv 1 \mod 3$, we clearly have $a \equiv 1 \pmod 3$, so that we use the index form

$$I(x,y) = \frac{(b(3z+1)+9n)(3x+y)^3 - by^3}{9}.$$

A calculation shows that

$$I(-z, 3z+1) = n.$$

If any of the equations

$$I(x,y) = \pm k, \quad k = 1,2,...,n-1$$

are solvable for integers x, y then at least one of the congruences

$$I(x,y) \equiv \pm k \pmod{p_k}, \quad k = 1,2,...,n-1$$

is solvable. These congruences reduce to

$$n(3x+y)^3 \equiv \pm k \pmod{p_k},$$

implying that the congruence

$$X^3 \equiv \pm n^2 k \pmod{p_k}$$

is solvable for X modulo p_k for some k, which contradicts the choice of the p_k. Thus each of the infinitely many pure cubic fields K in this case satisfy

$$m(K) = n,$$

completing the proof. □

We now give examples illustrating our main result.

Example 5.4.2. *We show there exists infinitely many pure cubic fields K with*

$$m(K) = 4.$$

Begin by choosing primes p_k, $k = 1,2,3$ *such that the cubic polynomials*

$$f_k(x) = x^3 - 4^2k, \quad k = 1,2,3$$

are irreducible modulo p_k. *We find that we may choose* $p_1 = p_2 = 7$ *and* $p_3 = 13$. *Thus* $b = 7 \cdot 13$. *Next we choose a positive integer* z *so that*

$$7 \cdot 13 \cdot (3z+1)^3 + 4 \cdot 9$$

is squarefree. We find the value $z = 0$ *yields the squarefree integer 127. As in the proof of our theorem, we have*

$$a = 127 \quad \text{and} \quad b = 91.$$

The pure cubic field

$$\mathbb{Q}\left(\sqrt[3]{127 \cdot 91^2}\right)$$

has index form

$$I(x,y) = \frac{127(3x+y)^3 - 91y^3}{9}.$$

The cubic index form equations

$$I(x,y) = \pm k, \quad k = 1,2,3$$

are insolvable by construction, but

$$I(0,1) = 4,$$

so that

$$m(K) = 4.$$

Next we consider an example which is not covered by our theorem.

Example 5.4.3. *We give a pure cubic field* K *with* $m(K) = 8$. *Set*

$$K = \mathbb{Q}\left(\sqrt[3]{23 \cdot 15^2}\right).$$

The index form for K is

$$I(x,y) = 23x^3 - 15y^3.$$

Using Magma, we find that the cubic index form equations

$$I(x,y) = \pm k, \quad k = 1,2,...,7$$

are all insolvable. However

$$I(1,1) = 8,$$

so that

$$m(K) = 8.$$

Chapter 6

Conclusion and Future Work

6.1 Conclusion

This thesis extends Hall's idea on the unboundedness of minimal indices of pure cubic fields. Our main goal was to construct a family of infinitely many pure cubic fields with the minimal index equal an arbitrary cubefree integer n. Chebotarev Density Theorem held an important role in performing this construction. In fact, we needed to choose proper primes so that we find the appropriate expressions for the index forms for these fields and show that the solvability of the index $I(x,y) = 1,2,...,n-1$ is impossible.

In Chapter 4, we observed that there was a special relationship between the conjugacy class of a Galois group G and the factorization of polynomials over some finite fields. By the Chebotarev Density Theorem, it turns out that the factorization of polynomials of the form $f(x) = x^3 - ab^2$ depends on the density $|C|/|G|$ where C is a conjugacy class of G. Further, the irreducibility of the polynomials $f(x)$ over $\mathbb{F}_p$ occurred for some primes of the form $p = 3k+1$.

In Chapter 5, we first introduced Dedekind's result on integral bases of pure cubic fields. Once the index forms were set up, we showed that the minimal indices of pure cubic fields are unbounded by Hall [1]. In section 5.4, We have constructed infinitely many pure cubic fields with minimal index equal to one. Then, we used Erdös' theorem on squarefree integers to set up appropriate expressions for each parameters a,b of the standard form $K = \mathbb{Q}(\sqrt[3]{ab^2})$. Finally, we used the Cheb-

otarev Density Theorem to show that the index form does not equal any positive integers less than the arbitrary cubefree integer n.

6.2 Future Work

We can apply our result to different algebraic number fields. Dummit and Kisilevsky [7] and Huard [8] showed that the minimal indices of cyclic cubic fields are unbounded. Funakura[12] computed integral bases of pure quartic fields. Gaál, and Petrányl [13] calculated the elements of minimal index in an infinite parametric family of simplest quartic fields. Nakahara [14, 15] proved that the minimal index is unbounded for bicyclic and cyclic quartic fields. The idea presented in this thesis can still be applied to these fields mentioned above. Our next goal is to extend our result to some of these fields mentioned above. We finish our discussion with providing some examples of the minimal indices of pure quartic and cyclic cubic fields.

Example 6.2.1. *Let $K = \mathbb{Q}(\sqrt[4]{2})$. Then $\theta = \sqrt[4]{2}$ is a root of the monic polynomial $f(x) = x^4 - 2$. The discriminant of θ is*

$$D(\theta) = -2048.$$

By the result in Funakura [12], an integral basis for K is

$$\left\{1, \theta, \theta^2, \theta^3\right\}.$$

Thus, the most general element α in the ring of integers O_K is expressed by

$$\alpha = a + b\theta + c\theta^2 + d\theta^4, \quad \text{where } a,b,c,d \in \mathbb{Z}.$$

By using Maple, we find that

$$D(\alpha) = -2048\{(-2d^2 + b^2)(4d^4 - 16bc^2d + 8c^4 + b^4 + 4b^2d^2)\}^2.$$

The Diophantine equation

$$(-2d^2 + b^2)(4d^4 - 16bc^2d + 8c^4 + b^4 + 4b^2d^2) = 1$$

is solvable if $(b,c,d) = (1,0,0)$. *Hence, the minimal index* $m(K) = 1$. *Therefore, K is a monogenic field.*

Example 6.2.1 considers one particular pure quartic field, which possesses a power basis. We immediately recognize that the index form is more complicated compared to the case of pure cubic fields even though we are considering the simplest pure quartic field. Finding a family of infinitely many of these fields with minimal index equal to an arbitrary integer can be a challenging work. The first step towards this problem would be to generalize the index forms of pure quartic fields by considering all the necessary cases for integral basis computed by Funakura [12]. Lastly, we look at an example of cyclic cubic fields.

Example 6.2.2. *Let* $K = \mathbb{Q}(c,d)$ *be a cyclic cubic field. We need to choose appropriate integers c and d so that every representation of*

$$4m = c^2 + 27d^2$$

characterizes a unique cyclic cubic field, where m is a product of distinct primes of the form $3k+1$. *Let* θ *be a root of* $f(x) = x^3 - 6717x - 203749$. *An integral basis for K is*

$$\left\{1, \frac{2+\theta}{3}, \frac{37+7\theta+\theta^2}{45}\right\}.$$

By Example 4.1.3, we have shown that

$$\mathrm{Gal}(K/\mathbb{Q}) \simeq \mathbb{Z}_3$$

as expected. The index form of K is

$$I(x,y) = 5x^3 - 371y^3 + 7x^2y - 146xy^2.$$

Magma shows that there is no integers x,y *such that* $I(x,y) = 1,2,3,$ *or* 4. *Since the equation* $I(1,0) = 5$,

$$m(K) = 5.$$

We made decent progress on constructing a family of infinitely many cyclic cubic fields of index equal to n. Example 6.2.2 only shows one particular cyclic

cubic field with the case $n = 5$ to confirm the progress. A lot of work has been done with algebraic number fields of degree 3. However, there is a lot of work waiting for us for higher degree number fields as mentioned above. There is huge research potential exploring the minimal indices of these number fields.

Bibliography

[1] M. Hall, *Indices in cubic fields*, Bull. Amer. Math. Soc., **43**, pp. 104-108, (1937) → pages 2, 5, 52, 58, 66

[2] S. Alaca and K. S. Williams, *Introductory Algebraic Number Theory*, Cambridge University Press, New York (2004) → pages 19, 32, 53

[3] J. B. Fraleigh, *A First Course in Abstract Algebra*, Pearson, New York, 7th Ed, (2002) → pages

[4] K. H. Rosen, *Elementary Number Theory and Its Application*, Pearson, Boston, 6th Ed, (2010) → pages

[5] H. T. Engstrom, *On the common index divisors of an algebraic field*, Transactions of the American Mathematical Society, vol. **32**, pp. 223-237, (1930) → pages 34

[6] I. Stewart, *Galois Theory*, Chapman and Hall, New York, 2nd Ed, (1989) → pages 41

[7] D. S. Dummit and H. Kisilevsky, *Indices in cyclic cubic fields*, Number Theory and Algebra, Academic Press, New York, pp. 29-42, (1977) → pages 67

[8] J. G. Huard, *Index Forms and power bases for cyclic cubic fields*, Ph. D. Thesis, The Pennsylvania State University, University Park, Pennsylvania, (1978) → pages 67

[9] H. W. Lenstra and P. Stevenhagen, *Chebotarëv and his density theorem*, The Mathematical Intelligencer, **18**, pp. 26-37, (1996) → pages 49, 62

[10] R. Dedekind, *Über die Anzahl der Idealklassen in reinen kubischen Zahlkörpern*, J. reine angew. Math. **121**, pp. 40-123, (1900) → pages 55

[11] P. Erdös, *Arithmetic properties of polynomials*, J. London Math. Soc. **28**, pp. 416-425 (1953) → pages 60

[12] T. Funakura, *On integral basis of pure quartic fields*, Math. J. Okayama Univ. **26**, pp. 27-41, (1984) → pages 67, 68

[13] I. Gaál, G. Petrányl, Debrecen *Calculating all elements of minimal index in the infinite parametric family of simplest quartic fields*, Czechoslovak Mathematical Journal, **64**, pp. 465-475, (2014) → pages 67

[14] T. Nakahara, *On the indices and integral bases of non-cyclic but abelian biquadratic fields*, Arch. Math. (Basel) **41**, pp. 504-508, (1983) → pages 67

[15] T. Nakahara, *On the minimum index of a cyclic quartic field*, Arch. Math. (Basel) **48**, pp. 322-325, (1987) → pages 67

[16] B. K. Spearman, Q. Yang, and J. Yoo, *Minimal indices of pure cubic fields*, Archiv der Mathematik, **106**, Issue 1, pp. 35-40, (2015) → pages iv

[17] D. A. Marcus, *Number Fields*, Springer-Verlag, New York, (1977) → pages

[18] J. P. Cook, *Computing integral bases*, `http://math.ou.edu/ jcook/LaTeX/integralbases.pdf` (Feb. 2010) → pages 25