The Classification of Monogenic Quartic Orders via Diophantine Equations

by

Jaxon Shumaker

A dissertation accepted and approved in partial fulfillment of the
requirements for the degree of
Doctor of Philosophy
in Mathematics

Dissertation Committee:
Ben Young, Chair
Shabnam Akhtari, Advisor
Ben Elias, Core Member
Chris Sinclair, Core Member
Matt Polizzotto, Institutional Representative

University of Oregon
Summer 2025

DISSERTATION ABSTRACT

Jaxon Shumaker

Doctor of Philosophy in Mathematics

Title: The Classification of Monogenic Quartic Orders via Diophantine Equations

In this study, we will focus on classifying quartic monogenic orders based on two algebraic relations. First, we introduce index forms and study the connection between the solution set of particular index form equations and the monogenizations type of quartic rings. Using these observations, we can completely classify all quartic polynomials that define monogenic rings satisfying one of the algebraic relations. Next, we incorporated information about the Galois groups of quartic polynomials and results counting the number of solutions to particular cubic Diophantine equations. Using this, we provide new results on the scarcity of monogenic orders that do not satisfy either of the algebraic relations, assuming the field of fractions of the order meets certain Galois conditions.

CURRICULUM VITAE

NAME OF AUTHOR: Jaxon Shumaker

GRADUATE AND UNDERGRADUATE SCHOOLS ATTENDED:

University of Oregon, Eugene
Portland State University, Portland
Clark College, Vancouver

DEGREES AWARDED:

Doctor of Philosophy, Mathematics, 2025, University of Oregon
Masters of Science, Mathematics, 2019, Portland State University
Bachelors of Science, Mathematics, 2017, Portland State University
Associate of Science, Science Transfer, 2015, Clark College

AREAS OF SPECIAL INTEREST:

Computational Number Theory including: Diophantine equations, Algebraic heights in Number fields, Power Integral basis, Integer representation by binary forms, and CM-fields.

PROFESSIONAL EXPERIENCE:

University of Oregon: Graduate Teaching Assistant
Johns Hopkins Center for Talented Youth: Teaching Assistant
Portland State University: Peer Math Tutor
Clark College: Peer Math Tutor

ACKNOWLEDGMENTS

I would like to express my deepest gratitude to my advisor, Shabnam Akhtari, for introducing me to this area of research and providing invaluable insight throughout my graduate studies. Without her guidance and expertise, the results presented in this dissertation would not have been possible. I am especially grateful for her understanding and support during the many personal and academic challenges I faced along the way.

I also wish to thank Ben Young, chair of my dissertation committee, whose guidance was instrumental in helping me navigate the dissertation process. His thoughtful advice, especially on writing and structure, was essential to the completion of this work. I am also grateful to the other members of my committee, Chris Sinclair, Ben Elias, and Matt Polizzotto, for their time, support, and thoughtful consideration of my dissertation. This research was supported by NSF grant number DMS-2039316.

I am especially thankful for the mathematical community at the University of Oregon, and in particular for my fellow graduate students Greg Knapp, Kyla Pohl, Samantha Platt, Francis Dunn, Sean Haight, Sidney Washburn, and many others. Their friendship, encouragement, and willingness to exchange ideas created a warm, collaborative, and intellectually stimulating environment that made this journey not only possible but enjoyable. The example they set, both professionally and personally, will stay with me for the rest of my life.

I want to extend special thanks to my close friend, Eric Driggers. His help during the early stages of developing my code was critical, and his generosity in allowing me to run extended computations on his server made much of this work feasible.

Finally, I want to express my heartfelt gratitude to my wife and daughter. Their constant belief in me, their encouragement during setbacks, and their joy in my successes have meant everything to me. They supported me through long nights of work, weekend grading marathons, and too many evenings away. This dissertation would not have been possible without their love and sacrifice.

Dedicated to my daughter, Tommi Lee, with the hope that you will always pursue your dreams with courage and joy.

TABLE OF CONTENTS

LIST OF FIGURES

Figure Page

LIST OF TABLES

Table Page

CHAPTER 1

INTRODUCTION

At the heart of classical algebraic number theory is the study of the arithmetic of algebraic integers in field extensions of the rational numbers. The arithmetic in the rings consisting of the integers in these number fields can present many complications that are not present when working over the rational integers. The existence of potentially infinitely many units, a breakdown of unique factorization, and the presence of primes not found in the rational integers all pose difficulties when performing computations. Occasionally, we will have the benefit of working in a ring of algebraic integers that is generated by a single element as an algebra over the rational integers. Such rings are called monogenic and benefit from having a simple multiplication table and a $\mathbb{Z}$-module structure. This makes many computations easier to perform in monogenic rings.

In this dissertation, we study monogenic rings in a quartic field extension of the rational numbers. For a given monogenic ring in a quartic field, we will investigate the algebraic relation that can exist between sufficiently distinct choices of generators. Bérczes, Evertse, and Győry in [BEG13] put forward two algebraic relations between the generators of monogenic rings. They then go on to show that if a field meets certain assumptions on its Galois group, then the monogenic orders with multiple distinct generators that do not meet either of their relations are uncommon. In this dissertation, we investigate the connection between the algebraic relation introduced in [BEG13] and a specific Diophantine equation associated with the index of an algebraic number. Our primary goal is to understand the prevalence of these exceptional monogenic rings under various assumptions regarding the Galois group. In our investigation, we slightly expand upon the results of Bérczes, Evertse, and Győry to include all biquadratic fields. We also provide some partial results for other quartic fields and a parametrization of the minimal polynomials for generators matching one of the relations given by Bérczes Evertse, and Győry. Lastly, using computational tools, we discovered more than 150 explicit examples of monogenic rings that do not satisfy either of the algebraic conditions set out by Bérczes, Evertse, and Győry.

1.1 Basic Concepts and Notation

A *rank n ring* is a free $\mathbb{Z}$-module of rank n, which possesses a multiplication making it into a $\mathbb{Z}$-algebra. A rank 3 ring is called a *cubic ring*, and a rank 4 ring is called a *quartic ring*. We will define a *number field* to be a finite algebraic extension of $\mathbb{Q}$. If K is a number field, we write $\mathcal{O}_K$ for the largest subring of K consisting entirely of algebraic integers; this ring is called the *ring of integers* of K. For a number field K, if the $\dim_{\mathbb{Q}}(K) = n$ then $\mathcal{O}_K$ is a rank n ring.

Definition 1.1. We say that $\mathcal{O}$ is an *order* of K if it is a subring of $\mathcal{O}_K$ such that the quotient module $\mathcal{O}_K/\mathcal{O}$ is finite. Alternatively, a subring $\mathcal{O}$ of $\mathcal{O}_K$ is an order if $\mathcal{O}$ is a ring of rank $\dim_{\mathbb{Q}}(K)$. Without regard to a number field, a finite rank ring, $\mathcal{O}$, is said to be an order if the fraction field of $\mathcal{O}$ is isomorphic to a number field.

Since orders are a somewhat uncommon algebraic object, the following example is provided.

Example 1.2. The number $\phi = (1 + \sqrt{5})/2$ is an algebraic integer with minimal polynomial $T^2 - T - 1$. The number field $K = \mathbb{Q}(\phi)$ is quadratic, and it is well known that the ring of integers of K is $\mathbb{Z}[\phi]$. Consider the ring $\mathbb{Z}[\sqrt{5}] \subseteq \mathbb{Z}[\phi]$. The set $\{1, \sqrt{5}\}$ is a $\mathbb{Z}$-module basis for $\mathbb{Z}[\sqrt{5}]$, so we can see that the module index $[\mathbb{Z}[\sqrt{5}] : \mathbb{Z}[\phi]] = 2$.

An order that is a quartic ring is a quartic order, and an order that is a cubic ring is a cubic order. Our primary consideration here is the study of quartic orders, which are generated by a single element as a $\mathbb{Z}$-algebra.

Definition 1.3. We say that an order $\mathcal{O}$ is *monogenic* if it is generated by a single element $\xi \in \mathcal{O}$ as a $\mathbb{Z}$-algebra, that is, $\mathcal{O} = \mathbb{Z}[\xi]$. For a monogenic order $\mathcal{O}$, if $\xi \in \mathcal{O}$ is such that $\mathcal{O} = \mathbb{Z}[\xi]$ we say that ξ is a *monogenizer* of $\mathcal{O}$.

For any algebraic integer $\xi \in \mathbb{C}$ whose minimal polynomial is of degree n, the ring $\mathbb{Z}[\xi]$ will be a monogenic order or rank n, in the field $\mathbb{Q}(\xi)$.

Definition 1.4. Let $\mathcal{O}$ be a monogenic order with monogenizer ξ. The *field of fractions of* $\mathcal{O}$ is the number field $\mathbb{Q}(\xi)$.

Our approach to quartic monogenic orders begins with a quartic algebraic integer ξ. Let

$$f_\xi(T) = T^4 + a_1T^3 + a_2T^2 + a_3T + a_4 \tag{1.1}$$

be the minimal polynomial of ξ. Then the $\mathbb{Z}$-algebra $\mathbb{Z}[\xi]$ is an order in $\mathbb{Q}(\xi)$, with the basis $\{1, \xi, \xi^2, \xi^3\}$ whose multiplication table is given by the relations $\xi^4 = -(a_1\xi^3 + a_2\xi^2 + a_3\xi + a_4)$ and $\xi^n\xi^m = \xi^{n+m}$. Several definitions relating to orders of the form $\mathbb{Z}[\xi]$ are given below.

Remark 1.5. When we write $\mathcal{O} = \mathbb{Z}[\xi]$, for an algebraic integer $\xi \in \mathbb{C}$, we specify $\mathcal{O}$ as a ring with $\mathbb{Z}$-module bases $\{1, \xi, \xi^2, ..., \xi^{n-1}\}$.

If ξ is a monogenizer of $\mathcal{O}$, then so is $\pm\xi + \lambda$ for any $\lambda \in \mathbb{Z}$.

Definition 1.6. We will say that two monogenizers ξ and β are $\mathbb{Z}$-*equivalent* if $\beta = \pm\xi + \lambda$. We call a $\mathbb{Z}$-equivalence class of monogenizers of $\mathcal{O}$ a *monogenization* of $\mathcal{O}$. We say "the monogenization defined by ξ", or "the monogenization ξ defines" to refer to the $\mathbb{Z}$-equivalence class containing ξ. Notationally, we write $\xi + \mathbb{Z} = \{\pm\xi + n : n \in \mathbb{Z}\}$ to represent the monogenization defined by ξ.

Since every monogenization will have an infinite number of monogenizers, we will study the monogenizations of an order.

Definition 1.7. A monogenic order is *n times monogenic* if it has at least n monogenizations, and it is *exactly n times monogenic* if it has exactly n monogenizations.

Our focus will not be on the number of monogenizations but on how different monogenizations are related. In [BEG13] Bérczes, Evertse, and Győry introduce two types of relations between the monogenizers of a given order.

Definition 1.8. Let ξ, β be monogenizers of an order $\mathcal{O}$. We say that ξ and β have a *type I* relation if the following holds true:

1. $\xi, \beta \in \mathcal{O}$, and $\mathbb{Z}[\xi] = \mathcal{O} = \mathbb{Z}[\beta]$, as rings.
2. There exists $A \in \mathrm{GL}_2(\mathbb{Z})$ such that

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

and

$$\beta = \frac{a\xi + b}{c\xi + d}$$

with $c \neq 0$. We will use the notation $A \cdot \xi$ to indicate the expression $\dfrac{a\xi + b}{c\xi + d}$.

We will write $\beta \sim_1 \xi$ in this case. An order $\mathcal{O}$ is said to be type 1 if it has two monogenizers ξ and β with $\xi \sim_1 \beta$.

Remark 1.9. Let $\xi, \beta \in \mathcal{O}$ be monogenizers of $\mathcal{O}$. If $\xi \sim_1 \beta$, then computationally we can show that $\beta + \lambda \sim_1 \xi$, for any $\lambda \in \mathbb{Z}$.

Therefore, we can extend the notion of type I relations to monogenizations. To indicate that the monogenizations $\xi + \mathbb{Z}$ and $\beta + \mathbb{Z}$ have a type I relation, we write $\xi + \mathbb{Z} \sim_1 \beta + \mathbb{Z}$. Thus, an order is type I if it has two monogenizations $\xi + \mathbb{Z}$ and $\beta + \mathbb{Z}$ such that $\xi + \mathbb{Z} \sim_1 \beta + \mathbb{Z}$.

Definition 1.10. Let ξ, β be monogenizers of $\mathcal{O}$. We say that ξ and β have a *type II* relation if the following is true:

1. $\mathcal{O} = \mathbb{Z}[\xi] = \mathbb{Z}[\beta]$.
2. There exists $m, n, k, \ell, c_0, c_1 \in \mathbb{Z}$ such that

$$\xi = m\beta^2 + k\beta + c_0 \tag{1.2}$$

and

$$\beta = n\xi^2 + \ell\xi + c_1. \tag{1.3}$$

In this case, we write $\beta \sim_2 \xi$. An order $\mathcal{O}$ is considered type II if it has two monogenizers ξ and β with $\beta \sim_2 \xi$. If $\beta \sim_2 \xi$ then $\xi \sim_2 \beta$ by definition and if $\xi + \lambda_0 \in \xi + \mathbb{Z}$ and $\beta + \lambda_1 \in \beta + \mathbb{Z}$ then substitution will give us $(\xi + \lambda_0) \sim_2 (\beta + \lambda_1)$. Therefore, we can extend the definition of type II to monogenizations. Similarly to type I, an order $\mathcal{O}$ is type II if it has two monogenizations $\xi + \mathbb{Z}$ and $\beta + \mathbb{Z}$ such that $\xi + \mathbb{Z} \sim_2 \beta + \mathbb{Z}$.

Example 1.11. Consider the polynomial $f(T) = T^4 - 4T^2 - T + 1$. One can show that f is irreducible. Let $\xi \in \mathbb{C}$ be a root of f. Then the ring $\mathcal{O} = \mathbb{Z}[\xi] \cong \mathbb{Z}[T]/(f(T))$ is monogenic. Fix the basis $\{1, \xi, \xi^2, \xi^3\}$ of $\mathcal{O}$. In [GPP96] Example 1, Gaál, Pethő, and Pohst give a list of all monogenizations of $\mathcal{O}$, which is shown below. For each monogenization, only the coordinates for ξ, ξ^2, and ξ^3 are given, as these uniquely identify them.

$$(1,0,0), (-12,1,3), (-8,1,2), (-5,0,1), (-4,0,1),$$
$$(-4,1,1), (-3,0,1), (0,1,0), (0,2,1), (1,2,-1), (3,1,-1),$$

$$(4,1,-1),(4,9,-5),(4,33,16),(8,1,-2),(14,3,-4).$$

Note that $(1,0,0)$ is the monogenization $\xi+\mathbb{Z}$, and $(0,1,0)$ represents the monogenization $\xi^2+\mathbb{Z}$. If we let $\beta=\xi^2$, then using the minimal polynomial for ξ we see

$$0=\xi^4-4\xi^2-\xi+1.$$

So,

$$\xi=\beta^2-4\beta+1.$$

Therefore, $\xi\sim_2\xi^2$ so $\mathcal{O}$ is a type II order.

The order $\mathcal{O}$ is also type I. The triple $(-4,0,1)$ represents the monogenization $(-4\xi+\xi^3)+\mathbb{Z}$. We will show that $(-4\xi+\xi^3)+\mathbb{Z}\sim_1\xi+\mathbb{Z}$. Consider the matrix

$$A=\begin{pmatrix}1 & -1\\ -1 & 0\end{pmatrix}\in \mathrm{GL}_2(\mathbb{Z}).$$

Notice that

$$A\cdot\xi=\frac{\xi-1}{\xi}, \tag{1.4}$$

and using the minimal polynomial, we see that

$$-1=\xi^4-4\xi^2-\xi. \tag{1.5}$$

Substituting for -1 in (1.4) using (1.5) we have

$$\begin{aligned}\frac{\xi-1}{\xi}&=\frac{\xi+\xi^4-4\xi^2-\xi}{\xi}\\ &=-4\xi+\xi^3.\end{aligned}$$

Thus, $\xi\sim_1(-4\xi+\xi^3)$, and $\mathcal{O}$ is type I.

For an algebraic number ξ we denote f_ξ to be the minimal polynomial of ξ and $\xi=\xi_{(1)},...,\xi_{(n)}$ to be the algebraic conjugates of ξ. Much of our discussion will utilize the homogenization of minimal polynomials. For this reason, we provide the following definition.

Definition 1.12. Let α be an algebraic number of degree n. We define the *minimal form of* α to be the binary form $T_2^n f_\alpha(T_1/T_2)$, where f_α is the minimal polynomial of α.

In Chapter 5, we will frequently make use of the Galois groups of normal closures of the field of fractions of an order. For convenience, we provide the following definition to be used in these situations.

Definition 1.13. For an order $\mathcal{O}$ with field of fractions K, and $\overline{K}$ the normal closure of K. We define the *Galois group of* K and *the Galois group of* $\mathcal{O}$ to both be the group $\mathrm{Gal}(\overline{\mathrm{K}}/\mathbb{Q})$.

In [BEG13] Bérczes, Evertse, and Győry prove that in a quartic field K whose Galois group is S_4, all but finitely many two times monogenic orders are type I or type II. They go on to produce an infinite family of type I and type II orders; however, no examples of orders that are neither type I nor type II are given. This motivated the following Conjecture.

Conjecture 1. *Let K be a quartic field. Then all but finitely many two times monogenic orders of K are type I or type II.*

Since the only possible Galois groups of a quartic number field are the subgroups of S_4 that act transitively on a set of size 4, the Galois group of K must be one of V_4, C_4, D_4, A_4, or S_4. One approach to investigating Conjecture 1 is to study fields for each of the possible Galois groups. The group S_4 is handled by Bérczes, Evertse, and Győry in [BEG13]. Here, we will complete the case of fields with Galois group V_4 and provide some limiting conditions on orders in fields with Galois groups C_4 and D_4.

1.2 Summary of Results

The first Theorem we will prove shows a connection between type I monogenizations and cubic resolvent rings. For any quartic ring Q, there is an associated cubic ring R called a cubic resolvent ring, [Bha04] Corollary 5. In Section 2.3, we establish the basics of cubic resolvent rings.

Theorem 1.14. *Let $\mathcal{O}$ be a two times monogenic quartic order. Then, either $\mathcal{O}$ is a type I order, or the cubic resolvent ring of $\mathcal{O}$ is two times monogenic.*

In Chapter 3, we will develop the tools needed to prove Theorem 1.14. Our work in Chapter 3 will also be needed to prove the following results.

Theorem 1.15. *Let $\mathcal{O}$ be a two times monogenic quartic order in $\mathbb{C}$. The following holds:*

1. *If the Galois group of $\mathcal{O}$ is V_4, then $\mathcal{O}$ is type I.*
2. *If the Galois group of $\mathcal{O}$ is C_4 or D_4 and $\mathrm{Disc}(\mathcal{O}) < 0$ then $\mathcal{O}$ is type I, for all but finitely many orders.*
3. *If the Galois group of $\mathcal{O}$ is C_4 or D_4 and $\mathrm{Disc}(\mathcal{O}) > 0$, then $\mathcal{O}$ is type I or there exists $\xi \in \mathcal{O}$ a monogenizer satisfying at least one of the following:*

   a)

$$\begin{aligned} &|(\xi_1-\xi_2)(\xi_1-\xi_4)(\xi_2-\xi_3)(\xi_3-\xi_4)| \\ &\leq \left|2(\xi_{(1)}\xi_{(3)}-\xi_{(2)}\xi_{(4)})+(\xi_1+\xi_3)(\xi_2+\xi_4)\right| \end{aligned}$$

   b)

$$\begin{aligned} &8(\xi_1-\xi_2)(\xi_1-\xi_4)(\xi_2-\xi_3)(\xi_3-\xi_4) \\ &\leq \left(2(\xi_{(1)}\xi_{(3)}-\xi_{(2)}\xi_{(4)})+(\xi_1+\xi_3)(\xi_2+\xi_4)\right)^2. \end{aligned}$$

A direct corollary of Theorem 1.15 is the following.

Corollary 1.16. *Let K be a biquadratic number field. Then, every two times monogenic order in K is of type I.*

Chapter 4 also provides a complete description of the orders, which are type II.

Theorem 1.17. *Let $\mathcal{O}$ be a quartic order. Then $\mathcal{O}$ is a type II monogenic order if and only if $\mathcal{O} = \mathbb{Z}[\xi]$ for an algebraic integer ξ with minimal polynomial*

$$f_\xi(T) = T^4 + 2kT^3 + (k^2+\ell)T^2 + (\ell k - 1)T + c,$$

or

$$f_\xi(T) = T^4 + kT^3 + \frac{k^2+\ell}{4}T^2 + \frac{k\ell-1}{8} + c,$$

where $(k, \ell, c) \in \mathbb{Z}^3$.

Using Theorem 1.17 in Section 4.1, we provide an infinite family of type II orders.

Chapter 2 presents a detailed study of the preliminary results necessary for our inquiry. Chapter 3 and Chapter 4 study the algebraic relations introduced in [BEG13] in the context of specific Diophantine equations related to the algebraic index of a number. While brief, Chapter 4 contains the proof of Theorem 1.17, as well as examples of Type II orders. In Chapter 5, we apply the results from Chapters 3 to fields with one of three different Galois groups. Chapter 6 provides several explicit examples of monogenic rings that are among the limited exceptions to the results from [BEG13].

CHAPTER 2

PRELIMINARIES

To prove our results, we will need to establish several preliminary concepts, lemmas, and theorems. We will begin with some basic facts about matrix actions on integral binary forms, and then proceed to a discussion of index form equations. We will conclude this chapter with a critical result on the Galois group of quartic polynomials.

2.1 Matrix Actions on Binary Forms

We briefly describe some basic facts about the action of $\mathrm{GL}_2(\mathbb{Z})$ on integral binary forms. The transpose of a matrix A will be denoted by A^{tr}. Let $F(T_1, T_2) \in \mathbb{Z}[T_1, T_2]$ be a binary form, and $A = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z})$. The action of $\mathrm{GL}_2(\mathbb{Z})$ is defined by

$$A \cdot F(T_1, T_2) = \frac{1}{\det(A)} F((T_1, T_2)A) \tag{2.1}$$

where $(T_1, T_2)A = (aT_1 + bT_2, cT_1 + dT_2)$.

Definition 2.1. We say that two binary forms $F, H \in \mathbb{Z}[T_1, T_2]$ are *G-equivalent*, where G is a subgroup of $\mathrm{GL}_2(\mathbb{Z})$, if there exists $A \in G$ such that $H = A \cdot F$.

We will typically work with the full group $\mathrm{GL}_2(\mathbb{Z})$ and may, for the purpose of readability, refer to forms F and H which are $\mathrm{GL}_2(\mathbb{Z})$-equivalent as *equivalent forms*. Notice that the action of $\mathrm{GL}_2(\mathbb{Z})$ on the space of binary forms is defined in terms of invertible linear transformations. Therefore, if $F(T_1, T_2)$ is an irreducible binary form and $A \in \mathrm{GL}_2(\mathbb{Z})$, the form $(A \cdot F)(T_1, T_2)$ will also be irreducible.

Finiteness Results for Equivalent Forms with a Given Discriminant

We address a finiteness result due to Birch and Merriman for equivalent forms with a given discriminant.

Definition 2.2. Let $f \in \mathbb{Z}[T]$, and $\deg(f) = n$, be such that f factors over $\mathbb{C}$ as $f(T) = \prod_{i=1}^{n}(T - \alpha_i)$. Then the *discriminant* of f is defined to be

$$\mathrm{Disc}(f) = \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)^2. \tag{2.2}$$

Definition 2.3. Let F be an integral binary form such that

$$F(T_1, T_2) = \prod_{i=1}^{n} (\beta_i T_1 - \alpha_i T_2),$$

where $F(\alpha_i, 1) = 0 = F(1, \beta_i)$ for all $1 \leq i \leq n = \deg(F)$. The *discriminant* of F is defined to be

$$\mathrm{Disc}(F) = \prod_{1 \leq i < j \leq n} (\alpha_i \beta_j - \alpha_j \beta_i)^2. \tag{2.3}$$

Definition 2.4. Let α be an algebraic integer. The *discriminant* of α is defined to be $\mathrm{Disc}(f_\alpha)$, where f_α is of the minimal polynomial of α.

If $F \in \mathbb{Z}[T_1, T_2]$ is a binary form then one can check by direct calculation that $\mathrm{Disc}(F) = \mathrm{Disc}(A \cdot F)$ for any $A \in \mathrm{GL}_2(\mathbb{Z})$, and $\mathrm{Disc}(F(T_1, T_2)) = \mathrm{Disc}(F(T_1, 1))$. In [BM72b] Birch and Merriman prove the following finiteness theorem for equivalent binary forms. Their result is proven for any number field K.

Theorem 2.5. *([BM72b] Theorem 2) Let K be a number field with ring of integers $\mathcal{O}_K$. Suppose that $n \geq 2$ is a natural number and $D_0 \in \mathcal{O}_K$. Then there are only finitely many $\mathrm{GL}_2(\mathcal{O}_K)$-orbit of binary forms $F \in \mathcal{O}_K[T_1, T_2]$ with $\deg(F) = n$ and $\mathrm{Disc}(F) = D_0$.*

Applying Theorem 2.5 to our setting tells us that there is a finite number of $\mathrm{GL}_2(\mathbb{Z})$ equivalence classes of binary forms for any given discriminant. The next Corollary of Theorem 2.5 from [BM72b] will prove very useful to our work.

Corollary 2.6. *([BM72b] Corollary of Theorem 2) Let $\overline{\mathbb{Q}}$ be an algebraic closure of $\mathbb{Q}$, and fix $D_0 \in \mathbb{Z}$. Up to translations of the type $\alpha \mapsto \alpha + m$ for $m \in \mathbb{Z}$ there are finitely many algebraic integers $\alpha \in \overline{\mathbb{Q}}$ satisfying*

$$\mathrm{Disc}(\alpha) = D$$

for any $D \in \mathbb{Z}$.

Restating Corollary 2.6 in the language we have introduced for studying monogenic orders we have the equivalent result.

Corollary 2.7. *For any fixed $D \in \mathbb{Z}$, there are finitely many $\mathbb{Z}$-equivalence classes of algebraic integers α such that*

$$\mathrm{Disc}(\alpha_1) = D.$$

for any $\alpha_1 \in \alpha + \mathbb{Z}$.

Note that the discriminants of α and $\alpha + \lambda$ are equal; this common fact is addressed briefly in Section 2.2. Corollary 2.7 will be a key part of the argument we use in Chapter 5 when studying monogenic orders by Galois group.

Equivalent Forms and Solutions to Unit Equations

We will see in Section 2.5 that the monogenizations of quartic orders are connected to solutions to unit equations

$$F(T_1, T_2) = \pm 1 \tag{2.4}$$

where F is a binary cubic or quartic form. Thue's Theorem, named after Thue, who proved it in 1909, tells us that (2.4) has finitely many integer solutions.

Theorem 2.8. *([Thu09] Let $F(T_1, T_2) \in \mathbb{Z}[T_1, T_2]$ be a homogeneous form of degree $n \geq 3$, and let m be a non-zero integer. Then the equations*

$$F(T_1, T_2) = m, \tag{2.5}$$

has finitely many solutions $(t_1, t_2) \in \mathbb{Z}^2$.

For cubic equations, Bennett gives results in [Ben01] which provide an upper bound on the number of solutions to $F(T_1, T_2) = \pm 1$ for different ranges of $\mathrm{Disc}(F)$. These bounds will make up the necessary part of the argument in Chapter 5 used to address orders in fields with Galois group D_4 or C_4.

Proposition 2.9. *(Theorem 2.1 of [Ben01]) Suppose that $F(T_1, T_2)$ is a reducible cubic form such that $F(T, 1)$ has at least two distinct roots over $\mathbb{C}$. Let N_F be the number of solutions to the equation $F(T_1, T_2) = \pm 1$. If $\mathrm{Disc}(F) > 0$, then $N_F \leq 4$. Further, if $N_F = 4$, then F is $\mathrm{GL}_2(\mathbb{Z})$-equivalent to*

$$T_1(T_1^2 - T_1T_2 - T_2^2),$$

with $\mathrm{Disc}(F) = 5$, and if $N_F = 3$ then F is $\mathrm{GL}_2(\mathbb{Z})$-equivalent to

$$T_1(T_1^2 - 2T_2^2)$$

with $\mathrm{Disc}(F) = 32$. If, $\mathrm{Disc}(F) \leq 0$, then $N_F \leq 2$ and $N_F = 2$ implies that F is $\mathrm{GL}_2(\mathbb{Z})$-equivalent to either

$$T_1(T_1^2 + nT_1T_2 + nT_2^2)$$

for $1 \leq n \leq 3$, *corresponding to* $\mathrm{Disc}(F) = -3, -16$ *or* -27, *respectively, or to*

$$T_1(T_1 + T_2)^2 \qquad \text{or} \qquad T_1(T_1 + 2T_2)^2$$

with $\mathrm{Disc}(F) = 0$.

There is a well-known connection between the $\mathrm{GL}_2(\mathbb{Z})$-orbit of a binary integral form $F(T_1, T_2)$ and the solutions to the Diophantine equation $F(T_1, T_2) = \pm 1$.

Lemma 2.10. *Let* F *be an integral binary form and suppose that* H *is a form in the* $\mathrm{GL}_2(\mathbb{Z})$*-orbit of* F. *Then there is a one-to-one correspondence between the solutions to* $F(T_1, T_2) = \pm 1$ *and the solutions to* $H(T_1, T_2) = \pm 1$.

Proof. Let $A \in \mathrm{GL}_2(\mathbb{Z})$ and let $H = A \cdot F$. Suppose that $(t_1, t_2) \in \mathbb{Z}^2$ is a solution to $H(T_1, T_2) = \pm 1$. Then

$$\pm 1 = H(t_1, t_2) = (A \cdot F)(t_1, t_2) = F((t_1, t_2)A),$$

So $(t_1, t_2)A$ is a solution to $F(T_1, T_2) = \pm 1$. Since $A \cdot F = H$, we see that $F = A^{-1} \cdot H$. Thus we have an invertible function defined by $(t_1, t_2) \mapsto (t_1, t_2)A^{-1}$, which sends solutions to $F(T_1, T_2)$ to solutions to $H(T_1, T_2)$. □

Definition 2.11. An integral binary form $F(T_1, T_2)$ is called *monic* if the polynomial $F(T, 1)$ is monic.

If $F(T_1, T_2)$ is monic, then we are guaranteed a solution to $F(T_1, T_2) = \pm 1$: the trivial solution $(t_1, t_2) = (\pm 1, 0)$. Now let F be a monic binary form of degree n. Suppose that $A \in \mathrm{GL}_2(\mathbb{Z})$ is such that $A \cdot F = H$ is monic. Then $H(1, 0) = \pm 1$. Note that $\det(A) = \pm 1$, so for simplicity we take $\det(A) = 1$. Let

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \tag{2.6}$$

then

$$\pm 1 = H(1, 0) = (A \cdot F)(1, 0) = F\big((1, 0)A\big) = F(a, b). \tag{2.7}$$

Thus, (a, b) is a solution to $F(T_1, T_2) = \pm 1$. In fact, if $(t_1, t_2) \in \mathbb{Z}^2$ is any solution to $F(T_1, T_2) = \pm 1$, we can find a monic form H in the $\mathrm{GL}_2(\mathbb{Z})$-orbit of F such that (t_1, t_2) corresponds to the trivial solution to $H(T_1, T_2) = \pm 1$, under the map from Lemma 2.10. We outline how to find such an H given a solution $(t_1, t_2) \in \mathbb{Z}^2$ to $F(T_1, T_2) = \pm 1$.

Let $(t_1, t_2) \in \mathbb{Z}^2$ be a solution to $F(T_1, T_2) = \pm 1$. Since

$$F(t_1, t_2) = t_1^n + \lambda_1 t_1^{n-1} t_2 + \cdots + \lambda_{n-1} t_1 t_2^{n-1} + \lambda_n t_2^n = \pm 1,$$

we see that $\gcd(t_1, t_2) = 1$. So, there exists $\nu, \mu \in \mathbb{Z}$ with $\mu t_1 - \nu t_2 = 1$. Pick any such ν and μ, and consider the matrix

$$A = \begin{pmatrix} t_1 & t_2 \\ \nu & \mu \end{pmatrix}. \tag{2.8}$$

Note that $A \in \mathrm{GL}_2(\mathbb{Z})$. Additionally, observe that

$$H(1,0) = (A \cdot F)(1,0) = F((1,0)A) = F(t_1, t_2) = \pm 1. \tag{2.9}$$

The relationship expressed in (2.9) demonstrates what we mean when we say that the trivial solution to H corresponds to the solution (t_1, t_2) to $F(T_1, T_2) = \pm 1$. We have thus established the following lemma.

Lemma 2.12. *Let F be a monic integral binary form. Then for each solution $(t_1, t_2) \in \mathbb{Z}^2$ to $F(T_1, T_2) = \pm 1$ there exists a monic form H in the $\mathrm{GL}_2(\mathbb{Z})$-orbit of F, and $A \in \mathrm{GL}_2(\mathbb{Z})$ satisfying*

$$(1,0)A = (t_1, t_2)$$

and

$$A \cdot F = H.$$

When finding the matrix for (2.8), we picked solutions to

$$t_1 X + t_2 Y = 1. \tag{2.10}$$

Since $\gcd(t_1, t_2) = 1$, it is well known that the solutions (2.10) are all pairs $(\nu + \lambda t_2, \mu - \lambda t_1)$, for $\lambda \in \mathbb{Z}$ and $(\nu, \mu) \in \mathbb{Z}^2$ a given solution to (2.10). Thus for all values $\lambda \in \mathbb{Z}$, and F a monic form, the form

$$\begin{pmatrix} t_1 & t_2 \\ (\mu - \lambda t_1) & \nu + \lambda t_2 \end{pmatrix} \cdot F = F_\lambda, \tag{2.11}$$

has $F_\lambda(1,0) = F(t_1, t_2) = 1$.

Given a form F, a solution $(t_1, t_2) \in \mathbb{Z}^2$, and $A \in \mathrm{GL}_2(\mathbb{Z})$ a matrix with $(A \cdot F)(1,0) = F(t_1, t_2)$, then every other matrix A_λ with $(A_\lambda \cdot F)(1,0) = F(t_1, t_2)$ can be written in the form

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^{\lambda} A = A_\lambda.$$

We can also use the action of $\mathrm{GL}_2(\mathbb{Z})$ to move between the minimal forms of monogenizers that define the same monogenization. Importantly, for any monic binary form F, we see that

$$\left(\begin{pmatrix} 1 & 0 \\ \lambda & 1 \end{pmatrix} \cdot F \right)(T_1, T_2) = F(T_1 + \lambda T_2, T_2).$$

So the action of a matrix $\begin{pmatrix} 1 & 0 \\ \lambda & 1 \end{pmatrix}$ does not change the value of F at $(1,0)$. Now, let $\mathcal{O}$ be an order of rank n, with monogenizers ξ_1 and ξ_2. If $\xi_2 = \xi_1 + \lambda$, and $F_1, F_2 \in \mathbb{Z}[T_1, T_2]$ are the minimal forms of ξ_1 and ξ_2, respectively, then

$$\begin{aligned} F_2(T_1, T_2) &= \prod_{i=1}^{n} \left(T_1 - (\xi_{(i)} + \lambda)T_2\right) = \prod_{i=1}^{n} (T_1 - \lambda T_2 + \xi_{(i)} T_2) \\ &= F_1(T_1 - \lambda T_2, T_2) = \begin{pmatrix} 1 & 0 \\ -\lambda & 1 \end{pmatrix} \cdot F_1, \end{aligned} \tag{2.12}$$

where $\xi_{(1)}, ..., \xi_{(n)}$ are the algebraic conjugates of ξ. We record this observation as a lemma for future reference.

Lemma 2.13. *Let ξ_1 and ξ_2 be monogenizers in a monogenic order $\mathcal{O}$, and let F_1 and F_2 the minimal forms of ξ_1 and ξ_2 respectively. If $\xi_1 + \mathbb{Z} = \xi_2 + \mathbb{Z}$, then there exists $\lambda \in \mathbb{Z}$ such that*

$$F_2(T_1, T_2) = \begin{pmatrix} 1 & 0 \\ -\lambda & 1 \end{pmatrix} \cdot F_1.$$

2.2 Index Form Equations

We are interested in the orders $\mathbb{Z}[\xi]$ that are two times monogenic. Let β be an algebraic integer in $\mathbb{Z}[\xi] \subseteq \mathcal{O}_K$ for $K = \mathbb{Q}(\xi)$. We wish to study when β is a monogenizer of $\mathbb{Z}[\xi]$, that is, $\mathbb{Z}[\beta] = \mathbb{Z}[\xi]$ as rings. For an order L of $\mathcal{O}_K$ let L^+ refer to L as a $\mathbb{Z}$-module. Since $\mathbb{Z}[\xi]$ is an order, the index $[\mathbb{Z}[\xi]^+ : \mathcal{O}_K^+]$ is finite. For a primitive element $\alpha \in K$ we write $I(\alpha) = [\mathbb{Z}[\alpha]^+ : \mathcal{O}_K^+]$. If $\beta \in \mathbb{Z}[\xi]$, then $\mathbb{Z}[\beta]^+$ is a

submodule of $\mathbb{Z}[\xi]^+$, so $I(\xi)$ divides $I(\beta)$. Thus, $\beta \in \mathbb{Z}[\xi]$ is a monogenizer of $\mathbb{Z}[\xi]$ if and only if $I(\beta) = I(\xi)$.

The statement $I(\beta) = m$, for $m \in \mathbb{Z}$, can be made into a Diophantine equation. Let K be a number field of degree n, and $\{1 = \omega_1, \omega_2, ..., \omega_n\}$ be an integral basis for K. We introduce the notation $\mathbf{X} = (X_1, ..., X_n)$, where the X_i's are formal indeterminates. In this section we will develop a form $\mathcal{I}(\mathbf{X})$ over $\mathbb{Z}$ such that if $(x_1, ..., x_n) \in \mathbb{Z}^n$ is a solution to the Diophantine equation

$$\mathcal{I}(X_1, ..., X_n) = m, \tag{2.13}$$

for any rational integer $m > 0$, then the algebraic number

$$\alpha = x_1 + x_2\omega_2 + \cdots + x_n\omega_n$$

will satisfy $I(\alpha) = m$. Such a form $\mathcal{I}$ is called a *index form* of K. We turn now to the construction of the form $\mathcal{I}$ for any given basis of K.
Let $\alpha_1, ..., \alpha_n$ be a linearly independent set of n elements in a number field K. Also, let $\varphi_1, ..., \varphi_n : k \to \mathbb{C}$ be the embeddings of K into $\mathbb{C}$.

Definition 2.14. The *discriminant* of $(\alpha_1, ..., \alpha_n)$ is defined as the square of the determinant of the $n \times n$ matrix

$$D_{k/\mathbb{Q}}(\alpha_1, ..., \alpha_n) = (\det(\varphi_i(\alpha_j))^2,$$

where $i, j \in \{1, ..., n\}$.

If $\{\beta_1, ..., \beta_n\}$ and $\{\omega_1, ..., \omega_n\}$ are integral bases for $\mathcal{O}_K$ then

$$D_{K/\mathbb{Q}}(\beta_1, ..., \beta_n) = D_{K/\mathbb{Q}}(\omega_1, ..., \omega_n),$$

see [Mil20] Lemma 2.23. So, for any integral basis $\{\beta_1, ..., \beta_n\}$ of K the discriminant of the field L is defined to be

$$D_K = D_{K/\mathbb{Q}}(\beta_1, ..., \beta_n).$$

For an order $\mathcal{O}$ of K, and $\{\gamma_1, ..., \gamma_n\}$ a $\mathbb{Z}$-basis for $\mathcal{O}$, we define the discriminant of $\mathcal{O}$ to be $D_{k/\mathbb{Q}}(\gamma_1, ..., \gamma_n)$. If $\alpha \in k$ is primitive then the set $\{1, \alpha, \alpha^2, ..., \alpha^{n-1}\}$ is $\mathbb{Q}$-linearly independent. We define the discriminant of α to be

$$D(\alpha) = D_{K/\mathbb{Q}}(1, \alpha, \alpha^2, ..., \alpha^{n-1}).$$

Using the Vandermonde determinant, it can be shown that,

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

The following lemma is a well-known but beneficial result. The version presented here is Lemma 1.3 of Chapter 1 in [Gaá19].

Lemma 2.15. *Let $\alpha_1, ..., \alpha_n \in \mathcal{O}_K$ be linearly independent over $\mathbb{Q}$ and set*

$$\mathcal{O} = \mathbb{Z}[\alpha_1, ..., \alpha_n].$$

Then

$$D_{k/\mathbb{Q}}(\alpha_1, ..., \alpha_n) = J^2 D_K, \tag{2.14}$$

where $J = [\mathcal{O}_K^+ : \mathcal{O}^+]$, the module index.

let

$$L(\mathbf{X}) = X_1 + \omega_2 X_2 + \cdots + \omega_n X_n, \tag{2.15}$$

with algebraic conjugates

$$L_{(i)}(\mathbf{X}) = X_1 + (\omega_2)_{(i)} X_2 + \cdots + (\omega_n)_{(i)} X_n,$$

for $(1 \le i \le n)$.

Definition 2.16. The form

$$D_{K/\mathbb{Q}}(L(\mathbf{X})) = \prod_{1 \le i < j \le n} (L_{(i)}(\mathbf{X}) - L_{(j)}(\mathbf{X}))^2 \tag{2.16}$$

is the *discriminant form* of K with respect to $\mathbb{Q}$.

Notice that in equation (2.16) for every pair (i, j) the X_1 terms in $\big(L_{(i)}(\mathbf{X}) - L_{(j)}(\mathbf{X})\big)$ cancel, thus the discriminant form of K is independent of X_1. Suppose that $\alpha \in \mathcal{O}_K$, and $\alpha = \sum_{i=1}^n x_i \omega_i$. Let $\mathbf{x} = (x_1, ..., x_n)$. Consider

$$\begin{aligned} D_{k/\mathbb{Q}}\left(L(\mathbf{x})\right) &= \prod_{1 \le i < j \le n} (L_{(i)}(\mathbf{x}) - L_{(j)}(\mathbf{x}))^2 \\ &= \prod_{1 \le i < j \le n} \left(\sum_{k=1}^n x_k (\omega_k)_{(i)} - \sum_{k=1}^n x_k (\omega_k)_{(j)} \right)^2 \\ &= \prod_{1 \le i < j \le n} \left(\alpha_{(i)} - \alpha_{(j)}\right)^2. \end{aligned}$$

So $D_{K/\mathbb{Q}}(L(\mathbf{x})) = D_{K/\mathbb{Q}}(\alpha)$. Now for $\alpha \in K$ primitive the set $\{1, \alpha, \alpha^2, ..., \alpha^{n-1}\}$ is linearly independent over $\mathbb{Q}$. So by Lemma 2.15 we see

$$D_{K/\mathbb{Q}}(L(\mathbf{x})) = D_{K/\mathbb{Q}}(\alpha) = [Z[\alpha]^+ : \mathcal{O}_K^+]D_K. \tag{2.17}$$

Repeating the calculation in equation (2.17) with the indeterminates $X_1, X_2, ..., X_n$ allows us to construct the index form for the basis $B = \{1 = \omega_1, \omega_2, ..., \omega_n\}$.

Lemma 2.17. *(Chapter 1 Lemma 1.4 of [Gaá19]) We have*

$$D_{k/\mathbb{Q}}(L(\mathbf{X})) = (\mathcal{I}(X_2, ..., X_n))^2 D_K, \tag{2.18}$$

where D_K is the discriminant of the field of K and the linear form $L(\mathbf{X})$ and its discriminant are defined in (2.15) *and* (2.16)*. The polynomial $\mathcal{I}(X_2, ..., X_n)$ is a homogeneous form in $n-1$ variables of degree $\frac{n(n-1)}{2}$ with integer coefficients.*

The form $\mathcal{I}(X_2, ..., X_n)$ defined in (2.18) is a *index form* for the field K. Note that for an algebraic integer

$$\alpha = x_1 + x_2\omega_2 + \cdots + x_n\omega_n$$

with $K = \mathbb{Q}(\alpha)$, we have by Lemma 2.17

$$I(\alpha) = |\mathcal{I}(x_2, ..., x_n)|. \tag{2.19}$$

Thus, the index form is independent of the value of x_1, which agrees with $I(\alpha) = I(\alpha + \lambda)$ for all $\lambda \in \mathbb{Z}$.

When applying the index form to monogenic orders, we will need to use a power basis $\{1, \alpha, \alpha^2, ..., \alpha^{n-1}\}$, for the field $K = \mathbb{Q}(\alpha)$. If $I_0 = I(\alpha)$ and $\beta \in \mathcal{O}_K$ then we can represent β as

$$\beta = \frac{1}{I_0}\sum_{i=0}^{n-1} x_i\alpha^i, \tag{2.20}$$

for $x_i \in \mathbb{Z}$. Now constructing an index form with the basis $\{1, \alpha, \alpha^2, ..., \alpha^{n-1}\}$ we will get a form $\mathcal{I}(X)$, such that

$$\mathcal{I}(x_0, x_1, ..., x_{n-1}) = \pm I_0^{\frac{n(n-1)}{2}} I(\beta)$$

where the ± 1 is to adjust for the possibility of the discriminant of K being a negative number. This adjustment lets us define an index form of K for any primitive element.

2.3 Cubic Resolvent Rings of Quartic Rings

Here, we provide a formal definition for the cubic resolvent ring of a quartic ring. At the end of this section, we give a vital theorem of Bhargava, which provides an elementary model of the cubic resolvent ring for a monogenic quartic order.

Formal Construction of Cubic Resolvent Rings

Let Q be a quartic ring. We present the definition of a cubic resolvent ring of Q as Bhargava developed in [Bha04], Definition 8, and also appearing in [Woo12] Section 8.

Definition 2.18. The S_4-*closure* of Q, denoted by $\overline{Q}$ is the ring $Q^{\otimes 4}/J_Q$, where J_Q is the $\mathbb{Z}$-saturation of the ideal I_Q generated by all elements of the form

$$x \otimes 1 \otimes 1 \otimes 1 + 1 \otimes x \otimes 1 \otimes 1 + 1 \otimes 1 \otimes x \otimes 1 + 1 \otimes 1 \otimes 1 \otimes x$$

for $x \in Q$ (that is $J_Q = \{r \in Q^{\otimes 4} : nr \in I_Q \text{ for some } n \in Z\}$.

In this setting the elements $1 \otimes x \otimes 1 \otimes 1$, $1 \otimes 1 \otimes x \otimes 1$, $1 \otimes 1 \otimes 1 \otimes x$ act as formal conjugates of $x \otimes 1 \otimes 1 \otimes 1$.

Definition 2.19. The *cubic invariant ring* of Q is the ring

$$R^{\text{inv}}(Q) = Z[\{x \otimes x \otimes 1 \otimes 1 + 1 \otimes 1 \otimes x \otimes x : x \in Q\} \subseteq \overline{Q}.$$

Every element of $R^{\text{inv}}(Q)$ is fixed by $D_4 \subseteq S_4$, thus $R^{\text{inv}}(Q)$ is a cubic ring. We can also think of the ring $R^{\text{inv}}(Q)$ as being the ring generated by the image of the map

$$\Phi(x) = x \otimes x \otimes 1 \otimes 1 + 1 \otimes 1 \otimes x \otimes x = x_{(1)}x_{(2)} + x_{(3)}x_{(4)}$$

where $x_{(i)}$ are the formal S_4 conjugates of x.

Definition 2.20. For a quartic ring Q the *cubic resolvent map* is the quadratic function $\Phi(x) = x_{(1)}x_{(2)} + x_{(3)}x_{(4)}$.

Now we can define a cubic resolvent ring of a quartic ring.

Definition 2.21. ([Bha04], Definition 8) C is a *cubic resolvent ring* of a quartic ring Q if $R^{\text{inv}}(Q) \subseteq C$ and $\text{Disc}(Q) = \text{Disc}(C)$.

As the definition indicates, a quartic ring can generally have more than one cubic resolvent ring.

Invariant Rings of Binary Forms

Let $F(T_1, T_2) = \sum_{i=0}^{n} c_i T_1^{n-i} T_2^i \in \mathbb{Z}[T_1, T_2]$ be an integral binary form. We define the invariant ring of F, R_F, to be the subring of $\mathbb{Q}[t]/(F(t,1))$, with $\mathbb{Z}$-module bases

$$\begin{aligned} w_0 &= 1 \\ w_1 &= c_0 t \\ w_2 &= c_0 t^2 + c_1 t \\ &\vdots \\ w_k &= c_0 t^k + \cdots + c_{k-1} t \\ &\vdots \\ w_{n-1} &= c_0 t^{n-1} + \cdots + c_{n-2} t. \end{aligned} \tag{2.21}$$

Birch and Merriman first introduced such rings in [BM72a].

If F is monic we can define a map on R_f given by $w_i \mapsto w_i$ for $i = 0, 1$ and

$$w_j \mapsto w_j - (c_1 w_{j-1} + c_2 w_{j-2} + \cdots + c_{j-1} w_1),$$

for $1 < i \leq n-1$. Let A be the matrix defining the map described above. Then A is an upper triangular matrix whose diagonal is only 1's. Thus $\det_{\mathbb{Z}}(A) = 1$, so A is invertible and defines a change of basis on R_F. So, we have proved the following result.

Lemma 2.22. *Let $f \in \mathbb{Z}[T]$ be monic and degree n, and let $H = T_2^n f(T_1/T_2)$. Then the invariant order $\mathcal{O}_H$ is isomorphic to $Z[T]/(f(T))$. Moreover, the order $\mathcal{O}_H$ is monogenic, and has power basis $\{1, T, T^2, ..., T^{\deg(H)-1}\}$.*

Lemma 2.22 tells us that the ring $\mathcal{O}_H$ is monogenic even if f is reducible. Most significant for defining cubic resolvent rings are the invariant orders of binary cubic forms. Let $F(T_1, T_2) = aT_1^3 + bT_1^2 T_2 + cT_1 T_2^2 + dT_2^3$, with $a, b, c, d \in \mathbb{Z}$. Let $\omega = -w_1$ and $\theta = -w_2 - c$, from (2.21). Then the multiplication table for R_F is as follows:

$$\begin{aligned} \omega\theta &= -ad \\ \omega^2 &= -ac + b\omega - a\theta \\ \theta^2 &= -bd + d\omega - c\theta. \end{aligned} \tag{2.22}$$

Definition 2.23. Let $\{1, \omega, \theta\}$ be a basis for a cubic ring. We say that the basis is *normal* if $\omega\theta \in \mathbb{Z}$.

The basis given in the multiplication table (2.22) is a normal basis. For a cubic ring R with basis $\{1, \omega, \theta\}$ we may always translate ω and θ by elements of $\mathbb{Z}$ to get a normal basis. Thus, we may freely assume that R has a normal basis, and for any basis of the $\mathbb{Z}$-module $R/\mathbb{Z}$, there exists a lift to a normal basis of R. This lets us define an action of $\mathrm{GL}_2(\mathbb{Z})$ on the set of cubic invariant rings by $A \circ R$ to be the ring with normal basis $\{1, \theta', \omega'\}$ that is a lift of the basis $\{(A\omega + \mathbb{Z}), (A\theta + \mathbb{Z})\}$ for the $\mathbb{Z}$-module $R/\mathbb{Z}$. One can show that if $R = \mathcal{O}_F$ for a binary cubic form F, then $A \circ R = \mathcal{O}_{A \cdot F}$ as rings.

This result was first presented by Dalone and Faddeev [DF64] but has been studied in a different form by many others. The version presented here most closely follows the work of Bhargava in [Bha22] Section 2.3. To summarize, we have the following theorem.

Theorem 2.24. *(Theorem 2.2 of [Bha22]) There is a bijection between the* $\mathrm{GL}_2(\mathbb{Z})$*-classes of integral binary cubic forms and the isomorphism classes of cubic rings.*

Using Theorem 2.24, Lemma 2.22, and Lemma 2.12, we can characterize the monogenizations of any cubic invariant ring.

Theorem 2.25. *([Bha22] Theorem 2.3) Let $F \in \mathbb{Z}[T_1, T_2]$ be a monic binary cubic form. Then the monogenizations of $\mathcal{O}_F$ are in one-to-one correspondence with the primitive solutions to $F(T_1, T_2) = \pm 1$.*

In [Bha22], Bhargava then goes on to prove an upper bound on the number of monogenizations of a cubic order using a result on the upper bound of the number of solutions to $F(T_1, T_2) = \pm 1$ for any cubic binary form F.

An Elementary Model for Cubic Resolvent Rings

For monogenic quartic orders, a more elementary construction of cubic resolvent rings is available. Let ξ be a quartic algebraic integer with minimal polynomial

$$f_\xi(T) = T^4 + a_1T^3 + a_2T^2 + a_3T + a_4 \tag{2.23}$$

and $K = \mathbb{Q}(\xi)$. Fix an algebraic closure $\overline{\mathbb{Q}} \subseteq \mathbb{C}$ of $\mathbb{Q}$, and denote the conjugates of ξ by $\xi = \xi_{(1)}, \xi_{(2)}, \xi_{(3)}, \xi_{(4)} \in \overline{\mathbb{Q}}$.

Definition 2.26. The *cubic resolvent polynomial* of f_ξ is the polynomial

$$\begin{aligned} r_\xi(T) &= \left(T - (\xi_{(1)}\xi_{(2)} + \xi_{(3)}\xi_{(4)})\right)\left(T - (\xi_{(1)}\xi_{(3)} + \xi_{(2)}\xi_{(4)})\right)\left(T - (\xi_{(1)}\xi_{(4)} + \xi_{(2)}\xi_{(3)})\right) \\ &= T^3 - a_2T^2 + (a_1a_3 - 4a_4)T - (a_3^2 + a_1^2a_4). \end{aligned}$$

We will frequently need to homogenize the polynomial r_ξ. For this reason, we provide the following definition.

Definition 2.27. The *cubic resolvent form* of ξ, is the binary form $T_2^3 r_\xi(T_1/T_2)$, where $r_\xi(T)$ is the cubic resolvent polynomial of ξ defined in 2.26

We will refer to the roots of r_ξ as follows:

$$\begin{aligned} \rho_1 &= \xi_{(1)}\xi_{(2)} + \xi_{(3)}\xi_{(4)}, \\ \rho_2 &= \xi_{(1)}\xi_{(3)} + \xi_{(2)}\xi_{(4)}, \\ \rho_3 &= \xi_{(1)}\xi_{(4)} + \xi_{(2)}\xi_{(3)}. \end{aligned} \tag{2.24}$$

The following theorem gives an explicit construction of cubic resolvent rings, which we will primarily use throughout our work.

Theorem 2.28. *(Theorem 3.3 of [Bha22]) Every quartic ring has at least one cubic resolvent ring. In particular, every monogenic quartic ring $Q = \mathbb{Z}[T]/(T^4 + a_1T^3 + a_2T^2 + a_3T + a_4)$ has a unique cubic resolvent ring R, and it is given by*

$$R = \mathbb{Z}[T]/\left(T^3 - a_2T^2 + (a_1a_3 - 4a_4)T - (a_3^2 + a_1^2a_4)\right).$$

Notice that

$$\begin{aligned} \mathrm{Disc}(f_\xi) &= (\xi_{(1)} - \xi_{(2)})^2(\xi_{(1)} - \xi_{(3)})^2(\xi_{(1)} - \xi_{(4)})^2(\xi_{(2)} - \xi_{(3)})^2(\xi_{(2)} - \xi_{(4)})^2(\xi_{(3)} - \xi_{(4)})^2 \\ &= \left((\xi_{(1)} - \xi_{(2)})(\xi_{(3)} - \xi_{(4)})\right)^2\left((\xi_{(1)} - \xi_{(3)})(\xi_{(2)} - \xi_{(4)})\right)^2\left((\xi_{(1)} - \xi_{(4)})(\xi_{(2)} - \xi_{(3)})\right)^2 \\ &= (\rho_1 - \rho_2)^2(\rho_1 - \rho_3)^2(\rho_2 - \rho_3)^2 = \mathrm{Disc}(r_\xi). \end{aligned}$$

Thus, we see that the discriminant of $\mathbb{Z}[\xi]$ is the same as that of the cubic resolvent ring R.

Even for a monic irreducible quartic polynomial f, the cubic resolvent polynomial r may be reducible. Specifically, if the Galois group of f is V_4, C_4, or D_4, r will be reducible. In this setting, we can still define the map Φ; however, if r_ξ is reducible, then the cubic resolvent ring will not be a domain and therefore will not be a subring of the algebraic closure $\overline{\mathbb{Q}}$. For this reason, we take the codomain of Φ

to be $\mathbb{C}$, and we slightly modify the definition of the cubic resolvent map given by Bhargava. In Chapter 5, we will make use of the reducibility of r_ξ to study the type of specific orders. If r_ξ is irreducible, then the image of Φ is in the cubic resolvent ring R_ξ.

Definition 2.29. The *cubic resolvent map* $\Phi : Q \to \mathbb{C}$ of the quartic ring Q is defined by $\Phi(x) = x_{(1)}x_{(2)}+x_{(3)}x_{(4)}$, where $x_{(i)}$, $1 \leq i \leq 4$ are the algebraic conjuncts of i.

In [Bha04], the map Φ for a quartic ring Q is defined in terms of the S_4 conjugates in the S_4 closure of Q, see Definition **??**. For our purpose, the Galois conjugates will play a central role, making the version of the cubic resolvent map given in definition 2.29 a reasonable modification of Bhargava's original constructions.

Notice that if ξ is a monogenizer of $\mathcal{O}$ then $\Phi(\xi) = \rho_1$. In the case that r_ξ is irreducible, and $\Phi(\xi) = \rho_1$ is a root of r_ξ. So by Theorem 2.28, and the first Isomorphism theorem, the ring $\mathbb{Z}[\Phi(\xi)]$ is isomorphic to the cubic resolvent ring of $\mathbb{Z}[\xi]$, when r_ξ is irreducible. We demonstrate the reducibility of r_ξ in some cases and address its implications for the monogenizations of quartic rings in Chapter 5. Because the cubic resolvent polynomial r can be reducible, it is helpful to consider the cubic resolvent ring of the quartic order $Z[T]/(f)$ to be the cubic invariant ring of the binary cubic form $T_2^3 r_\xi(T_1/T_2)$. Lastly, we note that for a quartic polynomial $f \in \mathbb{Z}[T]$ whose Galois group is S_4 or A_4, the cubic resolvent polynomial r is irreducible. In this case, the ring $\mathbb{Z}[T]/(r)$ will be a cubic order.

2.4 Cubic Index Form Equations and Monogenic Cubic Orders

If the Galois group of a quartic order is S_4 or A_4, then by Theorem 2.28, the cubic resolvent ring of a quartic order will be a cubic order. In Section 2.5, we will see that there is a connection between the monogenizations of a quartic order $\mathbb{Q}$ and its cubic resolvent. For that reason, we briefly discuss some facts about cubic rings.

Let γ be a cubic algebraic integer with minimal polynomial

$$f_\gamma(x) = T^3 + c_1T^2 + c_2T + c_3, \tag{2.25}$$

and consider the cubic field $K = \mathbb{Q}(\gamma)$. Also, let $H_\gamma(T_1, T_2)$ be the minimal form of γ. Because our ultimate goal is to study monogenic orders, we take $\{1, \gamma, \gamma^2\}$ as our

$\mathbb{Q}$-basis for K. Now for any algebraic integer $\beta \in \mathcal{O}_K$ we have

$$\beta = \frac{a + x\gamma + y\gamma^2}{I}$$

with $a, x, y \in \mathbb{Z}$ and $I \in \mathbb{Z}$ the index of γ in $\mathcal{O}_K$.

In [Gaá19], Gaál provides the following result.

Lemma 2.30. *(Theorem 8.1 of [Gaá19]) Let γ be a cubic algebraic integer, and $K = \mathbb{Q}(\gamma)$. If $\beta \in \mathcal{O}_K$ and*

$$\beta = \frac{a + x\gamma + y\gamma^2}{I},$$

where $a, x, y \in \mathbb{Z}$ and $I \in \mathbb{Z}> 0$ is the index of γ in $\mathcal{O}_K$. Then $I(\beta) = m$ if and only if

$$x^3 - 2a_1x^2y + (a_1^2 + a_2)xy^2 - (a_1a_2 - a_3)y^3 = \pm I^2 m \tag{2.26}$$

Proof. Let $\beta' = I\beta = a + x\gamma + y\gamma^2$. We denote the algebraic conjugates of β' and γ by $\beta'_{(j)}$, $\gamma_{(j)}$ for $j \in \{1, 2, 3\}$. Note that

$$\frac{I(\beta')}{I(\gamma)} = \frac{I(\gamma)^3 m}{I(\gamma)},$$

or equivalently

$$\prod_{1 \le i < j \le 3} \frac{\beta'_i - \beta'_j}{\gamma_i - \gamma_j} = \frac{d^3 m}{I(\xi)}.$$

Now for any $1 \le i < j \le 3$ we have

$$\begin{aligned}\frac{\beta'_i - \beta'_j}{\gamma_i - \gamma_j} &= \frac{x(\gamma_i - \gamma_j) + y(\gamma_i^2 - \gamma_j^2)}{\gamma_i - \gamma_j} \\ &= x + y(\gamma_i + \gamma_j) = x + y(-c_1 - \gamma_k),\end{aligned}$$

where $(i, j) = (1, 2), (1, 3), (2, 3)$ and $k = 3, 2, 1$ respectively. Hence the product for $1 \le i < j \le 3$ is just the norm of $x + y(-c_1 - \gamma)$. Using symmetric polynomials, one finds

$$N_{K/\mathbb{Q}}(x + y(-c_1 - \gamma)) = x^3 - 2c_1x^2y + (c_1^2 + a_2)xy^2 - (c_1c_2 - c_3)y^3.$$

□

We are interested in the case of $\beta \in \mathbb{Z}[\xi]$ with $\mathbb{Z}[\beta] = \mathbb{Z}[\xi]$. For this case, we have

$$I(\beta) = I(\gamma), \text{ and } \beta = a + x\gamma + y\gamma^2. \tag{2.27}$$

Once we specialize Lemma 2.30 to the case of $\beta \in \mathbb{Z}[\gamma]$ with $I(\beta) = I(\gamma)$ we get:

Lemma 2.31. *Let $f_\gamma(T) = T^3 + c_1T^2 + c_2T + c_3$ be the minimal polynomial of a algebraic integer γ. Suppose that $\beta = c + t_1\gamma + t_2\gamma^2 \in \mathbb{Z}[\gamma]$, then $\mathbb{Z}[\beta] = \mathbb{Z}[\gamma]$ if and only if (t_1, t_2) satisfy the equation*

$$T_1^3 - 2c_1T_1^2T_2 + (c_1^2 + c_2)T_1T_2^2 - (c_1c_2 - c_3)T_2^3 = \pm 1. \tag{2.28}$$

Proof. Suppose that $\beta \in \mathbb{Z}[\gamma]$, then $\mathbb{Z}[\beta] = \mathbb{Z}[\gamma]$ if and only if $I(\beta) = I(\gamma)$. Let $f_\gamma(T) = T^3 + c_1T^2 + c_2T + c_3$ be the minimal polynomial of γ. Since $\{1, \gamma, \gamma^2\}$ is a basis for $\mathbb{Z}[\gamma]$, there exist $a, t_1, t_2 \in \mathbb{Z}$ such that

$$\beta = a + t_1\gamma + t_2\gamma^2.$$

From the properties of the index, we see that $I(\beta) = I(\beta - a) = I(x\gamma + y\gamma^2)$. Thus,

$$I(\beta) = I(t_1\gamma + t_2\gamma^2) = I(\gamma). \tag{2.29}$$

Since $I(\beta) = I(\gamma)$, we can divide all sides of the above equations by $I(\gamma)$. The results of dividing by $I(\gamma)$ is the following equation

$$1 = \prod_{1 \le i < j \le 3} \frac{\beta_{(i)} - \beta_{(j)}}{\gamma_{(i)} - \gamma_{(j)}}, \tag{2.30}$$

where $\beta_{(i)}$ and $\gamma_{(i)}$ for $1 \le i \le 3$ are the algebraic conjugates of β and γ respectively. By the same reasoning as in Lemma 2.30, we recognize the product in (2.30) as the field norm $N_{\mathbb{Q}(\gamma)/\mathbb{Q}}(t_1 + t_2(-c_1 - \gamma)$. Thus $(t_1, t_2) \in \mathbb{Z}^2$ solves the equation

$$T_1^3 - 2c_1T_1^2T_2 + (c_1^2 + c_2)T_1T_2^2 - (c_1c_2 - c_3)T_2^3 = \pm 1. \tag{2.31}$$

Therefore, $\beta \in \mathbb{Z}[\gamma]$, then $\mathbb{Z}[\beta] = \mathbb{Z}[\gamma]$ if and only if there exists $(x, y) \in \mathbb{Z}^2$ solving the equation

$$T_1^3 - 2c_1T_1^2T_2 + (c_1^2 + c_2)T_1T_2^2 - (c_1c_2 - c_3)T_2^3 = \pm 1.$$

□

The algebraic numbers β and $\beta + a$ will have the same index and define the same monogenization of $\mathbb{Z}[\gamma]$. Let

$$C(T_1, T_2) = T_1^3 - 2c_1T_1^2T_2 + (c_1^2 + c_2)T_1T_2^2 - (c_1c_2 - c_3)T_2^3. \tag{2.32}$$

Thus, the monogenizations of $\mathbb{Z}[\gamma]$ are all of the form $(t_1\gamma + t_2\gamma^2) + \mathbb{Z}$ where $(t_1, t_2) \in \mathbb{Z}^2$ satisfy $C(t_1, t_2) = \pm 1$. We will use these lemmas in Section 3.3 to provide a proof that all cubic orders are of type I.

2.5 Quartic Index Form Equations

This section will study the index form equations for quartic number fields. The result will be a reduction of the equation $\mathcal{I}(X, Y, Z) = m$ to solving a system of three lower-degree polynomials. The reduction as well as an algorithm for reducing quartic index form equations is due to Gaál, Pethő, and Pohst in [GPP93], and [GPP96], and can also be found in [Gaá19] Section 9.1 or section 3 of [Akh22]. An explicit version of the algorithm is given in Appendix A.1.

Let ξ be a quartic algebraic integer with minimal polynomial

$$f_\xi(T) = T^4 + a_1T^3 + a_2T^2 + a_3T + a_4 \tag{2.33}$$

and $I(\xi) = I_0$. Denote the conjugates of ξ by $\xi = \xi_{(1)}, \xi_{(2)}, \xi_{(3)}, \xi_{(4)}$ and $\mathbb{Q}(\xi) = K$. Suppose that $B = \{1 = \omega_0, \omega_1, \omega_2, \omega_3\}$ is an integral basis for K. Note that $\xi = c_\xi + x_\xi\omega_1 + y_\xi\omega_2 + z_\xi\omega_3$, for some $c_\xi, x_\xi, y_\xi, z_\xi \in \mathbb{Z}$, and

$$\mathcal{I}(x_\xi, y_\xi, z_\xi) = \pm I_0.$$

Pick any primitive $\beta \in \mathcal{O}_K$ such that $I(\beta) = m$. There exists $c_0, x_0, y_0, z_0 \in \mathbb{Z}^3$ such that

$$\beta = c + x_0\omega_1 + y_0\omega_2 + z_0\omega_3. \tag{2.34}$$

Note that β and $\beta - c$ will have the same index and generate the same $\mathbb{Z}$-algebra in $\mathcal{O}_K$. So we may take $c = 0$. Notice (x_0, y_0, z_0) satisfy $\mathcal{I}(X, Y, Z) = \pm m$, where $\mathcal{I}$ is the index from of K for the basis $\{1, \omega_1, \omega_2, \omega_3\}$. Since I_0 is the index of ξ in $\mathcal{O}_K$ we see that

$$I_0\beta \in \mathbb{Z}[\xi].$$

Let $\beta' = I_0\beta$ then

$$I_0\beta = \beta' = c_1 + x_1\xi + y_1\xi^2 + z_1\xi^3 \in \mathbb{Z}[\xi]. \tag{2.35}$$

So,

$$I(\beta') = I(x_1\xi + y_1\xi^2 + z_1\xi^3) = \pm I_0^6 m. \tag{2.36}$$

Recall from Lemma 2.18 that for $(x\omega_1 + y\omega_2 + z\omega_3) \in \mathcal{O}_K$,

$$I(x_1\xi + y_1\xi^2 + z_1\xi^3) = \mathcal{I}(x, y, z),$$

and

$$D_{K/\mathbb{Q}}(L(x, y, z)) = \mathcal{I}(x, y, z)^2 D_K. \tag{2.37}$$

Upon dividing both sides of equation (2.36) by $\mathcal{I}(x_\xi, y_\xi, z_\xi) = I_0$, we get

$$\prod_{(i,j,k,l)} \left(\frac{\beta'_{(i)} - \beta'_{(j)}}{\xi_{(i)} - \xi_{(j)}} \right) \left(\frac{\beta'_{(k)} - \beta'_{(l)}}{\xi_{(k)} - \xi_{(j)}} \right) = \pm \frac{I_0^6 m}{\pm I_0} = \pm I_0^5 m, \tag{2.38}$$

where we take the product for $(i, j, k, l) = (1, 2, 3, 4)$, $(1, 3, 2, 4)$, $(1, 4, 2, 3)$. For each tuple (i, j, k, l), equation (2.36) tells us

$$\left(\frac{\beta'_{(i)} - \beta'_{(j)}}{\xi_{(i)} - \xi_{(j)}} \right) \left(\frac{\beta'_{(k)} - \beta'_{(l)}}{\xi_{(k)} - \xi_{(j)}} \right) = Q_1(x_1, y_1, z_1) - \xi_{(i,j,k,l)} Q_2(x_1, y_1, z_1), \tag{2.39}$$

where $\xi_{(i,j,k,l)} = \xi_{(i)}\xi_{(j)} + \xi_{(k)}\xi_{(l)}$,

$$Q_1(X, Y, Z) = X^2 - a_1XY + a_2Y^2 + (a_1^2 - 2a_2)XZ + (a_3 - a_1a_2)YZ + (-a_1a_3 + a_2^2 + a_4)Z^2, \tag{2.40}$$

and

$$Q_2(X, Y, Z) = Y^2 - XZ - a_1YZ + a_2Z^2. \tag{2.41}$$

The coefficients of Q_1 and Q_2 are polynomials in the coefficients of f_ξ. Also, we point out that the $\xi_{(i,j,k,l)}$ are the roots ρ_1, ρ_2, and ρ_3 of the cubic resolvent polynomial r_ξ of f_ξ, see (2.26). Define the linear forms

$$L_i(T_1, T_2) = T_1 - \rho_i T_2 \tag{2.42}$$

for $i = 1, 2, 3$. Then the product from equation (2.38) can be expressed as

$$\prod_{i=1}^{3} L_i(Q_1(x, y, z), Q_2(x, y, z)) = F_\xi(Q_1(x, y, z), Q_2(x, y, z)) = \pm I_0^5 m, \tag{2.43}$$

where $F_\xi(T_1, T_2)$ is the cubic resolvent form of ξ, defined in 2.27. Thus, we have established the following Proposition.

Proposition 2.32. *(Theorem 2.1 of [GPP93]) Let ξ be a quartic algebraic integer and $I_0 = I(\xi)$. Assume that $\mathcal{I}(X, Y, Z)$ is an index form for the quartic number field $\mathbb{Q}(\xi)$. The triple $(x, y, z) \in \mathbb{Z}^3$ is a solution to the index form equation*

$$\mathcal{I}(X, Y, Z) = \pm I_0^5 m$$

with $m \in \mathbb{Z}$ if and only if there exists a solution $(t_1, t_2) \in \mathbb{Z}^2$ of the cubic equation

$$F_\xi(T_1, T_2) = \pm I_0^5 m \tag{2.44}$$

such that (x, y, z) *satisfies*

$$\begin{aligned} Q_1(x,y,z) =& x^2 - a_1xy + a_2y^2 + (a_1^2 - 2a_2)xz \\ &+ (a_3 - a_1a_2)yz + (-a_1a_3 + a_2^2 + a_4)z^2 = t_1, \end{aligned} \tag{2.45}$$

and

$$Q_2(x,y,z) = y^2 - xz - a_1yz + a_2z^2 = t_2. \tag{2.46}$$

Proposition 2.32 gives the basic outline of an algorithm developed by Gaál, Pethő, and Pohst in [GPP93] for reducing quartic index form equations.

Quartic Monogenic Orders

Let ξ be an algebraic integer such that $Q(\xi)$ is a quartic number field. Suppose that $\beta \in \mathbb{Z}[\xi]$. Now β will be a monogenizer of $\mathbb{Z}[\xi]$ if and only if $I(\beta) = I(\xi)$. Thus, we may specialize Proposition 2.32 to find monogenizers of monogenic quartic orders. This specialization is due to Akhtari in [Akh22] Section 4.

Proposition 2.33. *(Section 4 Lemma 4.1 [Akh22]) Let* $\mathbb{Z}[\xi]$ *be a quartic order. The algebraic integer* $x\xi + y\xi^2 + z\xi^3$*, with* $x, y, z \in \mathbb{Z}$*, is a monogenizer of* $\mathbb{Z}[\xi]$ *if and only if there exists* $(t_1, t_2) \in \mathbb{Z}^2$ *such that* (x, y, z) *is a solution to the system of equations:*

$$F_\xi(T_1, T_2) = \pm 1 \tag{2.47}$$

and

$$Q_1(X,Y,Z) = t_1, \qquad Q_2(X,Y,Z) = t_2. \tag{2.48}$$

Where, $F_\xi(T_1, T_2)$ *is the cubic resolvent form of* ξ*, and* Q_1 *and* Q_2 *are defined to be*

$$Q_1(X,Y,Z) = X^2 - a_1XY + a_2Y^2 + (a_1^2 - 2a_2)XZ + (a_3 - a_1a_2)YZ + (-a_1a_3 + a_2^2 + a_4)Z^2, \tag{2.49}$$

and

$$Q_2(X,Y,Z) = Y^2 - XZ - a_1YZ + a_2Z^2. \tag{2.50}$$

Proof. Suppose that $\beta \in \mathbb{Z}[\xi]$. Then there exist $c, x, y, z \in \mathbb{Z}$ such that

$$\beta = c + x\xi + y\xi^2 + z\xi^3.$$

Thus,

$$I(\beta) = I(x\xi + y\xi^2 + z\xi^3). \tag{2.51}$$

Now if we assume that β is a monogenizer of $\mathbb{Z}[\xi]$ then $I(\beta) = I(\xi)$ and equation (2.51) becomes

$$I(\beta) = I(x\xi + y\xi^2 + z\xi^3) = I(\xi).$$

Dividing all sides by $I(\xi)$ we get

$$\begin{aligned}\pm 1 = \frac{I(\beta)}{I(\xi)} =& \frac{I(x\xi + y\xi^2 + z\xi^3)}{I(\xi)} \\ &= \prod_{(i,j,k,l)} \left(\frac{\beta_{(i)} - \beta_{(j)}}{\xi_{(i)} - \xi_{(j)}}\right)\left(\frac{\beta_{(k)} - \beta_{(l)}}{\xi_{(k)} - \xi_{(j)}}\right).\end{aligned}$$

The results follow from the same argument used in Proposition 2.32. □

Proposition 2.33 shows that we can organize the monogenizations of the order $\mathbb{Z}[\xi]$ by the solutions $(t_1, t_2) \in \mathbb{Z}^2$ to (2.47). We introduce the following formal notation, for convenience, to be used going forward:

Definition 2.34. Let ξ be an algebraic integer such that $\mathbb{Q}(\xi)$ is a quartic number field.

1. We denote the set of all monogenizations of $\mathbb{Z}[\xi]$ by $\mathcal{M}(\xi)$. That is,

$$\mathcal{M}(\xi) = \{\beta + \mathbb{Z} : \mathbb{Z}[\xi] = \mathbb{Z}[\beta]\}. \tag{2.52}$$

2. We may represent the monogenizations of $\mathbb{Z}[\xi]$ as $(x\xi + y\xi^2 + z\xi^3) + \mathbb{Z}$ for $x, y, z \in \mathbb{Z}$.

   Define $\mathcal{S}_\xi(t_1, t_2)$ to be the set of all monogenizations, $(x\xi + y\xi^2 + z\xi^3) + \mathbb{Z}$, of $\mathbb{Z}[\xi]$ satisfying $\big((Q_1(x, y, z), Q_2(x, y, z)\big) = \pm(t_1, t_2)$ for a fixed solution $(t_1, t_2) \in \mathbb{Z}^2$ to equation (2.47). That is,

$$S_\xi(t_1, t_2) = \{(x\xi + y\xi^2 + z\xi^3) + \mathbb{Z} \in \mathcal{M}(\xi) : \big(Q_1(x, y, z), Q_2(x, y, z)\big) = \pm(t_1, t_2)\}. \tag{2.53}$$

Returning to the first example of a monogenic quartic order, we show how the monogenizations are separated by the solution to (2.47).

Example 2.35. We saw in Example 1.11 that $f(T) = T^4 - 4T^2 - T + 1$ is irreducible, and if ξ is a root of f then the ring $\mathbb{Z}[\xi]$ is a monogenic quartic order with monogenizations define by the points shown below in the basis $\{1, \xi, \xi^2, \xi^3\}$.

$$(1, 0, 0), (-12, 1, 3), (-8, 1, 2), (-5, 0, 1), (-4, 0, 1),$$

$$(-4,1,1),(-3,0,1),(0,1,0),(0,2,1),(1,2,-1),(3,1,-1),$$
$$(4,1,-1),(4,9,-5),(4,33,16),(8,1,-2),(14,3,-4).$$

The cubic resolvent polynomial of f is

$$r_\xi(T) = T^3 + 4T^2 - 4T - 17,$$

and the primitive solutions to the equation

$$F_\xi(T_1, T_2) = T_2^3 r_\xi(T_1/T_2) = \pm 1$$

are $(1,0)$, $(2,1)$, $(2,-1)$, and $(4,-1)$. Dividing up the monogenizations of $\mathbb{Z}[\xi]$ by these solutions we get

$$\begin{aligned}
\mathcal{S}_\xi(1,0) =& \{(1,0,0),(0,2,1),(-3,-1,1),(-4,0,1)\},\\
\mathcal{S}_\xi(2,1) =& \{(-12,1,3),(-5,0,1),(4,9,-5),(8,1,-2)\},\\
\mathcal{S}_\xi(2,-1) =& \{(-3,0,1),(-8,1,2),(2,1,-1),(4,1,-1)\},\\
\mathcal{S}_\xi(4,-1) =& \{(0,1,0),(-1,-2,1),(-14,-3,4),(4,33,16),(-4,1,1)\}.
\end{aligned}$$

In light of Theorem 2.24 we can think of Proposition 2.33 as picking a monogenization of the cubic resolvent ring, given by the solution $(t_1, t_2) \in \mathbb{Z}^2$, and then finding a subset of the quartic monogenizations associated to that cubic solution, ie, finding $\mathcal{S}_\xi(t_1, t_2)$.

For any monogenic order $\mathbb{Z}[\xi]$, we will always have the trivial solutions $(\pm 1, 0, 0)$ corresponding to the monogenizations $\xi + \mathbb{Z}$. A simple calculation shows that $\pm(1,0)$ is a solution to equation (2.47) and $\xi + \mathbb{Z} \in \mathcal{S}_\xi(1,0)$. In [GPP96] it is shown that for each solution $(t_1, t_2) \in \mathbb{Z}^2$ to equation (2.47) there exists a finite set of integral binary quartic form equations whose solutions correspond to the monogenizations in $\mathcal{S}_\xi(t_1, t_2)$. The binary form associated with the trivial solution $(1,0)$ to (2.47) is explicitly constructed by Akhtari in Section 4.1 of [Akh22]. This form will be connected to the monogenizations which have a type I relation to ξ in the order $\mathbb{Z}[\xi]$. We summarize a few facts about the binary form associated with the trivial solution to (2.47) for later reference.

Lemma 2.36. *([Akh22]) Let $\beta = x\xi + y\xi^2 + z\xi^3$ with $x, y, z \in \mathbb{Z}$, be a monogenizer of $\mathbb{Z}[\xi]$. Suppose that (x, y, z) satisfy*

$$Q_1(x,y,z) = \pm 1 \qquad \textit{and} \qquad Q_2(x,y,z) = 0,$$

where Q_1 and Q_2 are defined in (2.49) *and* (2.50)*. Then the following statements hold:*

1. *The triples $(x, y, z) \in \mathbb{Z}^3$ such that $(x\xi + y\xi^2 + z\xi^3) + \mathbb{Z} \in \mathcal{S}_\xi(1, 0)$ are parameterized by pairs $(p, q) \in \mathbb{Z}^2$ with $q > 0$ or $(p, q) = (1, 0)$, satisfying the following equations:*

$$X(P, Q) = P^2 - a_1PQ + a_2Q^2, \quad Y(P, Q) = PQ, \quad Z(P, Q) = Q^2, \tag{2.54}$$

and

$$\mathcal{Q}_\xi(P, Q) = Q_1\big(X(P, Q), Y(P, Q), Z(P, Q)\big) = \pm 1. \tag{2.55}$$

2. *The binary quartic form $\mathcal{Q}_\xi$ satisfies*

$$\mathcal{Q}_\xi(P, Q) = Q^4 f_\xi\left(\frac{P}{Q} - a_1\right). \tag{2.56}$$

2.6 Galois Groups of Quartic Polynomials

In Chapter 5, we explore the type classification of monogenic orders in number fields with Galois groups V_4, C_4, and D_4. Here, we introduce an essential theorem for studying quartic polynomials in terms of their Galois group.

Let $f \in \mathbb{Q}[T]$ be an irreducible polynomial of degree n. Since $\mathbb{Q}$ is characteristic 0, f is separable. Let $\xi \in \mathbb{C}$ be a root of f, $K = \mathbb{Q}(\xi)$ and $\overline{K}$ be the splitting field of f. Then $\overline{K}$ is a Galois extension of $\mathbb{Q}$, let $G = \mathrm{Gal}(\overline{K}/\mathbb{Q})$. The action of G permutes the roots of f in $\overline{K}$.

Definition 2.37. Let $f \in \mathbb{Q}[T]$ and K the splitting field of f. The *Galois group of* f is defined to be the Galois group $\mathrm{Gal}(K/\mathbb{Q})$. We denote the Galois group of f by $\mathrm{Gal}(f)$.

It is well known that the group $G = \mathrm{Gal}(f)$ acts transitively on the roots of f and that the size of G is divisible by $\deg(f)$; see Chapter 14, Section 6 of [DF03]. Labeling the roots of f as $\xi_{(1)}, \xi_{(2)}, ..., \xi_{(n)}$ defines embedding of G into the group S_n. Our primary concern will be the Galois groups of quartic polynomials. We can see that such a group must be isomorphic to a transitive subgroup of S_4. Table 2.1 shows one conjugate subgroup for each transitive subgroup of S_4. The groups D_4 and C_4 have transitive conjugate subgroups in S_4. When working with the Galois group of a polynomial, we will typically only identify with a subgroup of S_n up to isomorphism.

An elementary test to determine the Galois group of irreducible quartic polynomials was developed by Kappe and Warren in [KW89].

Theorem 2.38. *(Theorem 1 of [KW89]) Let* $f(T) = T^4 + a_1T^3 + a_2T^2 + a_3T + a_4 \in \mathbb{Z}[T]$ *be irreducible over* $\mathbb{Q}$*. Let* $r(T) = T^3 - a_3T^2 + (a_1a_3 - 4a_4)T - (a^2a_4 - 4a_2a_4 + a_3^2)$ *the cubic resolvent polynomial of* f*. Also, let* L *be the splitting field of* r*. Then* $\mathrm{Gal}(f)$ *is isomorphic to:*

1. V_4 *if and only if* $r(T)$ *splits completely over* $\mathbb{Q}$*.*
2. C_4 *if and only if* $r(T)$ *has exactly one root in* $\rho \in \mathbb{Q}$ *and*

$$g(T) = (T^2 - \rho T + a_4)(T^2 + a_1T + (a_3 - \rho)) \tag{2.57}$$

   splits over L*.*

3. D_4 *if and only if* $r(T)$ *has exactly one root over* $\mathbb{Q}$ *and* $g(T)$ *as defined in* (2.57) *does not split over* L*.*
4. A_4 *if and only if* $r(T)$ *is irreducible over* $\mathbb{Q}$ *and the discriminant of* f *is a square in* $\mathbb{Z}$*.*
5. S_4 *if and only if* $r(T)$ *is irreducible over* $\mathbb{Q}$ *and the discriminant of* f *is not a square in* $\mathbb{Z}$*.*

Theorem 2.38 indicates that if $f \in \mathbb{Z}[T]$ is an irreducible quartic polynomial with $\mathrm{Gal}(f) \cong V_4, C_4$ or D_4, then the cubic resolvent polynomial of f, $r(T)$ defined in 2.26 is reducible over $\mathbb{Q}$. We will show the reducibility of r directly in Chapter 5,

Group	Size	Elements
S_4	24	all of S_4
A_4	12	all even permutations
D_4	8	$\{1, (1324), (12)(34), (1423), (13)(24), (14), (23), (12), (34)\}$
V_4	4	$\{1, (12)(34), (13)(24), (14)(23)\}$
C_4	4	$\{1, (1234), (13)(24), (1432)\}$

Table 2.1. One conjugate subgroup for each of the transitive subgroups of S_4. Since the Galois group of a degree 4 polynomial must be a transitive subgroup of S_4, the table identifies all the possible Galois groups up to isomorphism.

where it will be essential to the argument used to address quartic fields with Galois group C_4, V_4, or D_4.

Theorem 2.38 provides a practical test for finding the Galois group of quartic polynomials, as can be seen in the example below. The logic of Theorem 2.38 was incorporated into a function in the SageMath code used to find examples of quartic orders that are neither type I nor type II but have exactly two monogenizations. Chapter 6 discusses several examples of interesting quartic orders found using tools developed in SageMath.

Example 2.39. We return to the polynomial $f(T) = T^4 - 4T^2 - T + 1$ from example 1.11. Using Sagemath, we verify that f is irreducible over $\mathbb{Q}$. Note that the discriminant, $\text{Disc}(f) = 1957$, is not a square in $\mathbb{Z}$. Therefore, by Theorem 2.38, the Galois group of f is S_4.

CHAPTER 3

ORDERS OF TYPE I

We study type I orders within the framework of index form equations. First, we will share some observations about the forms arising when solving index form equations for degrees 3 and 4. Next, we will briefly address some facts about type I relations in a monogenic ring of any rank. With these observations, we will address cubic type I orders and then quartic type I orders. At the end of the chapter, we will provide several examples of quartic type I orders.

3.1 Matrix Actions and Solutions to Cubic and Quartic Index Form Equations

For cubic and quartic monogenic orders, the monogenizations are determined by solutions to particular Diophantine equations. See Lemma 2.31 and Proposition 2.32.

Cubic Monogenic Orders

For a cubic order $\mathbb{Z}[\gamma]$, where the minimal polynomial of γ is $f_\gamma(T) = T^3 + c_1T^2 + c_2T + c_3$, Lemma 2.31 tells us that the monogenizations are given by the solutions to

$$C_\gamma(T_1, T_2) = T_1^3 - 2c_1T_1^2T_2 + (c_1^2 + c_2)T_1T_2^2 - (c_1c_2 - c_3)T_2^3 = \pm 1. \tag{3.1}$$

Let $H_\gamma(T_2, T_2) = T_1^3 + c_1T_1^2T_2 + c_2T_1T_2^2 + c_3T_2^3$ be the minimal form of γ. Then we notice that

$$\begin{pmatrix} 1 & 0 \\ -c_1 & 1 \end{pmatrix} \cdot H_\gamma(T_1, T_2) = C_\gamma(T_1, T_2).$$

Therefore, C_γ is $\mathrm{GL}_2(\mathbb{Z})$-equivalent to H_γ. So, by Lemma 2.10 the solutions to $C_\gamma(T_1, T_2) = \pm 1$ are in one-to-one correspondence with the solutions to $H_\gamma(T_1, T_2) = \pm 1$. In this correspondence, we send a solution $(t_1, t_2) \in \mathbb{Z}^2$ to the point $(t_1 + c_1t_2, t_2)$. The following lemma summarizes our observations.

Lemma 3.1. *Suppose that γ is a cubic algebraic integer with minimal form*

$$H_\gamma(T_1, T_2) = T_1^3 + c_1T_1^2T_2 + c_2T_1T_2^2 + c_3T_2^3.$$

Then the set of primitive solutions $(t_1, t_2) \in \mathbb{Z}$ *to* $H_\gamma(T_1, T_2) = \pm 1$ *is in bijection with the set of monogenizations of* $\mathbb{Z}[\gamma]$*. The bijection is defined by*

$$(t_1, t_2) \mapsto \left((t_1 + c_1 t_2)\gamma + t_2\gamma^2\right) + \mathbb{Z}$$

for $(t_1, t_2) \in \mathbb{Z}^2$ *a primitive solutions to* $H_\gamma(T_1, T_2) = \pm 1$*.*

We can see that, under this correspondence, the trivial solution to $H_\xi(T_1, T_2) = \pm 1$ corresponds to the monogenization defined by γ.

Quartic Monogenic Orders

Let ξ be a quartic algebraic integer and $H_\xi(T) = T^4 + a_1T^3 + a_2T^2 + a_3T + a_4$ be the minimal form of ξ. As we saw in Proposition 2.33, the monogenizations of $\mathbb{Z}[\xi]$ are determined by the solutions to the system of equations (2.47) and (2.48). Additionally, the monogenizations in $\mathcal{S}_\xi(1, 0)$ correspond to the solutions to the binary quartic form equation $\mathcal{Q}_\xi(P, Q) = \pm 1$, defined in (2.55).

We observe that

$$\mathcal{Q}_\xi = \begin{pmatrix} 1 & 0 \\ -a_1 & 1 \end{pmatrix} H_\xi. \tag{3.2}$$

Thus, the solutions to $\mathcal{Q}_\xi(P, Q) = \pm 1$ are in one-to-one correspondence with the solutions to $H_\xi(T_1, T_2) = \pm 1$. Specifically, if (t_1, t_2) is a solution to $H_\xi(T_1, T_2) = \pm 1$, then $p = t_1 + a_1t_2$, and $q = t_2$ will be a solution to $\mathcal{Q}_\xi(P, Q) = \pm 1$. This lets us find the monogenizations of $\mathbb{Z}[\xi]$ in $\mathcal{S}_\xi(1, 0)$. The following lemma summarizes our observation.

Lemma 3.2. *Let* ξ *be a quartic algebraic integer whose minimal form is* $H_\xi(T_1, T_2)$*. Then there is a two-to-one map between the integral solutions to* $H_\xi(T_1, T_2) = \pm 1$ *and the monogenizations of* $\mathbb{Z}[\xi]$*. The map is defined by*

$$\pm(t_1, t_2) \mapsto \left((t_1^2 + a_1t_1t_2 + a_2t_2^2)\xi + (a_1t_2^2 + t_1t_2)\xi^2 + t_2^2\xi^3\right) + \mathbb{Z}. \tag{3.3}$$

Furthermore, the image of this map is the subset $\mathcal{S}_\xi(1, 0)$ *of monogenizations that give the trivial solution to the cubic equation* $F_\xi(T_1, T_2) = \pm 1$*, where* F_ξ *is the cubic resolvent form of* ξ*.*

3.2 The Type I Relation and Connections to Minimal Polynomials

The following lemma provides an equivalent condition for two monogenizers of the same ring having a type I relation.

Lemma 3.3. *Let ξ be an algebraic integer, and $\beta \in \mathbb{Z}[\xi]$. Suppose that β is a monogenizer of $\mathbb{Z}[\xi]$, then $\beta \sim_1 \xi$ if and only if there exist integers $a, b, c, d \in \mathbb{Z}$ such that $|ac - bd| = 1$, $c \neq 0$, and*

$$\beta(c\xi + d) = a\xi - b.$$

As one may have suspected for algebraic integers ξ and β with $\mathbb{Z}[\xi] = \mathbb{Z}[\beta]$, the condition of $\xi \sim_1 \beta$ can be stated in terms of an action of $\mathrm{GL}_2(\mathbb{Z})$. Let

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z})$$

and $\alpha \in K = \mathbb{Q}(\xi)$. We define an action of $\mathrm{GL}_2(\mathbb{Z})$ on K by

$$A \cdot \alpha = \frac{a\alpha + b}{c\alpha + d}.$$

So, if $\xi \sim_1 \beta$ then ξ and β are in the same $\mathrm{GL}_2(\mathbb{Z})$-orbit in $\mathbb{Z}[\xi] \subseteq \mathcal{O}_K$, and $\beta + \mathbb{Z} \neq \xi + \mathbb{Z}$. However, it is not true that for any $A \in \mathrm{GL}_2(\mathbb{Z})$ then $A \cdot \xi$ will be a monogenizer of $\mathbb{Z}[\xi]$, or even that $A \cdot \xi \in \mathbb{Z}[\xi]$. Still, the action of $\mathrm{GL}_2(\mathbb{Z})$ on the algebraic integer ξ and the minimal form of H_ξ of ξ are connected. The following lemma highlights a particular aspect of the connection relevant to type I relations.

Lemma 3.4. *Let ξ be an algebraic integer, and let H_ξ be the minimal form of ξ. Suppose that β is a monogenizer of $\mathbb{Z}[\xi]$ and $\beta + \mathbb{Z} \neq \xi + \mathbb{Z}$ as monogenizations. If $(t_1, t_2) \in \mathbb{Z}^2$ is such that $H_\xi(t_1, t_2) = \pm 1$ and $A = \begin{pmatrix} a & b \\ -t_2 & t_1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z})$ satisfies*

$$\beta = A \cdot \xi,$$

then the minimal form of β, H_β satisfies

$$H_\beta = (A^{\mathrm{tr}})^{-1} H_\xi.$$

Proof. First note that if $\beta = A \cdot \xi$ then

$$\xi = A^{-1} \cdot \beta = \frac{t_1\beta - b}{t_2\beta + a}, \tag{3.4}$$

and observe that

$$(A^{\mathrm{tr}})^{-1} = \begin{pmatrix} t_1 & t_2 \\ -b & a \end{pmatrix}.$$

Let $B = (A^{\mathrm{tr}})^{-1}$ and $H_0 = B \cdot H_\xi$. Then

$$\begin{aligned} H_0(T_1, T_2) =& B \cdot H_\xi(T_1, T_2) = (\det B)^{-1} H_\xi(t_1 T_1 - bT_2, t_2 T_1 + aT_2) \\ =& (\det B)^{-1} (t_2 T_1 + aT_2)^n f_\xi \left(\frac{t_1 T_1 - bT_2}{t_2 T_1 + aT_2} \right). \end{aligned} \tag{3.5}$$

So $H_0(1, 0) = H_\xi(t_1, t_2) = 1$, and thus H_0 is monic. Additionally,

$$H_0(\beta, 1) = (t_1\beta - b)^n f_\xi \left(\frac{t_1\beta - b}{t_2\beta + a} \right) \tag{3.6}$$

$$= (t_1\beta - b)^n f_\xi(\xi) = 0, \tag{3.7}$$

where the equality (3.7) is due to $A^{-1} \cdot \beta = \xi$. Therefore, $H_0(T, 1)$ is a monic polynomial in $\mathbb{Z}[T]$ of degree $n = \deg \xi = \deg \beta$, which has β as a root. Thus, H_0 is the minimal form of β. □

3.3 Cubic Orders of Type I

We will prove that if $\mathbb{Z}[\gamma]$ is two times monogenic, then it is a type I order. This result is known; see [BEG13], Theorem 1.2. However, the proof method used here differs from what appears in [BEG13].

Theorem 3.5. *Let γ be a cubic algebraic integer, $H_\gamma(T) = T_1^3 + c_1 T_1^2 T_2 + c_2 T_1 T_2^2 + c_3 T_2^2$ be the minimal form of γ, and $\beta \in \mathbb{Z}[\gamma]$. If β and γ define distinct monogenizations of $\mathbb{Z}[\gamma]$ then $\beta \sim_1 \gamma$.*

Proof. Suppose $\beta \in \mathbb{Z}[\gamma]$ is a monogenizer. Then, by Lemma 3.1, there exist $(t_1, t_2) \in \mathbb{Z}^2$ such that $H_\gamma(t_1, t_2) = \pm 1$ and

$$\beta = \lambda + (t_1 + c_1 t_2)\gamma + t_2\gamma^2, \tag{3.8}$$

for some $\lambda \in \mathbb{Z}$. Note that if $t_2 = 0$, then $t_1 = \pm 1$, and β will be $\mathbb{Z}$-equivalent to γ. Thus, we take $t_2 \neq 0$ and for simplicity we assume $H_\gamma(t_1, t_2) = 1$.
Now consider

$$1 = H(t_1, t_2) = t_1(t_1^2 + c_1 t_1 t_2 + c_2 t_2^2) - t_2(-c_3 t_2^2). \tag{3.9}$$

Let $P_\gamma(t_1, t_2) = t_1^2 + c_1 t_1 t_2 + c_2 t_2^2$ and

$$A(t_1, t_2) = \begin{pmatrix} P_\gamma(t_1, t_2) & c_3 t_2^2 \\ -t_2 & t_1 \end{pmatrix}. \tag{3.10}$$

Note that $\det A(t_1, t_2) = 1$ by equation (3.9). Following Lemma 3.3 we will check that $A(t_1, t_2) \cdot \xi = \beta$ by verifying that

$$0 = (\beta - \lambda)\big(- t_2\gamma + t_1) - (P_\gamma(t_1, t_2)\gamma + c_3 t_2^2\big). \tag{3.11}$$

Substituting for β from equation (3.8) in equation (3.11) we get

$$\begin{aligned} &(\beta - \lambda)\big(- t_2\gamma + t_1) - (P_\gamma(t_1, t_2)\gamma + c_3 t_2^2\big) \\ &= \big((t_1 + c_1 t_2)\gamma + t_2\gamma^2\big)\ \big(- t_2\gamma + t_1) - (P_\gamma(t_1, t_2)\gamma + c_3 t_2^2\big) \\ &= - t_2^2(\gamma^3 + c_1\gamma^2 + c_2\gamma + c_3) = -t_2^2 f_\gamma(\gamma) = 0. \end{aligned}$$

Therefore, $\beta \sim_1 \gamma$ by Lemma 3.3. □

3.4 Quartic Orders of Type I

Let ξ be an algebraic integer with $\mathbb{Z}[\xi]$ a quartic order. We aim to determine which solutions to the quartic index form equations for $\mathbb{Z}[\xi]$ yield type I monogenizations. In addition, we will explore the connection between type I quartic monogenizers and the $\mathrm{GL}_2(\mathbb{Z})$-orbits of binary quartic forms.

Theorem 3.6. *Let ξ be a quartic algebraic integer and $H_\xi(T_1, T_2) = T_1^4 + a_1 T_1^3 T_2 + a_2 T_1^2 T_2^2 + a_3 T_1 T_2^3 + a_4 T_2^4$ the minimal form of ξ. Also, let β be a monogenizer of $\mathbb{Z}[\xi]$ satisfying $\xi + \mathbb{Z} \neq \beta + \mathbb{Z}$ as monogenizations. Then $\beta \sim_1 \xi$ if and only if there exists $x, y, z \in Z$ such that, $\beta + \mathbb{Z} = (x\xi + y\xi^2 + z\xi^3) + \mathbb{Z}$ as monogenizations, and $(x\xi + y\xi^2 + z\xi^3) + \mathbb{Z} \in \mathcal{S}_\xi(1, 0)$. Equivalently,*

$$Q_1(x, y, z) = \pm 1, \qquad\qquad Q_2(x, y, z) = 0,$$

for Q_1 and Q_2 defined in (2.49) *and* (2.50).

Proof. Let $\beta \in \mathbb{Z}[\xi]$, $\mathbb{Z}[\beta] = \mathbb{Z}[\xi]$, and

$$f_\xi(T) = T^4 + a_1 T^3 + a_2 T^2 + a_3 T + a_4 \in \mathbb{Z}[T] \tag{3.12}$$

be the minimal polynomial of ξ. First, we assume that $\xi \sim_1 \beta$. Then there exists

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z})$$

such that

$$\beta = \frac{a\xi + b}{c\xi + d} \tag{3.13}$$

with $c \neq 0$. Since $\beta \in \mathbb{Z}[\xi]$, we may take

$$\beta = \lambda + x\xi + y\xi^2 + z\xi^3 \tag{3.14}$$

for $\lambda, x, y, z \in \mathbb{Z}$. Now, β and $\beta + \lambda$ will have the same index and define the same homogenization, so we can assume that $\lambda = 0$.

Using equations (3.13) and (3.14), with $\lambda = 0$, together we find that,

$$0 = (x\xi + y\xi^2 + z\xi^3)(c\xi + d) - (a\xi + b). \tag{3.15}$$

Let

$$p(T) = (xT + yT^2 + zT^3)(cT + d) - (aT + b).$$

Note that, $p(T)$ is degree 4 with coefficients in $\mathbb{Z}$, and $p(\xi) = 0$. Therefore,

$$p(T) = m f_\xi(T)$$

for some $m \in \mathbb{Z}$. Rewriting p and equating the coefficients, we get the following relations:

$$cz = m, \tag{3.16}$$

$$cy + dz = ma_1, \tag{3.17}$$

$$cx + dy = ma_2, \tag{3.18}$$

$$dx - a = ma_3, \tag{3.19}$$

$$-b = ma_4. \tag{3.20}$$

Solving these relations for x, y and z give us:

$$z = \frac{m}{c}, \tag{3.21}$$

$$y = m\frac{ca_1 - d}{c^2}, \tag{3.22}$$

$$x = m\frac{c^2a_2 + cda_1 - d^2}{c^3}. \tag{3.23}$$

Substituting our expressions for x, y and z into Q_2 from (2.50) gives us

$$\begin{aligned} Q_2(x,y,z) =& y^2 - xz - a_1yz + a_2z^2 \\ =& m^2\Bigg(\left(\frac{ca_1 - d}{c^2}\right)^2 - \left(\frac{c^2a_2 + cda_1 - d^2}{c^3}\right)\left(\frac{1}{c}\right) \\ & - a_1\left(\frac{ca_1 - d}{c^2}\right)\left(\frac{1}{c}\right) + a_2\left(\frac{1}{c}\right)^2\Bigg) = 0. \end{aligned}$$

Since β is by assumption a monogenizer, we know from Proposition 2.33 that the cubic resolvent form of ξ, F_ξ, satisfies

$$F_\xi(Q_1(x,y,z), Q_2(x,y,z)) = \pm 1.$$

Thus, $Q_1(x,y,z) = \pm 1$, since F_ξ is degree 3 and monic. Therefore,

$$\beta + \mathbb{Z} = (x\xi + y\xi^2 + z\xi^3) + \mathbb{Z} \in \mathcal{S}_x(1,0).$$

Next, suppose that $\beta = \lambda + x\xi + y\xi^2 + z\xi^3$, where $\lambda \in \mathbb{Z}$ and $(x,y,z) \in \mathbb{Z}^3$ satisfies

$$Q_1(x,y,z) = \pm 1, \qquad\qquad Q_2(x,y,z) = 0,$$

for Q_1 and Q_2 defined in (2.49) and (2.50). Let H_ξ be the minimal form of ξ. Then by Lemma 3.2 there exist $(t_1,t_2) \in \mathbb{Z}^2$ such that $H_\xi(t_1,t_2) = \pm 1$ and

$$(\beta - \lambda) = (t_1^2 + a_1t_1t_2 + a_2t_2^2)\xi + (a_1t_2^2 + t_1t_2)\xi^2 + t_2^2\xi^3. \tag{3.24}$$

We can see that if $t_2 = 0$ then β will be $\mathbb{Z}$-equivalent to ξ, so we may take $t_2 \neq 0$. Observe that

$$\pm 1 = H_\xi(t_1,t_2) = t_1(t^3 + a_1t_1^2t_2 + a_2t_1t_2^2 + a_3t_2^3) + t_2(a_4t_2^3). \tag{3.25}$$

Denote

$$G_\xi(T_1,T_2) = T_1^3 + a_1T_1^2T_2 + a_2T_1T_2^2 + a_3T_2^3, \tag{3.26}$$

and consider the matrix

$$M(t_1,t_2) = \begin{pmatrix} G_\xi(t_1,t_2) & a_4t_2^3 \\ -t_2 & t_1 \end{pmatrix}. \tag{3.27}$$

Note that $\det M(t_1, t_2) = H_\xi(t_1, t_2) = \pm 1$. Now we verify that $\beta - \lambda = M(t_1, t_2) \cdot \xi$. Consider

$$\begin{aligned}
&(\beta - \lambda)(-t_2\xi + t_1) - (G_\xi(t_1, t_2)\xi + a_4 t_2^3) \\
&= \left((t_1^2 + a_1 t_1 t_2 + a_2 t_2^2)\xi + (a_1 t_2^2 + t_1 t_2)\xi^2 + t_2^2\xi^3\right)(-t_2\xi + t_1) - (G_\xi(t_1, t_2)\xi + a_4 t_2^3) \\
&= -t_2^3(\xi^4 + a_1\xi^3 + a_2\xi^2 + a_3\xi + a_4) = -t_2^3 f_\xi(\xi) = 0
\end{aligned} \tag{3.28}$$

Therefore, by Lemma 3.3 $\beta \sim_1 \xi$ via the matrix $M(t_1, t_2)$. □

The proof of Theorem 3.6 shows that we can formulate the type I relation between monogenizers in terms of the solutions to the minimal form.

Corollary 3.7. *Let ξ be a quartic algebraic integer, H_ξ the minimal form of ξ, and $\beta \in \mathbb{Z}[\xi]$ be a monogenizer. Then $\xi \sim_1 \beta$ if and only if there exist $(t_1, t_2) \in \mathbb{Z}^2$, $(t_1, t_2) \neq (\pm 1, 0)$ such that $H_\xi(t_1, t_2) = \pm 1$, and*

$$\beta = \lambda + (t_1^2 + a_1 t_1 t_2 + a_2 t_2^2)\xi + (t_1 t_2 + a_1 t_2^2)\xi^2 + t_2^2\xi^3$$

for some $\lambda \in \mathbb{Z}$. Moreover, the matrix $M_\xi(t_1, t_2) \in \mathrm{GL}_2(\mathbb{Z})$ defined in (3.27) is such that $\beta - \lambda = M_\xi(t_1, t_2) \cdot \xi$.

Proof. Suppose that $\beta \sim_1 \xi$. Then by Theorem 3.6 $\beta + \mathbb{Z} \in \mathcal{S}_\xi(1, 0)$. This is equivalent to the existence of $x, y, z \in \mathbb{Z}$ such that

$$\beta + \mathbb{Z} = (x\xi + y\xi^2 + z\xi^3) + \mathbb{Z},$$

as monogenizations, and

$$Q_1(x, y, z) = \pm 1, \qquad Q_2(x, y, z) = 0,$$

for Q_1 and Q_2 defined in (2.49) and (2.50). Then by Lemma 3.2 there exist $(t_1, t_2) \in \mathbb{Z}^2$ satisfying $H_\xi(t_1, t_2) = \pm 1$ and

$$\beta = \lambda + (t_1^2 + a_1 t_1 t_2 + a_2 t_2^2)\xi + (t_1 t_2 + a_1 t_2^2)\xi^2 + t_2^2\xi^3,$$

for some $\lambda \in \mathbb{Z}$. Now, if we let $M(t_1, t_2)$ be as in (3.27), the calculation in 3.28 shows that $\beta + \mathbb{Z} = M(t_1, t_2) \cdot \xi + \mathbb{Z}$ as monogenizations. □

With Theorem 3.6, we can now find all the monogenization of the order from Example 1.11 that have a type I relation with the given monogenizer ξ.

Example 3.8. We saw in Example 2.35 the order $\mathbb{Z}[\xi]$ where ξ is a root of $f(T) = T^4 - 4T^2 - T + 1$ has 17 monogenizations divided into four groups by the solutions to $F_\xi(T_1, T_2) = \pm 1$, where F_ξ is the cubic resolvent form of ξ, see definition 2.27. We show the monogenizations here represented by points in the basis $\{1, \xi, \xi^2, \xi^3\}$.

$$\begin{aligned}
\mathcal{S}_\xi(1,0) =& \{(1,0,0),(0,2,1),(-3,-1,1),(-4,0,1)\},\\
\mathcal{S}_\xi(2,1) =& \{(-12,1,3),(-5,0,1),(4,9,-5),(8,1,-2)\},\\
\mathcal{S}_\xi(2,-1) =& \{(-3,0,1),(-8,1,2),(2,1,-1),(4,1,-1)\},\\
\mathcal{S}_\xi(4,-1) =& \{(0,1,0),(-1,-2,1),(-14,-3,4),(4,33,16),(-4,1,1)\}.
\end{aligned}$$

So, by Theorem 3.6, the monogenizations

$$(2\xi + \xi^3) + \mathbb{Z}, \qquad (-3\xi - \xi^2 + \xi^3) + \mathbb{Z}, \qquad \text{and} \qquad (-4\xi + \xi^3) + \mathbb{Z},$$

all are type I related to $\xi + \mathbb{Z}$.

One can see that the matrix $M_\xi(t_1, t_2)$, from (3.27), satisfies the requirements of Lemma 3.4. Therefore, if ξ is a quartic algebraic integer and $\beta \in \mathbb{Z}[\xi]$ is such that $\beta \sim_1 \xi$, then the minimal forms of ξ and β are $\mathrm{GL}_2(\mathbb{Z})$-equivalent. However, it is not true that two quartic algebraic integers with equivalent minimal forms will have a type I relation. The following example demonstrates that two algebraic integers in the same order can have equivalent minimal forms that do not exhibit a type I relation.

Example 3.9. Let ζ be a fifth root of unity and consider the ring $\mathbb{Z}[\zeta]$. Recall that $\mathbb{Z}[\zeta]$ is the ring of integers for the cyclotomic field $\mathbb{Q}(\zeta)$ and that $\mathbb{Q}(\zeta)$ is a Galois field with Galois group C_4. Note that, ζ^2 is a monogenizer of $\mathbb{Z}[\zeta]$, defining the basis $\{1, \zeta^2, \zeta^4, (\zeta^2)^3 = \zeta\}$. Suppose that $a, b, c, d \in \mathbb{Z}$ are such that,

$$0 = \zeta^2(c\zeta + d) - (a\zeta + b) = c\zeta^3 + d\zeta^2 - a\zeta - b.$$

Thus, $p(T) = cT^3 + dT^2 - aT - b \in \mathbb{Z}[T]$ is a polynomial such that $p(\zeta^2) = 0$, but ζ^2 is an algebraic conjugate of ζ. So, its minimal polynomial is the fifth cyclotomic polynomial, which is of degree 4. Therefore, $a = b = c = d = 0$, and by Lemma 3.3, ζ and ζ^2 are not type I. Since ζ and ζ^2 are algebraic conjugates, they will have the same (and therefore $\mathrm{GL}_2(\mathbb{Z})$-equivalent) minimal forms.

Example 3.9 illustrates the heart of the issue: minimal forms only specify algebraic numbers up to their algebraic conjugates. Taking this into account, we can provide a partial converse to Lemma 3.4 for quartic orders.

Lemma 3.10. *Let ξ be a quartic algebraic integer and $\beta \in \mathbb{Z}[\xi]$ a monogenizer such that ξ and β define distinct monogenizations. Also, let H_ξ and H_β be the minimal forms of ξ and β, respectively. If H_ξ is $\mathrm{GL}_2(\mathbb{Z})$-equivalent to H_β, and $H_\xi \neq H_\beta$, then there exists an algebraic conjugate to β, $\beta' \in \mathbb{Z}[\xi]$, such that $\beta' + \mathbb{Z} \sim_1 \xi + \mathbb{Z}$.*

Proof. Let H_ξ and H_β be the minimal forms of ξ and β, respectively. Suppose that there exists $A \in \mathrm{GL}_2(\mathbb{Z})$ such that $H_\beta = A \cdot H_\xi$. Let

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}. \tag{3.29}$$

Since ξ and β define different monogenizations and $H_\xi \neq H_\beta$, we have $b \neq 0$, by the calculation in (2.12). Consider

$$1 = H_\beta(1,0) = (A \cdot H_\xi)(a,b),$$

so (a,b) is a nontrivial solution to $H_\xi(T_1,T_2) = \pm 1$. Therefore, $(A^{-1})^{\mathrm{tr}} = M_\xi(a,b)$ from (3.27). Thus by Corollary 3.7, there exists a β' monogenizer of $\mathbb{Z}[\xi]$ satisfying

$$\beta' = \lambda + (t_1^2 + a_1 t_1 t_2 + a_2 t_2^2)\xi + (t_1 t_2 + a_1 t_2^2)\xi^2 + t_2^2 \xi^3$$

for $(t_1,t_2) = (a,b)$, and $\lambda \in \mathbb{Z}$, such that $\beta' - \lambda = (A^{-1})^{\mathrm{tr}} \cdot \xi$. Now, since $H_\beta = A \cdot H_\xi$, $H_\xi = A^{-1} H_\beta$. Let f_ξ and f_β be the minimal polynomials of ξ and β. Consider

$$\begin{aligned} 0 =& H_\xi(\xi,1) = (A^{-1} \cdot H_\beta)(\xi,1) = \frac{(-b\xi + a)^4}{\det(A)} f_\beta\left(\frac{d\xi - c}{-b\xi + a}\right) \\ =& \frac{(-b\xi + a)^4}{\det(A)} f_\beta\left((A^{-1})^{\mathrm{tr}} \cdot \xi\right) = \frac{(-b\xi + a)^4}{\det(A)} f_\beta(\beta'). \end{aligned}$$

Note that $\frac{(-b\xi+a)^4}{\det(A)} \neq 0$ since ξ is a quartic algebraic integer and A is an invertible matrix. Thus, β' is a root of f_β and therefore is a conjugate of β. □

We see that Lemma 3.10 gives us a test for type I orders.

Lemma 3.11. *Let $\mathcal{O}$ be a quartic monogenic ring with monogenizers ξ and β, defining distinct monogenizations. Also, let H_ξ and H_β be the minimal forms of ξ and β, respectively. If H_ξ is $\mathrm{GL}_2(\mathbb{Z})$-equivalent to H_β and $H_\xi \neq H_\beta$ then $\mathcal{O}$ is a type I order.*

Proof. Let $\mathcal{O}$ be a quartic order with monogenizers $\xi, \beta \in O$, such that $\xi + \mathbb{Z} \neq \beta + \mathbb{Z}$, the minimal forms $H_\xi \neq H_\beta$, and H_ξ is $\mathrm{GL}_2(\mathbb{Z})$-equivalent to H_β. Then by Lemma 3.10 there exists $\beta' \in \mathcal{O}$, such that $\xi \sim_1 \beta'$. Therefore, $\mathcal{O}$ is a type I order. □

Theorem 3.6 hints that there is a connection between quartic monogenizers up to type I relation and the cubic resolvent polynomial. We briefly explore that connection now.

For a quartic order $\mathcal{O} \subseteq \mathbb{C}$, we defined the cubic resolvent map in Definition 2.29 to be

$$\Phi : \mathcal{O} \to \mathbb{C} \tag{3.30}$$

by $\Phi(x) = x_{(1)}x_{(2)} + x_{(3)}x_{(4)}$ where $x_{(i)}$ are the algebraic conjugates of x.

Lemma 3.12. *Let ξ be a quartic algebraic integer and $\beta \in \mathbb{Z}[\xi]$ a monogenizer. If $\beta \sim_1 \xi$ then there exists $\lambda \in \mathbb{Z}$ such that $\beta_{(1)}\beta_{(2)} + \beta_{(3)}\beta_{(4)} + \lambda = \xi_{(1)}\xi_{(2)} + \xi_{(3)}\xi_{(4)}$.*

Proof. Let H_ξ be the minimal form of ξ. Suppose that $\beta \in \mathbb{Z}[\xi]$ and $\beta \sim_1 \xi$. Then by Corollary 3.7 there exists $(d, c) \in \mathbb{Z}^2$ such that

$$A = \begin{pmatrix} a & b \\ -c & d \end{pmatrix} \in \mathrm{GL}_2(Z),$$

(d, c) is a solution to the $H_\xi(T_1, T_2) = \pm 1$, and $\beta = A \cdot \xi$. For $\alpha \in \mathbb{Z}[\xi]$ let

$$\Phi(\alpha) = \alpha_{(1)}\alpha_{(2)} + \alpha_{(3)}\alpha_{(4)} \in \mathbb{C}.$$

We will show that $\Phi(\xi) = \Phi(\beta) + \lambda$, for some $\lambda \in \mathbb{Z}$. We begin by calculating $\Phi(\beta)$. Consider

$$\Phi(\beta) = \Phi\left(\frac{a\xi + b}{-c\xi + d}\right) \tag{3.31}$$

$$= \frac{a\xi_{(1)} + b}{(-c\xi_{(2)} + d)} \frac{a\xi_{(2)} + b}{(-c\xi_{(1)} + d)} + \frac{a\xi_{(3)} + b}{(-c\xi_{(3)} + d)} \frac{a\xi_{(4)} + b}{(-c\xi_{(4)} + d)} \tag{3.32}$$

$$= \frac{(a\xi_{(1)} + b)(a\xi_{(2)} + b)(-c\xi_{(3)} + d)(-c\xi_{(4)} + d)}{(-c\xi_{(1)} + d)(-c\xi_{(2)} + d)(-c\xi_{(3)} + d)(-c\xi_{(4)} + d)} \tag{3.33}$$

$$+ \frac{(a\xi_{(3)} + b)(a\xi_{(4)} + b)(-c\xi_{(1)} + d)(-c\xi_{(2)} + d)}{(-c\xi_{(1)} + d)(-c\xi_{(2)} + d)(-c\xi_{(3)} + d)(-c\xi_{(4)} + d)}. \tag{3.34}$$

From here, we independently evaluate the denominator and numerator of (3.33) and (3.34). For the denominator, we see

$$(-c\xi_{(1)} + d)(-c\xi_{(2)} + d)(-c\xi_{(3)} + d)(-c\xi_{(4)} + d) = \prod_{i=1}^{4}(d - c\xi_{(i)}) = H_\xi(d, c), \tag{3.35}$$

and $H_\xi(d,c) = \pm 1$ by assumption.
For the numerator, we will find it helpful to introduce an expression for the elementary symmetric polynomials evaluated at the conjugates of an element of $\mathbb{Z}[\xi]$. For $\alpha \in \mathbb{Z}[\xi]$ we define the following expressions:

$$\begin{aligned}
\sigma_1(\alpha) =& \alpha_{(1)} + \alpha_{(2)} + \alpha_{(3)} + \alpha_{(4)} \\
\sigma_2(\alpha) =& \alpha_{(1)}\alpha_{(2)} + \alpha_{(1)}\alpha_{(3)} + \alpha_{(1)}\alpha_{(4)} + \alpha_{(2)}\alpha_{(3)} + \alpha_{(2)}\alpha_{(4)} + \alpha_{(3)}\alpha_{(4)} \\
\sigma_3(\alpha) =& \alpha_{(1)}\alpha_{(2)}\alpha_{(3)} + \alpha_{(1)}\alpha_{(2)}\alpha_{(4)} + \alpha_{(1)}\alpha_{(3)}\alpha_{(4)} + \alpha_{(2)}\alpha_{(3)}\alpha_{(4)} \\
\sigma_4(\alpha) =& \alpha_{(1)}\alpha_{(2)}\alpha_{(3)}\alpha_{(4)}.
\end{aligned}$$

Notice that $H_\xi(T_1,T_2) = T_1^4 + \sum_{i=1}^4 (-1)^i \sigma_i(\xi) T_1^{4-i} T_2^i$. So $\sigma_i(\xi) \in \mathbb{Z}$ for $i = 1,2,3,4$. Now, using the σ_i, we see that the numerator of (3.33) and (3.34) simplifies too:

$$\begin{aligned}
&(a\xi_{(1)} + b)(a\xi_{(2)} + b)(-c\xi_{(3)} + d)(-c\xi_{(4)} + d) \\
&+ (a\xi_{(3)} + b)(a\xi_{(4)} + b)(-c\xi_{(1)} + d)(-c\xi_{(2)} + d) \\
&= a^2d^2(\Phi(\xi)) + b^2c^2(\Phi(\xi)) - 2abcd(\xi_{(1)}\xi_{(3)} + \xi_{(1)}\xi_{(4)} + \xi_{(2)}\xi_{(3)} + \xi_{(2)}\xi_{(4)}) + \lambda \\
&= a^2d^2(\Phi(\xi)) + b^2c^2(\Phi(\xi)) - 2abcd(\xi_{(1)}\xi_{(3)} + \xi_{(1)}\xi_{(4)} + \xi_{(2)}\xi_{(3)} + \xi_{(2)}\xi_{(4)}) + \lambda \\
&+ 2abcd(\Phi(\xi)) - 2abcd(\Phi(\xi)) \\
&= \Phi(\xi)(a^2d^2 + 2adcd + b^2c^2) - 2abcd(\sigma_2(\xi)) + \lambda \\
&= \Phi(\xi)(ad - (-c)b)^2 + \lambda' = (\det A)^2\Phi(\xi) + \lambda'
\end{aligned}$$

for $\lambda, \lambda' \in \mathbb{Z}$. Thus $\Phi(\beta) - \lambda' = \Phi(\xi)$. □

From the calculation in Lemma 3.12, there is a connection between the cubic resolvent forms of monogenizers with a type I relation. Specifically, from Lemma 3.12, we get the following corollary.

Corollary 3.13. *Let $\mathcal{O}$ be a monogenic quartic order with monogenizers β_1 and β_2, and let F_1 and F_2 be the cubic resolvent forms of β_1 and β_2, respectively. If $\beta_1 \sim_1 \beta_2$ then there exists an integer $\lambda \in \mathbb{Z}$ such that*

$$F_2(T_1,T_2) = F_2(T_1 - \lambda T_2, T_2).$$

Recall that if the Galois group of $\mathbb{Z}[\xi]$ is A_4 or S_4 then the cubic resolvent ring is isomorphic to $\mathbb{Z}[\Phi(\xi)]$, and $\mathrm{Im}\Phi \subseteq \mathbb{Z}[\Phi(\xi)]$. In this case, we see using Lemma 3.1 and Lemma 3.12 that for every monogenization $\beta + \mathbb{Z}$ in $\mathcal{S}_\xi(1,0)$, the image $\Phi(\beta + \mathbb{Z})$ will be in the monogenization defined by $\Phi(\xi)$. Thus, we have the following corollary.

Corollary 3.14. *Let $\mathcal{O}$ be a monogenic quartic order with Galois group A_4 or S_4. For monogenizers $\beta, \xi \in \mathcal{O}$, if $\xi \sim_1 \beta$ then $\Phi(\xi) + \mathbb{Z} = \Phi(\beta) + \mathbb{Z}$ in the cubic resolvent ring of $\mathcal{O}$.*

3.5 Examples of Type I Orders

The following is a direct result of Theorem 3.6 and Lemma 3.2.

Corollary 3.15. *Let $H(T_1, T_2)$ be an irreducible monic integral binary quartic form. Then the equation*

$$H(T_1, T_2) = \pm 1 \tag{3.36}$$

has a non-trivial integer solution if and only if the order $\mathbb{Z}[T]/(H(T, 1))$ is of type I.

Proof. Suppose that $H(T_1, T_2)$ is an irreducible monic binary form in $\mathbb{Z}[T_1, T_2]$. Let $f(T) = H(T, 1) \in \mathbb{Z}[T]$, and note that f is irreducible and monic since H is irreducible and monic. Now take $\xi \in \mathbb{C}$ to be a root of f, so f is the minimal polynomial of ξ and H is the minimal form of ξ. By Corollary 3.7, $\mathbb{Z}[\xi]$ is a type I order if and only if there is a non-trivial solution to $H(T_1, T_2) = \pm 1$.
Next, we show that the ring $\mathbb{Z}[T]/(H(T, 1)) = Z[T]/(f(T))$ is isomorphic to $\mathbb{Z}[\xi]$. Consider the map $\varphi : \mathbb{Z}[T] \to Z[\xi]$ defined by the evaluation of polynomials at ξ. Note that $\ker \varphi = (f(T))$, since $f(T)$ is the minimal polynomial of ξ. Observe, also that φ is surjective since φ is a $\mathbb{Z}$-linear map and $\varphi(T^m) = \xi^m$ for any m. Therefore, $\mathbb{Z}[T]/(H(T, 1)) \cong \mathbb{Z}[\xi]$ by the first isomorphism theorem. So $\mathbb{Z}[T]/(H(T, 1))$ will be a type I order if and only if $\mathbb{Z}[\xi]$ is a type I order. □

Corollary 3.15 allows us to provide a simple family of examples.

Example 3.16. Let $f(T) = T^4 + a_1T^3 + a_2T^2 + a_3T + 1 \in \mathbb{Z}[T]$ be irreducible. We can see that $(1, 0)$ and $(0, 1)$ are distinct primitive solutions to

$$H(T_1, T_2) = T_1^4 + a_1T_1^3T_2 + a_2T_1^2T_2^2 + a_3T_1T_2^3 + T_2^3 = \pm 1.$$

Therefore, by Corollary 3.15, $\mathbb{Z}[T]/(f)$ is a type I order.
There are infinitely many polynomials satisfying the above conditions. For example if $a_1, a_2 \equiv 2 \pmod 4$, $a_3 \equiv 0 \pmod 4$ and p is an odd prime then the constant term of $f(T + p)$ will be

$$p^4 + a_1p^3 + a_2p^2 + a_3p + 1 \equiv 1 + a_1 + a_2 + a_3p + 1 \pmod 4$$

$$\equiv 2 \pmod 4,$$

and the other non-leading coefficients will all be even. So, by Eisenstein's criterion, $f(T+p)$ is irreducible, and thus, $f(T)$ is irreducible.

Examples of Type I Orders, Found by Computer Search

For a fixed quartic algebraic integer ξ, we can use a solver from Pari/gp to solve the equation (3.36). This provides a method to check for monogenizations of $\mathbb{Z}[\xi]$, which have a type I relation with ξ. It is important to note that the order $\mathbb{Z}[\xi]$ may still be type I even if ξ does not have a type I relation with any other monogenizer.

Still, to look for type I examples, it is effective to check for a solution to the equation $H_\xi(T_1, T_2) = \pm 1$, where H_ξ is the minimal form of a quartic algebraic integer ξ. In practice, we will search over irreducible quartic integer polynomials whose coefficients are bounded. Although this approach risks producing duplicate orders, as many polynomials can define the same monogenic order, it is computationally straightforward.

In all the following examples, we provide an irreducible quartic polynomial f and look for monogenizations in the order $\mathbb{Z}[\alpha]$, where $\alpha \in \mathbb{C}$ is a root of f, by looking for solutions to the equation $H(T_1, T_2) = T_2^4 f(T_1/T_2) = \pm 1$. Using Corollary 3.7 if $(t_1, t_2) \in \mathbb{Z}^2$ is a solution to $H(T_1, T_2) = \pm 1$ then

$$\alpha_{t_1,t_2} = (t_1^2 + a_1 t_1 t_2 + a_2 t_2^2)\xi + (t_1 t_2 + a_1 t_2^2)\xi^2 + t_2^2 \xi^3 = x\alpha + y\alpha^2 + z\alpha^3$$

defines a monogenization with a type I relation to $\alpha + \mathbb{Z}$. For each ring $\mathbb{Z}[\alpha]$, we will use the basis $\{1, \alpha, \alpha^2, \alpha^3\}$ and report the solutions to $H(T_1, T_2) = \pm 1$ and the corresponding coordinates of the monogenizer with a type I relation to $\alpha + \mathbb{Z}$. Remember that the map from Lemma 3.2 between solutions to $H(T_1, T_2) = \pm 1$ and monogenizations of $\mathbb{Z}[T]/(H(T, 1))$ is a two-to-one map. Thus, we adopt the convention of only presenting solutions with $t_2 \geq 0$, and if $t_2 = 0$, we require $t_1 > 0$. Lastly, we will also provide the discriminant of f to ensure that each example is of a different ring. The examples are shown in 3.1.

3.6 Proof of Theorem 1.14

Suppose that $\mathcal{O}$ is a quartic order, which is two times monogenic. Additionally, suppose that $\mathcal{O}$ is not type I. Let ξ and β be monogenizers of $\mathcal{O}$ such that $\xi + \mathbb{Z} \neq$

$\beta + \mathbb{Z}$ as monogenizations. Because $\mathcal{O}$ is not a type I order, $\xi \not\sim_1 \beta$. Fix the basis for $\mathcal{O}$ of $\{1, \xi, \xi^2, \xi^3\}$, and let$\beta = \lambda + x\xi + y\xi^2 + z\xi^3$. Now by Theorem 3.6 because ξ is not type I to β we must have $\big(Q_1(x,y,z), Q_2(x,y,z)\big) \neq \pm(1,0)$,, for Q_1 and Q_2 defined in (2.49) and (2.50). Since β is a monogenizer of $\mathbb{Z}[\xi]$ and β does not have a type I relations with ξ, the pair $\big(Q_1(x,y,z), Q_2(x,y,z)\big)$ gives a non-trivial integer solution to the cubic equation $F_\xi(T_1, T_2) = \pm 1$, where F_ξ is the cubic resolvent form of ξ.

Now, by Theorem 2.25, the solutions to $F_\xi(T_1, T_2) = \pm 1$ are in bijection with monogenizations to the cubic resolvent ring of $Z[\xi]$. Because $\big(Q_1(x,y,z), Q_2(x,y,z)\big)$ is a nontrivial solution to $F_\xi(T_1, T_2) = \pm 1$, there must be at least two monogenizations of the cubic resolvent ring of ξ. $\square$

$f(T)$	$\mathrm{Disc}(f)$	(t_1, t_2)	(x, y, z)
$T^4 + T^3 + T^2 + T + 1$	125	$(1, 0)$ $(-1, 1)$ $(0, 1)$	$(1, 0, 0)$ $(1, 0, 1)$ $(1, 1, 1)$
$T^4 + 8T^3 - 68T^2 + 53T + 7$	3747127637	$(1, 0)$ $(1, 1)$	$(1, 0, 0)$ $(-59, 9, 1)$
$T^4 - 35T^3 + 31T^2 + 52T + 35$	-62124240383	$(1, 0)$ $(2, 1)$	$(1, 0, 0)$ $(-35, -33, 1)$
$T^4 + 77T^3 - 57T^2 - 27T - 1$	33353306141	$(1, 0)$ $(0, 1)$	$(1, 0, 0)$ $(-57, 77, 1)$
$T^4 - 48T^3 + 68T^2 + 54T - 64$	163234623824	$(1, 0)$ $(-1, 1)$	$(1, 0, 0)$ $(117, -49, 1)$
$T^4 - 17T^3 - 62T^2 + 43T + 88$	50646476489	$(1, 0)$ $(-1, 1)$	$(1, 0, 0)$ $(-44, -18, 1)$
$T^4 - 73T^3 + 73T^2 - 93T + 1$	-908432332075	$(1, 0)$ $(0, 1)$	$(1, 0, 0)$ $(73, -73, 1)$
$T4 + 76T^3 - 72T^2 + 25T - 29$	-644550587163	$(1, 0)$ $(1, 1)$	$(1, 0, 0)$ $(-117, -94, 1)$
$T^4 + 44T^3 - 18T^2 - 64T + 88$	-562365904896	$(1, 0)$ $(3, -2)$	$(1, 0, 0)$ $(-327, 170, 4)$
$T^4 + 138T^3 + 175T^2 - 31T + 1$	191271266897	$(1, 0)$ $(0, 1)$ $(2, 17)$	$(1, 0, 0)$ $(175, 138, 1)$ $(55271, 39916, 289)$
$T^4 - 167T^3 - 217T^2 + 138T - 207$	-1640978513728911	$(1, 0)$ $(2, -1)$	$(1, 0, 0)$ $(121, -169, 1)$
$T^4 + 37T^3 + 188T^2 - 208T + 49$	105372161973	$(1, 0)$ $(3, 5)$	$(1, 0, 0)$ $(5264, 940, 25)$
$T^4 + 25T^3 - 24T^2 - 181T + 2$	421697347425	$(1, 0)$ $(3, 1)$	$(1, 0, 0)$ $(60, 28, 1)$

Table 3.1. Examples of type I quartic orders. Each order is of a unique isomorphism class, since all the given examples have distinct discriminants.

CHAPTER 4

QUARTIC ORDERS OF TYPE II

Let $\mathcal{O}$ be a two-times monogenic quartic order; we will investigate when the order $\mathcal{O}$ is of type II. From definition 1.10 a quartic order is type II if there exists a $\xi, \beta \in \mathcal{O}$, such that

$$\mathbb{Z}[\beta] = \mathbb{Z}[\xi],$$

and

$$\beta = m\xi^2 + k\xi \tag{4.1}$$

and

$$\xi = n\beta^2 + \ell\beta + c, \tag{4.2}$$

with $m, n, k, \ell, c \in \mathbb{Z}$ and $mn \neq 0$. Notice that we are taking $c_0 = 0$ in $\beta = m\xi^2 + k\xi + c_0$, and ξ has been expressed in terms of this β. In addition, we may select one of β or $-\beta$, so that

$$mn > 0.$$

Now substituting (4.1) into (4.2) we have

$$\xi = mn^2\xi^4 + 2kmn\xi^3 + (k^2m + \ell n)\xi^2 + k\ell\xi + c, \tag{4.3}$$

so

$$0 = mn^2\xi^4 + 2kmn\xi^3 + (k^2m + \ell n)\xi^2 + (k\ell - 1)\xi + c. \tag{4.4}$$

Let $P(T) = mn^2T^4 + 2kmnT^3 + (k^2m + \ell n)T^2 + (k\ell - 1)T + c$, note that $P(\xi) = 0$, and P is degree 4. Therefore P is a multiple of $f_\xi(T) = T^4 + a_1T^3 + a_2T^2 + a_3T + a_4$, the minimal polynomial of ξ. Additionally, we observe that nm^2 must divide all the coefficients of P, as f_ξ is monic. Comparing coefficients, we have

$$a_1 = \frac{2kmn}{nm^2} = \frac{2k}{m}, \tag{4.5}$$

$$a_2 = \frac{(k^2m + \ell n)}{nm^2}, \tag{4.6}$$

$$a_3 = \frac{(k\ell - 1)}{nm^2}, \tag{4.7}$$

$$a_4 = \frac{c}{nm^2}. \tag{4.8}$$

Now substituting (4.2) into (4.1) and apply the same reasoning with the minimal polynomial $f_\beta(T) = T^4 + b_1T^3 + b_2T^2 + b_3T + b_4$, we see:

$$b_1 = \frac{2\ell mn}{m^2n} = \frac{2\ell}{m}, \tag{4.9}$$

$$b_2 = \frac{mk + n\ell^2 + 2cnm}{mn^2}, \tag{4.10}$$

$$b_3 = \frac{2m\ell c + k\ell - 1}{mn^2}, \tag{4.11}$$

$$b_4 = \frac{mc^2 + kc}{mn^2}. \tag{4.12}$$

Since $a_i, b_i \in \mathbb{Z}$ for $i = 1, 2, 3, 4$, all the fractions in (4.5) - - (4.12) are integers.

We will argue now that $n = m = \pm 1$ or $n = m = \pm 2$. First, assume that m is odd. Then by (4.5) m divides k. So, from (4.7), we see $0 \equiv \ell k - 1 \equiv -1 \pmod{m}$, thus $m = \pm 1$. Since $m = \pm 1$, (4.6) and (4.7) tell us that $n = \pm 1$. If we assume instead that n is odd, then a similar argument using (4.9), (4.10), and (4.11) shows that $n = \pm 1$ and this implies that $m = \pm 1$. Since we took $nm > 0$ we get $n = m = \pm 1$, if n or m is odd.

Next, assume that $m = 2m'$, then from (4.5), we have that m' divides k. Following the same argument from the odd case, we see that $m' = \pm 1$, thus $n = m = \pm 2$. We have two pairs of minimal polynomials, each depending on ℓ and k. If $m = n = \pm 1$ then

$$f_\xi(T) = T^4 \pm 2kT^3 + (k^2 + \ell)T^2 \pm (\ell k - 1)T \pm c \tag{4.13}$$

and

$$f_\beta(T) = T^4 \pm 2\ell T^3 + (k \pm 2c + \ell^2)T^2 + (2c\ell \pm \ell k \mp 1)T + (c^2 \pm ck). \tag{4.14}$$

If $m = n = \pm 2$ then

$$f_\xi(T) = T^4 \pm kT^3 + \frac{k^2 + \ell}{4}T^2 \pm \frac{k\ell - 1}{8} \pm c \tag{4.15}$$

and

$$f_\beta(T) = T^4 \pm \ell T^3 + \frac{\ell^2 + k \pm 4c}{4}T^2 + \frac{(4c \pm k)\ell \mp 1}{8}T + \frac{2c^2 \pm ck}{8}. \tag{4.16}$$

Next we will show that if ξ and β have minimal polynomials given by (4.13) and (4.14) or, by (4.15) and (4.16) then ξ and β have a type II relation. First, suppose

that the minimal polynomial of ξ is as in (4.13). Then the cubic resolvent form of ξ is

$$\begin{aligned} F_\xi(T_1,T_2) = T_1^3 - (k^2-\ell)T_1^2T_2 + (2k(\ell k-1) - 4a_4)T_1T_2^2 \\ + \big(4a_4(k^2+\ell) - (\ell k-1)^2 - 4k^2a_4\big)\big)T_2^3. \end{aligned} \tag{4.17}$$

Note that $(T_1,T_2) = (1,0)$ and $(T_1,T_2) = (\ell,1)$ are solutions to $F_\xi(T_1,T_2) = \pm 1$. Next, we observe that

$$Q_1(k,1,0) = \ell, \qquad\qquad Q_2(k,1,0) = 1,$$

where Q_1 and Q_2 are defined in (2.49) and (2.50). So, by Proposition 2.33, $\beta = \xi^2 + k\xi$ is a monogenizer of $\mathbb{Z}[\xi]$ and the minimal polynomial of β is as in (4.14). If we take the minimal polynomial of ξ to by as in (4.15), then

$$\begin{aligned} F_\xi(T_1,T_1) = T_1^3 - \frac{k^2+\ell}{4}T_1^2T_2 + \left(\frac{k(\ell k-1)}{8} - a_4\right)T_1T_2^2 \\ + \left(a_4(k^2+\ell) - \left(\frac{\ell k-1}{8}\right)^2 - k^2a_4\right)T_2^3. \end{aligned}$$

We can see that $(T_1,T_2) = (1,0)$ and $(T_1,T_2) = (\ell,4)$ are solutions to $F_\xi(T_1,T_2) = \pm 1$. Additionally,

$$Q_1(k,2,0) = \ell, \qquad\qquad Q_2(k,2,0) = 4.$$

Thus, by Proposition 2.33, $\beta = 2\xi^2 + k\xi$ is a monogenizer of $\mathbb{Z}[\xi]$ and the minimal polynomial of this β will be as in (4.16).

Lastly, we study the index form for $\mathbb{Z}[\beta]$. Thus, we need to show that ξ is a monogenizer of $\mathbb{Z}[\beta]$ and that we do not need β^3 to write ξ in the power basis of β. As above, we follow Proposition 2.33, but we use the minimal polynomial of β, and its coefficients, for the forms $Q_1(X,Y,Z)$, $Q_2(X,Y,Z)$ and $F(T_1,T_2)$. If the minimal polynomial of β is as in (4.14), then we see that

$$Q_1(\ell,1,0) = 2a_4 + k, \qquad\qquad Q_2(\ell,1,0) = 1.$$

Additionally,

$$F(2a_4+k,1) = -1.$$

If the minimal polynomial of β is as in (4.16) then

$$Q_1(\ell,2,0) = 4a_4 + k, \qquad\qquad Q_2(\ell,2,0) = 4,$$

and

$$F(4a_4 + k, 4) = -1.$$

Therefore, $\xi = n\beta^2 + \ell\beta + a_4$ is a monogenizer of $\mathbb{Z}[\beta]$ for $n = \pm 2$ or $n = \pm 1$. It follows that $\mathbb{Z}[\xi]$ is a type II order if and only if the minimal polynomial of ξ is as in (4.13) or (4.15).

4.1 Examples of Type II Quartic Orders

We will provide a few examples of type II orders.

Example 4.1. Consider $k, \ell, c \in \mathbb{Z}$ with $\ell = 1$, $c \equiv 2 \pmod 4$, and $k > 1$ odd. Note that $2k$, $k^2 + 1$, and $k - 1$ are all even. So, by Eisenstein's criterion, the polynomial

$$f(T) = T^4 + 2kT^3 + (k^2 + 1)T^2 + (k - 1)T + c,$$

is irreducible. For ξ a root of f, $\mathbb{Z}[\xi]$ is a type II quartic order. Let

$$\beta = \pm\xi^2 + k\xi,$$

then,

$$\xi = \pm\beta^2 + \beta + c.$$

So ξ and β are monogenizers of $\mathbb{Z}[\xi]$ such that $\beta \sim_2 \xi$.

Example 4.2. In [BEG13] the authers consider polynomials of the form $f(T) = (T^2 - r)^2 - T - s$, with $r, s \in \mathbb{Z}$, such that f is irreducible and has Galois group S_4. They show that if ξ is a root of f, then $\mathbb{Q}(\xi)$ contains infinitely many type II orders. We point out here that even if f does have a Galois group other than S_4, we still see that

$$f(T) = T^4 + 2kT^3 + (k^2 + \ell)T^2 + (\ell k - 1)T + c,$$

for $k = 0$, $\ell = -2r$ and $c = (r^2 - s)$. Thus, by Theorem 1.17, if ξ is a root of f, then $\mathbb{Z}[\xi]$ is a type II order. Furthermore, we see that the monogenizer

$$\beta = \xi^2$$

will define a type II monogenization to $\xi + \mathbb{Z}$, since

$$\xi = \beta^2 - 2r\beta + r^2 - s.$$

CHAPTER 5

ORDERS IN NUMBER FIELDS BY GALOIS GROUP

Let $\mathcal{O}$ be a quartic monogenic order with monogenizer ξ, f_ξ the minimal polynomial of ξ, and let K be the fraction field of $\mathcal{O}$. Additionally, let $\overline{K}$ be the normal closure of K. Then $\overline{K}$ is Galois over $\mathbb{Q}$, and we take $G = \mathrm{Gal}(\overline{K}/\mathbb{Q})$. Recall that we refer to the group G as the Galois group of $\mathcal{O}$. This Chapter will explore the type classification of $\mathcal{O}$ as it relates to the group structure of G. Our approach relies on the fact from Theorem 2.38, which we will demonstrate, that the cubic resolvent polynomial of ξ is reducible if $G = V_4$, C_4, or D_4.

We first need to establish some basic notation and observations. We use the notation $\xi_{(i)}$ for $i = 1, 2, 3, 4$ to represent the algebraic conjugates of ξ. Let r_ξ be the cubic resolvent polynomial of ξ, defined in 2.26. Recall from Section 2.3 the roots of r_ξ over $\mathbb{C}$ are

$$\begin{aligned}\rho_1 &= \xi_{(1)}\xi_{(2)} + \xi_{(3)}\xi_{(4)},\\ \rho_2 &= \xi_{(1)}\xi_{(3)} + \xi_{(2)}\xi_{(4)},\\ \rho_3 &= \xi_{(1)}\xi_{(4)} + \xi_{(2)}\xi_{(3)},\end{aligned}$$

for any fixed ordering of the conjugates of ξ.

In [GPP93] Gaál, Pethő, and Pohst remark that the roots of r_ξ are all distinct since the discriminant of r_ξ equals the discriminant of f_ξ, and the discriminant of f_ξ is non-zero. They go on to say that:

1. $F_\xi(T_1, T_2)$ has three distinct linear factors over $\mathbb{Q}$ if the Galois group of K is V_4;

2. $F_\xi(T_1, T_2)$ has a linear and a quadratic factor over $\mathbb{Q}$ if the Galois group of K is C_4 or D_4.

In Section 5.1 we consider the case where the Galois group of K is V_4, and in Section 5.2 we look at orders in fields with Galois group C_4 or D_4.

5.1 Quartic Orders in Fields With Galois Group V_4

Suppose that the Galois group of K is $G = V_4$. Call the generators of G, σ_1 and σ_2. Let $\xi \in \mathcal{O}_K$ and suppose that $K = \mathbb{Q}(\xi)$. Since ξ is a primitive element of

K, the Galois group of K acts transitively on the set of conjugates of ξ. Denote the cubic resolvent polynomial of ξ by r_ξ. Note that

$$r_\xi(T) = (T - \rho_1)(T - \rho_2)(T - \rho_3).$$

Since K is Galois all the conjugates of $\xi \in K$, thus we also have that $\rho_1, \rho_2, \rho_3 \in K$. We will show that, in fact, each $\rho_i \in \mathbb{Z}$ for $i = 1, 2, 3$. First, index the conjugates of ξ so that $\xi = \xi_{(1)}$ and

$$\sigma_1(\xi_{(1)}) = \xi_{(2)} \qquad \sigma_2(\xi_{(1)}) = \xi_{(3)} \qquad \sigma_1\sigma_2(\xi_{(1)}) = \xi_{(4)}.$$

So we can write each of the ρ_i for $i = 1, 2, 3$ in terms of the action of G on the conjugates of ξ. Specifically we have

$$\begin{aligned}
\rho_1 =& \xi\sigma_1(\xi) + \sigma_2(\xi)\sigma_1\sigma_2(\xi) \\
\rho_2 =& \xi\sigma_2(\xi) + \sigma_1(\xi)\sigma_1\sigma_2(\xi) \\
\rho_3 =& \xi\sigma_1\sigma_2(\xi) + \sigma_1(\xi)\sigma_2(\xi)
\end{aligned}$$

Using this identification, we can easily compute the action of G on the ρ_i for $i = 1, 2, 3$. Now, we see how the generators of V_4 act on the ρ_i for $i = 1, 2, 3$. Consider the following

$$\begin{aligned}
\sigma_1(\rho_1) =& \sigma_1\left(\xi\sigma_1(\xi) + \sigma_2(\xi)\sigma_1\sigma_2(\xi)\right) \\
=& \sigma_1(\xi)\sigma_1^2(\xi) + \sigma_1\sigma_2(\xi)\sigma_1^2\sigma_2(\xi) \\
=& \sigma_1(\xi)\xi + \sigma_1\sigma_2(\xi)\sigma_2(\xi) \\
=& \rho_1
\end{aligned}$$

and,

$$\begin{aligned}
\sigma_2(\rho_1) =& \sigma_2\left(\xi\sigma_1(\xi) + \sigma_2(\xi)\sigma_1\sigma_2(\xi)\right) \\
=& \sigma_2(\xi)\sigma_1\sigma_2(\xi) + \sigma_2^2(\xi)\sigma_1\sigma_2^2(\xi) \\
=& \sigma_2(\xi)\sigma_1\sigma_2(\xi) + \xi\sigma_1(\xi) \\
=& \rho_1.
\end{aligned}$$

For ρ_2 we see,

$$\begin{aligned}
\sigma_1(\rho_2) =& \sigma_1\left(\xi\sigma_2(\xi) + \sigma_1(\xi)\sigma_1\sigma_2(\xi)\right) \\
=& \sigma_1(\xi)\sigma_1\sigma_2(\xi) + \sigma_1^2(\xi)\sigma_1^2\sigma_2(\xi)
\end{aligned}$$

$$\begin{aligned}
&= \sigma_1(\xi)\sigma_1\sigma_2(\xi) + \xi\sigma_2(\xi) \\
&= \rho_2,
\end{aligned}$$

and,

$$\begin{aligned}
\sigma_2(\rho_2) &= \sigma_2\left(\xi\sigma_2(\xi) + \sigma_1(\xi)\sigma_1\sigma_2(\xi)\right) \\
&= \sigma_2(\xi)\sigma_2^2(\xi) + \sigma_1\sigma_2(\xi)\sigma_1\sigma_2^2(\xi) \\
&= \sigma_2(\xi)\xi + \sigma_1\sigma_2(\xi)\sigma_1(\xi) \\
&= \rho_2.
\end{aligned}$$

Therefore, ρ_1 and ρ_2 are in the subfield of K fixed by G and thus by the Fundamental Theorem of Galois Theory, $\rho_1, \rho_2 \in \mathbb{Q}$. Now $r_\xi(T)$ is a degree 3 polynomial over $\mathbb{Z}$ that has 2 rational roots. Thus, the extension $\mathbb{Q}[T]/(r_\xi(T))$ is degree 1 and we see that ρ_3 is also in $\mathbb{Q}$.

Since $\xi \in \mathcal{O}_K$ and K are Galois, we know that the conjugates of ξ are also algebraic integers. Thus $\rho_i \in \mathcal{O}_K$ for $i = 1, 2, 3$. So $\rho_i \in \mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}$, for $i = 1, 2, 3$. This demonstrates that the cubic resolvent polynomial $r_\xi(T)$ is completely reducible over $\mathbb{Z}$.

Now we turn to studying the monogenizations of $\mathbb{Z}[\xi]$ using Proposition 2.33. First, we focus on the solution to the equation $F_\xi(T_1, T_2) = \pm 1$, where F_ξ is the cubic resolvent form of ξ. Since $r_\xi(T)$ splits over $\mathbb{Z}$, solving $F_\xi(T_1, T_2) = \pm 1$ is equivalent to solving the linear system

$$T_1 - \rho_1 T_2 = \delta_1, \tag{5.1}$$

$$T_1 - \rho_2 T_2 = \delta_2, \tag{5.2}$$

$$T_1 - \rho_3 T_2 = \delta_3, \tag{5.3}$$

where $\delta_i \in \{1, -1\}$ for $i = 1, 2, 3$.

To begin studying this system, observe that all three linear equations above represent distinct lines. This indicates that the system of equations given by (5.1), (5.2), and (5.3) can have one or zero solutions for each of the possible values of the δ_i, $i = 1, 2, 3$. If $(t_1, t_2) \in \mathbb{Z}^2$ is a solution to the system with δ values $(\delta_1, \delta_2, \delta_3)$ then $-(t_1, t_2)$ will be a solution to the system for the δ values $-(\delta_1, \delta_2, \delta_3)$. Therefore, we need only look at triples of the δ with $\delta_1 = 1$. There are four cases defined by $(\delta_1, \delta_2, \delta_3) = (1, 1, 1)$, $(1, -1, 1)$, $(1, 1, -1)$, and $(1, -1, -1)$.

If $(\delta_1, \delta_2, \delta_3) = (1, 1, 1)$ then we have the trivial solution $(t_1, t_2) = (1, 0)$. In every other case, at least one of δ_2 or δ_3 will be negative, so $(t_1, t_2) = (1, 0)$ will not be a solution to the system (5.1), (5.2) and (5.3). Thus, if exactly one of δ_2 or δ_3 is negative, then there are no solutions with $T_2 = 0$. Suppose that $\delta_2 = -\delta_3$. Without loss of generality we assume that $\delta_2 = 1$, the system becomes

$$T_1 - \rho_1 T_2 = 1, \tag{5.4}$$

$$T_1 - \rho_2 T_2 = 1, \tag{5.5}$$

$$T_1 - \rho_3 T_2 = -1. \tag{5.6}$$

Now subtracting (5.5) from (5.4) gives

$$(\rho_2 - \rho_1) T_2 = 0. \tag{5.7}$$

Since $T_2 \neq 0$ and all the ρ_i are distinct, there is no solution to (5.7). Therefore, there is no solutions to the system (5.1) – (5.3) when $\delta_2 = -\delta_3$. A completely analogous argument applies to the case of $\delta_2 = \delta_3 = -1$. Therefore the only solution to $F_\xi(T_1, T_2) = \pm 1$ is the trivial solution $(\pm 1, 0)$. We have thus proven the following lemma.

Lemma 5.1. *If ξ is a quartic algebraic integer and $\mathbb{Q}(\xi)$ has Galois group V_4, then $\pm(1, 0)$ is the only integer solution to the equation*

$$F_\xi(T_1, T_2) = \pm 1,$$

where $F_\xi(T, 1)$ is the cubic resolvent polynomial of ξ.

Together with Lemma 5.1 and Theorem 3.6, we have the following result.

Theorem 5.2. *Let $\mathcal{O}$ be a quartic monogenic order which is two times monogenic. If the field of fraction of $\mathcal{O}$ has Galois group V_4, then $\mathcal{O}$ is a type I order.*

Examples in Bi-quadratic Fields

One of the most studied examples of quartic number fields is the bi-quadratic fields.

Definition 5.3. A *bi-quadratic number field* is a field extension of $\mathbb{Q}$ of the form $\mathbb{Q}(\sqrt{a}, \sqrt{b})$ for a and b distinct squarefree integers.

If $\ell = \gcd(a,b)$, $a_1 = a/\ell$, and $K = \mathbb{Q}(\sqrt{a},\sqrt{b})$ then the set $\{1,\sqrt{a},\sqrt{b},\sqrt{a_1 b_1}\}$ is a $\mathbb{Q}$-basis for K. The field K can be generated by the element $\sqrt{a}+\sqrt{b}$. The minimal polynomial of $\sqrt{a}+\sqrt{b}$ is

$$f(T) = T^4 - 2(a+b)T^2 + (a-b)^2, \tag{5.8}$$

and its roots are

$$\sqrt{a}+\sqrt{b}, \qquad -\sqrt{a}+\sqrt{b}, \qquad \sqrt{a}-\sqrt{b}, \qquad -\sqrt{a}-\sqrt{b}.$$

Thus K is the splitting field of $f(T) = T^4 - 2(a+b)T^2 + (a-b)^2$, and therefore K is Galois with Galois group V_4.

The order $Z[\sqrt{a}+\sqrt{b}]$ is monogenic, and the minimal polynomial of $\sqrt{a}+\sqrt{b}$ is given in 5.8. So the minimal form of $\sqrt{a}+\sqrt{b}$ is

$$H(T_1,T_2) = T_1^4 - 2(a+b)T_1^2T_2^2 + (a-b)^2T_2^4. \tag{5.9}$$

Since $\mathcal{O} = Z[\sqrt{a}+\sqrt{b}]$ is an order in a biquadratic field, the Galois group of $\mathcal{O}$ is V_4. Therefore, by Theorem 5.2, if $\mathcal{O}$ is two times monogenic, then it is of type I.

We now provide a family of two times monogenic quartic orders whose field of fractions are bi-quadratic number fields. From (5.9) if $|a-b| = 1$, then $H(1,0) = \pm 1 = H(0,1)$. Thus by Corollary 3.7 $Z[\sqrt{a}+\sqrt{b}]$ is a type I order with

$$(\sqrt{a}+\sqrt{b}) \sim_1 -2(a+b)(\sqrt{a}+\sqrt{b}) + (\sqrt{a}+\sqrt{b})^3.$$

If a is a non-zero integer, then $\gcd(a,a+1) = 1$ and since there is infinitely many integers $a > 0$ such that a and $a+1$ are squarefree, there are infinitely many orders $\mathbb{Z}[\sqrt{a}+\sqrt{a+1}]$ that are of type I.

5.2 Quartic Orders in Fields With Galois Group C_4 or D_4

Suppose that K is a quartic number field with normal closure $\overline{K}$. Let $G = \mathrm{Gal}(\overline{K}/\mathbb{Q}) = C_4$ or D_4, with generators $\langle \sigma | \sigma^4 = e\rangle = C_4$ or $\langle \sigma,\tau | \sigma^4 = \tau^2 = (\sigma\tau)^4 = e\rangle = D_4$. Let $\xi \in \mathcal{O}_K$ be such that $\mathbb{Q}(\xi) = K$. Also, let f_ξ be the minimal polynomial of ξ and r_ξ be the cubic resolvent polynomial of ξ. Label the conjugates of ξ such that

$$\xi = \xi_{(1)} \qquad \xi_{(2)} = \sigma(\xi) \qquad \xi_{(3)} = \sigma^2(\xi) \qquad \xi_{(4)} = \sigma^3(\xi).$$

Then the action of τ is defined by $\tau(\xi_{(2)}) = \xi_{(4)}$ and $\tau(\xi_{(j)}) = \xi_{(j)}$ for $j = 1, 3$. This allows us to express the roots of r_ξ as

$$\begin{aligned}\rho_1 =& \xi\sigma(\xi) + \sigma^2(\xi)\sigma^3(\xi),\\ \rho_2 =& \xi\sigma^2(\xi) + \sigma(\xi)\sigma^3(\xi),\\ \rho_3 =& \xi\sigma^3(\xi) + \sigma(\xi)\sigma^2(\xi)\end{aligned}$$

Using this identification, we can efficiently compute the action of G on the ρ_i for $i = 1, 2, 3$. Examining how σ acts on the ρ_i, for $i = 1, 2, 3$ we see that

$$\begin{aligned}\sigma(\rho_1) =& \sigma\left(\xi\sigma(\xi) + \sigma^2(\xi)\sigma^3(\xi)\right)\\ =& \sigma(\xi)\sigma^2(\xi) + \sigma^3(\xi)\xi\\ =& \rho_3.\end{aligned}$$

For ρ_2 we see,

$$\begin{aligned}\sigma(\rho_2) =& \sigma\left(\xi\sigma^2(\xi) + \sigma(\xi)\sigma^3(\xi)\right)\\ =& \sigma(\xi)\sigma^3(\xi) + \sigma^2(\xi)\xi\\ =& \rho_2.\end{aligned}$$

Next examining the action of τ on the ρ_i we see that

$$\tau(\rho_1) = \tau\left(\xi_{(1)}\xi_{(2)} + \xi_{(3)}\xi_{(4)}\right) = \xi_{(1)}\xi_{(4)} + \xi_{(3)}\xi_{(2)} = \rho_3,$$

and

$$\tau(\rho_2) = \tau\left(\xi_{(1)}\xi_{(3)} + \xi_{(2)}\xi_{(4)}\right) = \xi_{(1)}\xi_{(3)} + \xi_{(4)}\xi_{(2)} = \rho_2.$$

Note that $\rho_i \in \mathcal{O}_{\overline{K}}$ for $i = 1, 2, 3$ since $\overline{K}$ is Galois over $\mathbb{Q}$. Then, from our calculation and the Fundamental Theorem of Galois Theory, we have that ρ_2 is in the fixed field of G, that is $\rho_2 \in \mathbb{Q} \cap \mathcal{O}_{\overline{K}} = \mathbb{Z}$. Additionally, ρ_1 and ρ_3 are algebraic integers in the unique quadratic subfield fixed by the group $\langle\sigma^2\rangle$ if $G = C_4$ or $\langle\sigma^2, \tau\rangle$ if $G = D_4$.

Now the cubic resolvent polynomial of ξ is reducible over $\mathbb{Q}$ as the product of a linear polynomial and an irreducible quadratic.

Lemma 5.4. *Let ξ be a monogenizer in a quartic order with Galois group D_4 or C_4. Then the cubic resolvent polynomial of ξ, defined in 2.27, is reducible over $\mathbb{Q}$ and has three distinct roots over $\mathbb{C}$.*

Theorem 5.5. *Let $G = D_4$ or C_4. Then there are at most finitely many isomorphism classes of two times monogenic quartic orders $\mathcal{O}$ such that the fraction field of $\mathcal{O}$ has Galois group G,* $\mathrm{Disc}(\mathcal{O}) < 0$*, and $\mathcal{O}$ is not type I.*

Proof. Suppose that $\mathcal{O}$ is a two time monogenic order with Galois group $G = C_4$ or D_4 and that $\mathcal{O}$ is not type I. Let ξ be any monogenizer of $\mathcal{O}$. Note that $\mathrm{Disc}(\xi) = \mathrm{Disc}(\mathcal{O})$. Denote the cubic resolvent form of ξ by F_ξ. By Proposition 2.33 and Theorem 3.6 since $\mathcal{O}$ is not type I the equation

$$F_\xi(T_1, T_2) = \pm 1 \tag{5.10}$$

has at least two primitive solutions. Let N_ξ be the number of primitive solutions to (5.10). By Lemma 5.4 the polynomial $F_\xi(T_1, 1)$ is reducible, with three distinct roots over $\mathbb{C}$. Since $\mathrm{Disc}(F_\xi) < 0$ and $N_\xi \geq 2$ we must have, by Proposition 2.9, that $N_\xi = 2$ and $\mathrm{Disc}(F_\xi) > -27$. Recall that

$$\mathrm{Disc}(F_\xi) = \mathrm{Disc}(\xi) = \mathrm{Disc}(\mathcal{O}) < 0.$$

So $-27 \geq \mathrm{Disc}(\xi) < 0$. Now, by Corollary 2.6, the set

$$M = \{\alpha + \mathbb{Z} : 0 > \mathrm{Disc}(\alpha) \geq -27 \text{ and } \alpha \in \overline{\mathbb{Q}}\}$$

where $\overline{\mathbb{Q}}$ is a fixed algebraic closer of $\mathbb{Q}$, is finite. Let M_4 be the subset of M defined by $M_4 = \{\alpha + \mathbb{Z} \in M : \deg(\alpha) = 4\}$. If $\mathcal{O}$ is a quartic monogenic order $\mathcal{O}$ satisfying all the condition below then every monogenization of $\mathcal{O}$ is in M_4:

1. $\mathrm{Disc}(\mathcal{O}) < 0$.
2. $\mathcal{O}$ is two times monogenic.
3. $\mathcal{O}$ has Galois group C_4 or D_4.

The number of isomorphism classes of two times monogenic order satisfying condition (1)-(3) above is at most $|M_4|$, which is finite. □

Theorem 5.5 addresses the case of orders with negative discriminant. For positive discriminant, Proposition 2.9 can not be used. However, using elementary methods, we can still provide some restrictions on two times monogenic quartic orders that are not type I.

Suppose that $\mathcal{O}$ is a monogenic quartic order with monogenizer ξ, and the Galois group of $\mathcal{O}$ is C_4 or D_4. Let $f_\xi(T) = T^4 + a_1T^3 + a_2T^2 + a_3T + a_4$, then

$$\begin{aligned} r_\xi(T) =& T^3 - a_2T^2 + (a_1a_3 - 4a_4)T + (4a_2a_4 - a_3^2 - a_1^2a_4) \\ =& (T - \rho_2)(T^2 - (\rho_1 + \rho_3)T + \rho_1\rho_2). \end{aligned} \tag{5.11}$$

We take $F_\xi(T_1, T_2)$ to be the cubic resolvent form of ξ. From Proposition 2.33, to find the monogenizations of $Z[\xi]$, we first solve $F_\xi(T_1, T_2) = \pm 1$. By our work above for Lemma 5.4, solving the equation $F_\xi(T_1, T_2) = \pm 1$ in this case is equivalent to solving the system of equations

$$T_1 - \rho_2T_2 = \delta_1, \tag{5.12}$$

$$T_1^2 - (\rho_1 + \rho_3)T_1T_2 + \rho_1\rho_3T_2^2 = \delta_2, \tag{5.13}$$

where $\delta_1, \delta_2 \in \{1, -1\}$. Since ρ_1 and ρ_3 are conjugate quadratic integers the equation,

$$\pm 1 = T_1^2 - (\rho_1 + \rho_3)T_1T_2 + \rho_1\rho_3T_2^2 \tag{5.14}$$

$$= (T_1 - \rho_1T_2)(T_1 - \rho_3T_2) \tag{5.15}$$

holds. Therefore, any $(t_1, t_2) \in \mathbb{Z}^2$ solving the system of equations (5.12) and (5.13) will give a pair of quadratic units $(t_1 - \rho_1t_2)$ and $(t_1 - \rho_3t_2)$ such that

$$(t_1 - \rho_3t_2) = \pm(t_1 - \rho_1t_2)^{-1} \tag{5.16}$$

as elements of $\mathbb{Q}(\rho_1)$.

Remark 5.6. The algebraic integers ρ_1 and ρ_3 are algebraic quadratic conjugates since they are the roots of the polynomial $T^2 - (\rho_1 + \rho_3)T + (\rho_1\rho_2)$. Thus, $\rho_3 \in \mathbb{Q}(\rho_1)$ since $\mathbb{Q}(\rho_1)$ is a quadratic number field.

We have thus established the following theorem.

Theorem 5.7. *Let K be a quartic number field with Galois group C_4 or D_4. Also, let $\xi \in \mathcal{O}_k$ be such that $K = \mathbb{Q}(\xi)$. If $\mathbb{Z}[\xi]$ is a two times monogenic order then, $\mathbb{Z}[\xi]$ is type I or, the equation $F_\xi(T_1, T_2) = \pm 1$ has a solution (t_1, t_2) such that*

$$t_1 - (\xi_{(1)}\xi_{(3)} + \xi_{(2)}\xi_{(4)})t_2$$

is a quadratic unit with inverse

$$\pm(t_1 - (\xi_{(1)}\xi_{(4)} + \xi_{(2)}\xi_{(3)})t_2).$$

Where the $\xi_{(i)}$ for $i = 1, 2, 3, 4$ are the algebraic conjugates of ξ.

In addition to Theorem 5.7, we can find two inequalities that can be used to determine if no solutions to the system of equations (5.12) and (5.13) exist. Using substitution, we can reduce this system to a single quadratic equation

$$(\rho_2 - \rho_1)(\rho_2 - \rho_3)T_2^2 - \delta_1(2\rho_2 + \rho_1 + \rho_3)T_2 + (1 - \delta_2) = 0. \tag{5.17}$$

We examine the cases based on the values of δ_1 and δ_2. First, suppose that $\delta_2 = 1$. Then (5.17) reduces to

$$0 = T_2\left((\rho_2 - \rho_1)(\rho_2 - \rho_3)T_2 - \delta_1(2\rho_2 + \rho_1 + \rho_3)\right).$$

From this, we have two solutions over $\mathbb{Q}$. The first is $(T_1, T_2) = (\delta_1, 0)$; the second is

$$T_2 = \pm\frac{2\rho_2 + \rho_1 + \rho_3}{(\rho_2 - \rho_1)(\rho_2 - \rho_3)}.$$

and

$$T_1 = \pm 1 - \rho_2 T_2.$$

Now we check the cases with $\delta_2 = -1$. We get the following quadratic equation in T_2:

$$0 = (\rho_2 - \rho_1)(\rho_2 - \rho_3)T_2^2 - \delta_1(2\rho_2 + \rho_1 + \rho_3)T_2 + 2. \tag{5.18}$$

Since (5.18) is a quadratic equation with integer coefficients, it can only have rational solutions if the discriminant of the polynomial

$$(\rho_2 - \rho_1)(\rho_2 - \rho_3)T_2^2 - \delta_1(2\rho_2 + \rho_1 + \rho_3)T_2 + 2 \tag{5.19}$$

is a square in $\mathbb{Z}$. So for a solution to $F_\xi(T_1, T_2) = \pm 1$ to exist either

$$\frac{2\rho_2 + \rho_1 + \rho_3}{(\rho_2 - \rho_1)(\rho_2 - \rho_3)} \in \mathbb{Z} \tag{5.20}$$

or

$$\left((2\rho_2 + \rho_1 + \rho_3)^2 - 8(\rho_2 - \rho_1)(\rho_2 - \rho_3)\right)^{1/2} \in \mathbb{Z}. \tag{5.21}$$

Weaker conditions than (5.20) or (5.21) are simply that,

$$\left|(\rho_2 - \rho_1)(\rho_2 - \rho_3)\right| \leq \left|2\rho_2 + \rho_1 + \rho_3\right|. \tag{5.22}$$

or

$$8(\rho_2 - \rho_1)(\rho_2 - \rho_3) \leq (2\rho_2 + \rho_1 + \rho_3)^2 \tag{5.23}$$

We record our observation as a lemma below.

Lemma 5.8. *Let $\mathcal{O}$ be a two times monogenic order with Galois group D_4 or C_4. Then either $\mathcal{O}$ is of type I, or there exists a monogenizer $\xi \in \mathcal{O}$ satisfying at least one of the following inequalities:*

1.

$$\begin{aligned}&\left|(\xi_{(1)} - \xi_{(2)})(\xi_{(1)} - \xi_{(4)})(\xi_{(2)} - \xi_{(3)})(\xi_{(3)} - \xi_{(4)})\right| \\ &\leq \left|2(\xi_{(1)}\xi_{(3)} - \xi_{(2)}\xi_{(4)}) + (\xi_{(1)} + \xi_{(3)})(\xi_{(2)} + \xi_{(4)})\right|\end{aligned}$$

2.

$$\begin{aligned}&8(\xi_1 - \xi_2)(\xi_1 - \xi_4)(\xi_2 - \xi_3)(\xi_3 - \xi_4) \\ &\leq \left(2(\xi_{(1)}\xi_{(3)} - \xi_{(2)}\xi_{(4)}) + (\xi_1 + \xi_3)(\xi_2 + \xi_4)\right)^2.\end{aligned}$$

Examples

We will address some simple examples of polynomials whose Galois groups are D_4 or C_4.

Example 5.9. Let $n \in \mathbb{Z}$ be squarefree and $n > 0$. Consider the polynomial $f(T) = T^4 - n$. Let $i = \sqrt{-1}$ then the roots of f are

$$r_0 = n^{1/4} \qquad r_1 = in^{1/4} \qquad r_2 = -n^{1/4} \qquad r_3 = -in^{1/4}.$$

So the splitting field of f is $K = \mathbb{Q}(i, n^{1/4})$. The Galois group $\mathrm{Gal}(K/\mathbb{Q})$ is generated by the maps

$$\sigma : n^{1/4} \mapsto in^{1/4} \qquad\qquad \tau : i \mapsto -i.$$

Consider that

$$\sigma(n^{1/4}) = in^{1/4} \quad \sigma^2(n^{1/4}) = -n^{1/4} \quad \sigma^3(n^{1/4}) = -in^{1/4} \quad \sigma^4(n^{1/4}) = n^{1/4},$$

and

$$\tau(i) = -i \qquad\qquad \tau^2(i) = i.$$

So τ has order 2 and σ has order 4. Lastly, we note that $\tau\sigma\tau = \sigma^3 = \sigma^{-1}$. Therefore, $\mathrm{Gal}(K/\mathbb{Q}) \cong D_4$. Now, let $\xi = n^{1/4}$. We will show that $\mathbb{Z}[\xi]$ is exactly one time monogenic or it is type I. The cubic resolvent form of ξ is $F_n(T_1, T_2) = T_1^3 -$

$4nT_1T_2^2 = T_1(T_1^2 - 4nT_2^2)$. Following Proposition 2.33, we need to find the solutions to $F_n(T_1, T_2) = \pm 1$. Since F_n is reducible the solutions to $F_n(T_1, T_2) = \pm 1$ are given by the solutions to the system,

$$\begin{aligned} T_1 =& \delta_1 \\ T_1^2 - 4nT_2^2 =& \delta_2 \end{aligned}$$

where $\delta_1, \delta_2 \in \{1, -1\}$. Consider that,

$$\begin{aligned} \rho_1 =& (n^{1/4})(in^{1/4}) + (-n^{1/4})(-in^{1/4}) = 2in^{1/2} \\ \rho_2 =& (n^{1/4})(-n^{1/4}) + (in^{1/4})(-in^{1/4}) = -n^{1/2} + n^{1/2} = 0 \\ \rho_3 =& (n^{1/4})(-in^{1/4}) + (-n^{1/4})(in^{1/4}) = -in^{1/2} - in^{1/2} = -2in^{1/2}. \end{aligned}$$

From our work above, if $\delta_2 = 1$ then the only possible solution is $(t_1, t_2) = (\pm 1, 0)$. If $\delta_2 = -1$ then

$$\begin{aligned} & ((2)\rho_2 + \rho_1 + \rho_3)^2 - 8(\rho_2 - \rho_1)(\rho_2 - \rho_3) \\ =& (0 + 2in^{1/2} - 2in^{1/2}) - 8(0 - 2in^{1/2})(0 + 2in^{1/2}) \\ =& 32i^2n = -32n < 0. \end{aligned}$$

So, there is no solution to the equation

$$0 = (\rho_2 - \rho_1)(\rho_2 - \rho_3)T_2^2 - \delta_1(2\rho_2 + \rho_1 + \rho_3)T_2 + 2.$$

Therefore, there are no rational solutions with $\delta_2 = -1$. Thus the only solutions to $F_n(T_1, T_2) = \pm 1$ are $(\pm 1, 0)$. By Theorem 3.6 and Corollary 3.7, the monogenizations in $\mathcal{S}_\xi(1, 0)$ are given by the solutions to the equation

$$T_1^4 - nT_2^4 = \pm 1. \tag{5.24}$$

Suppose that $n = m^4 \pm 1$ for $m \in \mathbb{Z}$ and $m \neq 0$. Note that infinitely many integers of the form $m^4 \pm 1$ will be squarefree. So, $(1, 0)$ and $(m, 1)$ will be solutions to (5.24). This establishes an infinite family of D_4 orders which are type I.

Example 5.10. Let ζ be a primitive fifth root of unity and let $n \in \mathbb{Z}$, $|n| > 1$. We can see that $K = \mathbb{Q}(n\zeta) = \mathbb{Q}(\zeta)$ for all $n \in \mathbb{Z}$. Consider the ring $R_n = \mathbb{Z}[n\zeta]$. Note that $[R_n^+ : \mathbb{Z}[\zeta]^+] = n$ so $\zeta \notin R_n$. Thus, there is no unit u in R_n such that $u^5 = 1$. It follows that R_n is not isomorphic to $\mathbb{Z}[\zeta]$ as a ring. Now, we will examine the

monogenizations of R_n. Let σ be the generator of $\mathrm{Gal}(K/\mathbb{Z})$, defined by $\sigma(\zeta) = \zeta^2$. Following our work above, we number the conjugate of $n\zeta$ as

$$\begin{aligned} \xi_{(1)} =& n\zeta, & \xi_{(2)} &= \sigma(n\zeta) = n\zeta^2, \\ \xi_{(3)} =& \sigma^2(n\zeta) = n\sigma(\zeta^2) = n\zeta^4, & \xi_{(4)} &= \sigma^3(n\zeta) = n\sigma(\zeta^4) = n\zeta^8 = n\zeta^3. \end{aligned}$$

So we have

$$\begin{aligned} \rho_1 =& r_0r_1 + r_2r_3 = n^2(\zeta^3 + \zeta^2), \\ \rho_2 =& r_0r_2 + r_1r_3 = n^2(1+1) = 2n^2, \\ \rho_3 =& r_0r_3 + r_1r_2 = n^2(\zeta^4 + \zeta_1). \end{aligned}$$

Next consider,

$$\rho_1 + \rho_3 = n^2(\zeta^4 + \zeta^3 + \zeta^2 + \zeta) = -n^2$$

and

$$\rho_1\rho_3 = n^4(\zeta^7 + \zeta^6 + \zeta^4 + \zeta^3) = n^4\zeta^3(\zeta^4 + \zeta^3 + \zeta + 1) = n^4\zeta^3(-\zeta^2) = -n^4.$$

So if $F_n(T_1, T_2)$ is the cubic resolvent form of $n\zeta$ then the solutions to $F_n(T_1, T_2) = \pm 1$ are given by the solutions to the system

$$\begin{aligned} T_1 - 2n^2T_2 &= \delta_1, \\ T_1^2 + n^2T_1T_2 - n^4T_2^2 &= \delta_2, \end{aligned}$$

where $\delta_1, \delta_2 \in \{1, -1\}$. If $\delta_2 = 1$ then $(1, 0)$ will be a solution. Checking the other possible value for T_2 from (5.17) we have

$$T_2 = \pm\frac{2\rho_2 + \rho_1 + \rho_3}{(\rho_2 - \rho_1)(\rho_2 - \rho_3)} = \frac{3n^2}{5n^4} < 1 \tag{5.25}$$

for all $n \in \mathbb{Z}$. So the only solutions with $\delta_2 = 1$ are $\pm(1, 0)$. Examining $\delta_2 = -1$ we note that

$$(2\rho_2 + \rho_1 + \rho_3)^2 - 8(\rho_2 - \rho_1)(\rho_2 - \rho_3) = 9n^4 - 8(4n^4) = -23n^4 < 0. \tag{5.26}$$

So, there are no integer solutions to the system of equations with $\delta_2 = -1$. Therefore, the only solution to $F_\xi(T_1, T_2) = \pm 1$ is the trivial solution. From Theorem 3.6, it follows that if R_n is a two times monogenic order, then it is type I. However, the minimal polynomial of $n\zeta$ is

$$f_{n\zeta}(T) = T^4 + nT^3 + n^2T^2 + n^3T + n^4 = H_\zeta(T, n), \tag{5.27}$$

where $H_\zeta(T_1, T_2)$ is the minimal form of ζ. So we have,

$$T_2^4 f_{n\zeta}(T_1/T_2) = H_\zeta(T_1, nT_2) \tag{5.28}$$

is satisfied. Let $Y_1 = T_1$ and $Y_2 = nT_2$. Then from Table 3.1 in section 3.5, all the integer solutions to $H_\zeta(Y_1, Y_2) = \pm 1$ have $Y_2 = \pm 1$. Thus the only solutions $H_\zeta(T_1, nT_2) = \pm 1$ have $nT_2 = \pm 1$. It follows that $T_2^4 f_{n\zeta}(T_1/T_2) = \pm 1$ will have only the trivial solution $\pm(1, 0)$ unless $n = \pm 1$. Therefore, if $|n| > 1$, the order $\mathcal{O}_n$ will be exactly one time monogenic by Proposition 2.33.

CHAPTER 6

EXCEPTIONAL QUARTIC ORDERS

Let ξ be a quartic algebraic integer and $K = \mathbb{Q}(\xi)$. Bérczes, Evertse, and Győry in [BEG13] prove that, if K is a number field with Galois group S_4, then all but finitely many two times monogenic orders are not type I or type II. However, [BEG13] does not have any examples of orders that are not type I or type II. In this section, we present several examples of two times monogenic orders that are neither type I nor type II. We will include examples from fields with Galois group C_4, D_4, and A_4, among the examples of exceptional orders.

Definition 6.1. A two times quartic monogenic order is an *exceptional* order if it is not type I or type II.

In Proposition 2.33, we see that the monogenizations of a monogenic ring $\mathbb{Z}[\xi]$ can be separated into subsets by the solutions to the equation

$$F_\xi(T_1, T_2) = \pm 1, \tag{6.1}$$

where $F_\xi(T, 1)$ is the cubic resolvent polynomial of ξ defined in 2.26.

Definition 6.2. Let $A \subseteq \mathbb{Z}^2$ be the set of solutions to (6.1). For each $p \in A$ we have a subset of monogenizations $\mathcal{S}_\xi(p)$, defined in 2.34. Define the *monogenic signature* of $\mathbb{Z}[\xi]$ to be the multiset

$$\{|S_\xi(p)| : p \in A\}.$$

A short corollary to Theorem 3.6 will help determine if a monogenic quartic order is not type I.

Corollary 6.3. *Suppose that $\mathcal{O}$ is a monogenic quartic order. If the monogenic signature of $\mathcal{O}$ is $\{1, 1\}$ then $\mathcal{O}$ is not type I.*

Proof. Suppose that $\mathcal{O}$ is a quartic monogenic order with monogenic signature $\{1, 1\}$. Then $\mathcal{O}$ is exactly two times monogenic, so $\mathcal{O}$ can only be type I if its two monogenizations have a type I relation. Let $\xi+\mathbb{Z}$ and $\beta+\mathbb{Z}$, be the monogenizations of $\mathcal{O}$. Since the monogenic signature is $\{1, 1\}$ the size of the subset of all monogenizations $\mathcal{S}_\xi(1, 0)$ must be 1. Therefore, $\beta + \mathbb{Z} \notin \mathcal{S}_\xi(1, 0)$ so $\beta + \mathbb{Z}$ does not have a type I relation with $\xi + \mathbb{Z}$. Thus, $\mathcal{O}$ is not a type I order. □

To find examples, we implemented the algorithm from [GPP93] and [GPP96] in SageMath, [The25a]. When looking for examples, we checked all 17^4 polynomials with coefficients bounded by ± 8. We also generated samples of 5000 irreducible polynomials with coefficients bounded by ± 16, ± 32, and ± 64 that were randomly selected. For the larger coefficient bound, the number of polynomials makes an exhaustive search impractical. Additionally, as the coefficients become larger, the computation time becomes a practical concern. The basic process for checking these polynomials is as follows:

1. Select the coefficient of a polynomial p to test.
2. Check for irreducibility of p.
3. If p is irreducible, continue; if not, select new coefficients.
4. Use the algorithm found in A.1 to find all the monogenizations of $\mathbb{Z}[T]/(p)$.
5. Record the coefficients, discriminant, monogenic signature, the Galois group, and if the roots of p give an integral power basis for the field $\mathbb{Q}(T)(p)$.

To guarantee that each polynomial represents a unique isomorphism class of monogenic orders, we eliminate all but one entry from any subsets that have the same values across the parameters for Disc(f), Disc(f)/Disc$\big(\mathbb{Q}$[T]/(f)$\big)$, Gal(f), and are also maximal orders in there field of fractions. After performing this reduction, a substantial number of orders remain in the dataset, as shown in Table 6.1 below.

Sample	Number of unique orders
Coefficient bound 8	23970
Coefficient bound 16	4943
Coefficient bound 32	4996
Coefficient bound 64	5000

Table 6.1. The number of polynomials from each coefficient bound after eliminating entries that may have defined isomorphic orders.

As can be seen in Figure 6.1 below, two times monogenic rings are relatively rare. Additionally, with the larger coefficient bound, the proportion of two times monogenic orders is decreasing. So interesting orders seem to become rarer as we move

to larger coefficients. Among the orders in the samples, which are two times monogenic, Figure 6.2 shows that nearly all two times monogenic orders are exactly two times monogenic.

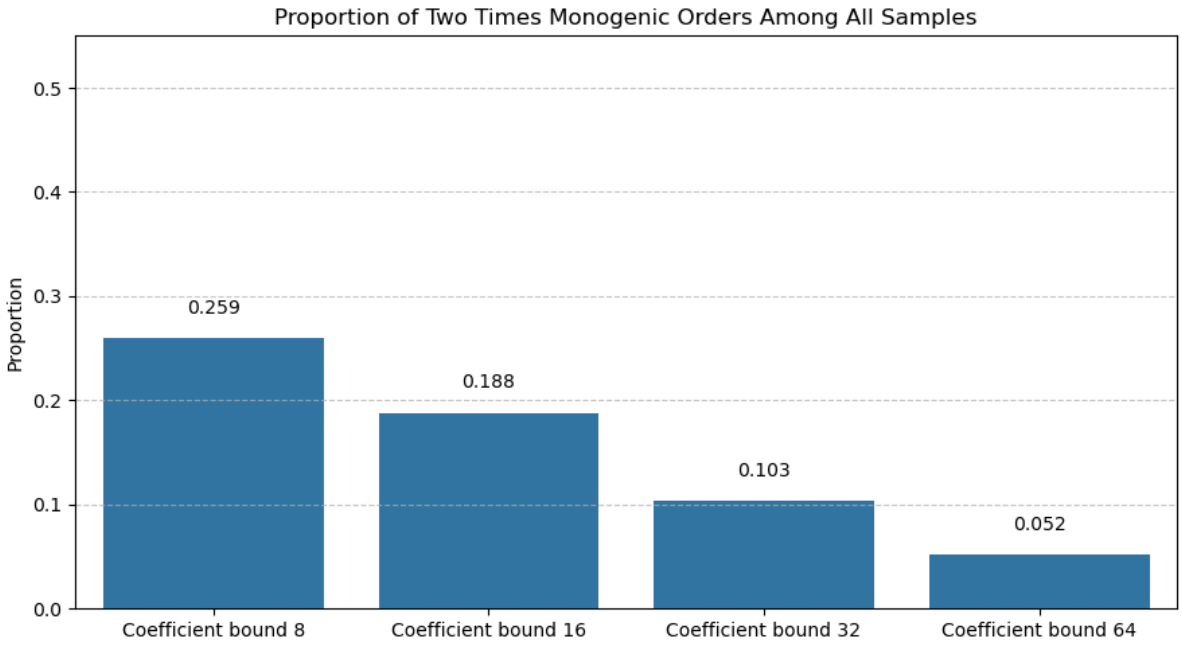

Figure 6.1. The proportion of two times monogenic orders among all orders defined by polynomials in the reduced sample.

Since the number of three times monogenic orders is small, we can filter for the orders that are not type I by looking for orders with monogenic signature $\{1, 1\}$. After applying this filter, we will be left with only orders that are exceptional or type II. Removing all the polynomials that could be type I by keeping only those orders with monogenic signature $\{1, 1\}$ leaves a total of 342 across all coefficient bounds. Using the algorithm from Appendix A.1 to find all monogenizations of each order, we eliminate any of the remaining 342 orders that may be type II. The Table 6.2 shows the number of exceptional orders represented by polynomials in the filtered dataset.

Galois Group	Number of Orders found
C_4	1
D_4	1
A_4	1
S_4	158

Table 6.2. All the exceptional orders found in the generated data.

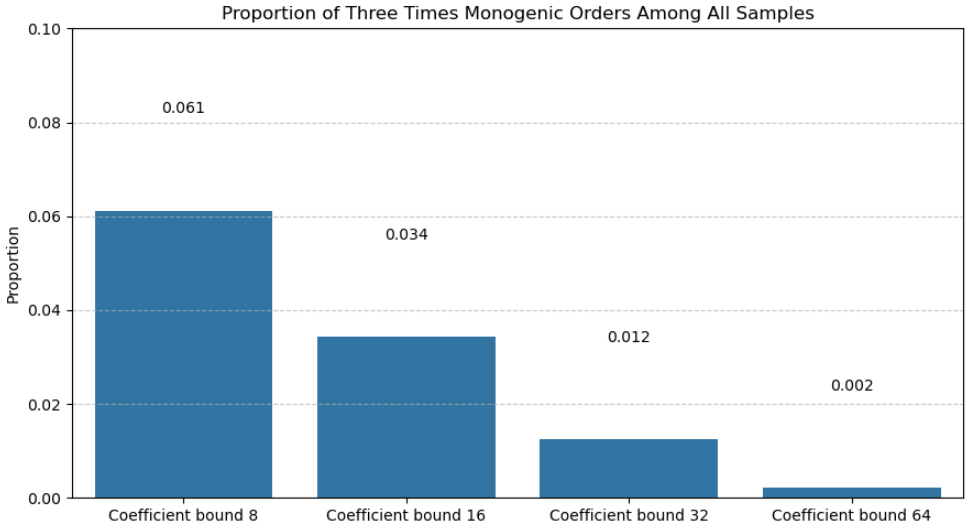

Figure 6.2. The proportion of three times monogenic orders among all orders defined by polynomials in the reduced sample.

6.1 Examples of Exceptional Orders with Galois Group C_4, D_4 or A_4

Every example given in this section is exactly two times monogenic. To determine this, we found all the monogenizations of each order using an implementation of the algorithm given in Appendix A.1. We outline each of the found examples with Galois group C_4, D_4, and A_4.

Example 6.4. Consider the irreducible polynomial $f(T) = T^4 + 4T^2 + 2$. Let ζ_{16} be a primitive 16th root of unity and $\alpha = \zeta_{16} - \zeta_{16}^{-1}$, then $f(\alpha) = 0$, so f is the minimal polynomial of α. We use Theorem 2.38 to find the Galois group of f. The cubic resolvent polynomial of α is

$$r_\alpha(T) = T^3 - 4T^2 - 8T + 32 = (T-4)(T^2-8).$$

The splitting field of r_α is the field $L = \mathbb{Q}(\sqrt{-8})$, and the polynomial $g(T) = (T^2 - 4T + 2)(T^2)$ from (2.57) splits in L as

$$g(T) = (T - 2 - 1/2\sqrt{-8})(T - 2 + 1/2\sqrt{-8})T^2.$$

Therefore, by Theorem 2.38, the Galois group of f is isomorphic to C_4.
Using the algorithm from Appendix A.1, we find the solutions to the equation

$$T_1^3 - 4T_1^2T_2 - 8T_1T_2^2 + 32T_2^3 = \pm 1 \tag{6.2}$$

are $(1,0)$ and $(-3,-1)$, and the two monogenizations for $\mathcal{O} = \mathbb{Z}[\alpha]$ are

$$\begin{aligned}\mathcal{S}_\alpha(1,0) =& \{\alpha + \mathbb{Z}\}\\ \mathcal{S}_\alpha(3,1) =& \{(3\alpha + \alpha^3) + \mathbb{Z}\}.\end{aligned}$$

We note some interesting additional facts about the ring $\mathbb{Z}[\alpha]$.

Using SageMath, [The25a] one can show $\{1, \alpha, \alpha^2, \alpha^3\}$ is an integral basis for K, therefore, $\mathbb{Z}[\alpha] = \mathcal{O}_K$. The field $\mathbb{Q}(\alpha)$ is a subfield of $\mathbb{Q}(\zeta_{16})$. Since $\mathbb{Q}(\zeta_{16})$ is a cyclotomic field it is a Galois extension of $\mathbb{Q}$ with Galois group

$$G = \mathrm{Gal}(\mathbb{Q}(\zeta_{16}/)/\mathbb{Q}) \cong (\mathbb{Z}/16\mathbb{Z})^\times \cong C_4 \times C_2.$$

G acts on the set of conjugates of ζ_{16} by sending ζ_{16} to a power ζ_{16}^a where $\gcd(a,16) = 1$. Therefore, the conjugates of α are all of the form

$$\zeta_{16}^a - \overline{\zeta_{16}^a}.$$

For any $a \in \mathbb{Z}$, we see that

$$\overline{\zeta_{16}^a - \overline{\zeta_{16}^a}} = \zeta_{16}^a - \overline{\zeta_{16}^a}.$$

So α and all its conjugates are real numbers.

Next, we will study two examples of orders with Galois group D_4. First, we will study an exceptional order, and second, we will study an order that is type II.

Example 6.5. Let $f(T) = 1 + 8T^2 - 8T + 2$ and α a root of f. Then the cubic resolvent polynomial of α is

$$r_\alpha(T) = T^3 - 8T^2 - 8T = T(T^2 - 8T - 8). \tag{6.3}$$

The rational root of r_α is 0, so the polynomial $g(T)$ from (2.57) is

$$g(T) = T^4 + 10T^2 + 16. \tag{6.4}$$

The splitting field of r_α is $L = \mathbb{Q}(\sqrt{2})$. Using SageMath [The25a], we find that $g(T)$ does not split over L. So by Theorem 2.38 the Galois group of f is D_4.

Using the algorithm from Appendix A.1, we find the solutions to

$$T_1^3 - 8T_1^2T_2 - 8T_1T_2^2 = \pm 1, \tag{6.5}$$

are $(1, 0)$ and $(1, -1)$, and the monogenizations of $\mathbb{Z}[\alpha]$ are

$$\begin{aligned} \mathcal{S}_\alpha(1, 0) &= \{\alpha + \mathbb{Z}\} \\ \mathcal{S}_\alpha(1, -1) &= \{(17\alpha + \alpha^2 + 2\alpha^3) + \mathbb{Z}\}. \end{aligned}$$

So $\mathbb{Z}[\alpha]$ is not type I or type II. Lastly with SageMath [The25a], we find $\{1, \alpha, \alpha^2, \alpha^3\}$ is an integral basis for K so $\mathbb{Z}[\alpha]$ is the ring of integers of K.

Example 6.6. Let $f(T) = T^4 + 6T^3 + 6T^2 - 8T + 8$ and α a root of f. The cubic resolvent polynomial of α is

$$r_\alpha(T) = T^3 - 6T^2 - 80T - 160 = (T + 4)(T^2 - 10T - 40).$$

The rational root of r_α is -4 and the polynomial $g(T)$ from (2.57) is defined by

$$g(T) = T^4 + 10T^3 + 42T^2 + 88T + 80.$$

The splitting field of r_α is $L = \mathbb{Q}(\sqrt{-15})$. We verify with SageMath [The25a] that $g(T)$ does not split over L; thus, by Theorem 2.38, the Galois group of $\mathbb{Q}(\alpha)$ is isomorphic to D_4. In this case, the discriminant of $\mathbb{Z}[\alpha]$ is 66560 while the discriminant of the field $\mathbb{Q}(\alpha)$ is 1040, so $\mathbb{Z}[\alpha]$ is a proper subring of the ring of integers of $\mathbb{Q}(\alpha)$.
Let $k = -3$ and $\ell = -3$ then

$$f(T) = T^4 - 2kT^3 + (k^2 + \ell)T^2 - (k\ell - 1)T + 8.$$

Therefore, $\mathbb{Z}[\alpha]$ is a type II order by Theorem 1.17.

Next, we will study an example with Galois group A_4.

Example 6.7. Let $f(T) = T^4 - 3T^3 + 8T^2 - 5T + 6$, and α a root of f. The cubic resolvent polynomial of α is

$$r_\alpha(T) = T^3 - 8T^2 - 9T + 113.$$

Note that r_α is irreducible over $\mathbb{Q}$. The discriminant of f is $41209 = 203^2$, so by Theorem 2.38, the Galois group of f is isomorphic to A_4.
Using the algorithm from Appendix A.1, we find the solutions to

$$T_1^3 - 8T_1^2T_2 - 9T_1T_2^2 + 113t_2^2 = \pm 1 \tag{6.6}$$

are $(1, 0)$ and $(7, 1)$, and the monogenizations of $\mathbb{Z}[\alpha]$ are

$$\begin{aligned}\mathcal{S}_\alpha(1,0) =& \{\alpha + \mathbb{Z}\}\\ \mathcal{S}_\alpha(7,1) =& \{(7\alpha - 3\alpha + \alpha^3) + \mathbb{Z}\}.\end{aligned}$$

So $\mathbb{Z}[\alpha]$ is an exceptional order. Using SageMath [The25a], we can see $\{1, \alpha, \alpha^2, \alpha^3\}$ is an integral basis for K. Therefore, $\mathbb{Z}[\alpha]$ is the ring of integers of $\mathbb{Q}(\alpha)$.

6.2 Examples of Exceptional Order with Galois Group S_4

In total, 158 exceptional orders with the Galois group S_4 were found. We outline three examples below.

Example 6.8. Let $f(T) = T^4 - 7T^3 + 8T^2 - 6T + 8$ and α a root of f. Also let $K = \mathbb{Q}(\alpha)$ we will analyze the order $\mathbb{Z}[\alpha]$ with basis $\{1, \alpha, \alpha^2, \alpha^3\}$. First, we

verify that the Galois group of f is S_4 using Theorem 2.38. The cubic resolvent polynomial of α is

$$r_\alpha(T) = T^3 - 8T^2 + 10T - 172,$$

which is irreducible over $\mathbb{Q}$. The discriminant of f is -900944, which is not a square in $\mathbb{Q}$; therefore, the Galois group of f is isomorphic to S_4.

Now, we use the Algorithm given in Appendix A.1 to verify that $\mathbb{Z}[\alpha]$ is an exceptional order. First, using SageMath [The25a], we find the solutions to

$$F_\alpha(T_1, T_2) = T^3 - 8T_1^2T_2 + 10T_1T_2^2 - 172T_2^3 = \pm 1, \tag{6.7}$$

are $\pm(1, 0)$ and $\pm(-9, -1)$. The the monogenizations of $\mathbb{Z}[\alpha]$ are

$$\mathcal{S}_\alpha(1, 0) = \{\alpha + \mathbb{Z}\} \qquad \mathcal{S}_\alpha(9, 1) = \{(7\alpha - 7\alpha^2 + \alpha^3) + \mathbb{Z}\}.$$

So $\mathbb{Z}[\alpha]$ is not a type I order by Corollary 6.3 since it has monogenic signature $\{1, 1\}$. Examining the monogenizations, we can see that the definition of a type II order is also not met. Therefore, $\mathbb{Z}[\alpha]$ is an exceptional order. The discriminant of K is -225236 thus $\mathbb{Z}[\alpha]$ is a proper subring of $\mathcal{O}_K$.

Example 6.9. Let $f(T) = T^46T^3 + 2T^2 - 3T + 3$ and α a root of f. Also let $K = \mathbb{Q}(\alpha)$ we analyze the order $\mathbb{Z}[\alpha]$ with basis $\{1, \alpha, \alpha^2, \alpha^3\}$. First, we verify that the Galois group of f is S_4 using Theorem 2.38. The cubic resolvent polynomial of α is

$$r_\alpha(T) = T^3 - 2T^2 + 30T + 75,$$

which is irreducible over $\mathbb{Q}$. The discriminant of f is -334875, which is not a square in $\mathbb{Q}$; therefore, the Galois group of f is isomorphic to S_4.

Now, the algorithm given in Appendix A.1 to verify that $\mathbb{Z}[\alpha]$ is an exceptional order. First, using SageMath [The25a], we find the solutions to

$$F_\alpha(T_1, T_2) = T^3 - 2T_1^2T_2 + 30T_1T_2^2 - 75T_2^3 = \pm 1, \tag{6.8}$$

are $\pm(1, 0)$ and $\pm(2, -1)$. The monogenizations of $\mathbb{Z}[\alpha]$ are

$$\mathcal{S}_\alpha(1, 0) = \{\alpha + \mathbb{Z}\} \qquad \mathcal{S}_\alpha(2, 1) = \{(\alpha + 6\alpha^2 + \alpha^3) + \mathbb{Z}\}.$$

So $\mathbb{Z}[\alpha]$ is not a type I order by Corollary 6.3 since it has monogenic signature $\{1, 1\}$. One can also see that the only two monogenizations of $\mathbb{Z}[\alpha]$ do not satisfy a type II relation. Therefore, $\mathbb{Z}[\alpha]$ is an exceptional order. The discriminant of K is -13395, which is not the same as the discriminant of $\mathbb{Z}[\alpha]$. Therefore $\mathbb{Z}[\alpha]$ is a proper subring of $\mathcal{O}_K$.

Example 6.10. Let $f(T) = T^4 - 5T^3 - 20T^2 - 54T - 59$ and α a root of f. We find the Galois group of f using Theorem 2.38. The cubic resolvent polynomial of α is

$$r_\alpha(T) = T^3 + 20T^2 + 506T + 3279,$$

which is irreducible over $\mathbb{Q}$, and the discriminant of f is -213727531 which is not a square. Thus, by Theorem 2.38, the Galois group of f is S_4.
Now we use the algorithm from Appendix A.1 to find the monogenizations of $\mathbb{Z}[\alpha]$. We find that the equations

$$F_\alpha(T_1, T_2) = T_1^3 + 20T_1^2T_2 + 506T_1T_2^2 + 3279T_2^3 = \pm 1 \tag{6.9}$$

has solutions $\pm(1, 0)$ and $\pm(8, -1)$. The monogenizations of $\mathbb{Z}[\alpha]$ are

$$\mathcal{S}_\alpha(1, 0) = \{\alpha + \mathbb{Z}\} \quad \text{and} \quad \mathcal{S}_\alpha(8, -1) = \{(20\alpha + 13\alpha^2 - 2\alpha^3) + \mathbb{Z}\}.$$

So $\mathbb{Z}[\alpha]$ is not a type II order, and by Corollary 6.3 $\mathbb{Z}[\alpha]$ is not a type I order. Therefore, $\mathbb{Z}[\alpha]$ is an exceptional order. Using SageMath [The25a], we determine that $\{1, \alpha, \alpha^2, \alpha^3\}$ is an integral basis for K so $\mathbb{Z}[\alpha] = \mathcal{O}_K$.

6.3 Examples of Highly Monogenic Orders

While many of the polynomials in the datasets define orders that have at least two monogenizations, several have many monogenizations. Below, we provided a table of some of the orders with the most monogenizations.

6.4 Monogenic Orders which are Maximal Orders in their Field of Fractions

The examples of exceptional orders we showed in Section 6.1 and Section 6.2 were largely examples in which the ring of integers of a number field was monogenic. This is generally not the case for number fields. In Figures 6.3, 6.4, and 6.5, we see that, compared to the data as a whole, a large proportion of exceptional orders are the rings of integers in there field of fractions. Number fields where the ring of integers is a monogenic order are often referred to as monogenic fields. The proportion of cubic and quartic fields is studied by Alpöge, Bhargava, and Shnidman in [ABS21a] and [ABS21b]. The high proportion of polynomials defining monogenic fields among the exceptional orders in the datasets suggests that more exceptional orders may be discovered by examining monogenic fields. In [HJ24], Harrington and Jones provided examples of infinite families of quartic polynomials defining monogenic fields for the Galois groups V_4, D_4, A_4, and S_4.

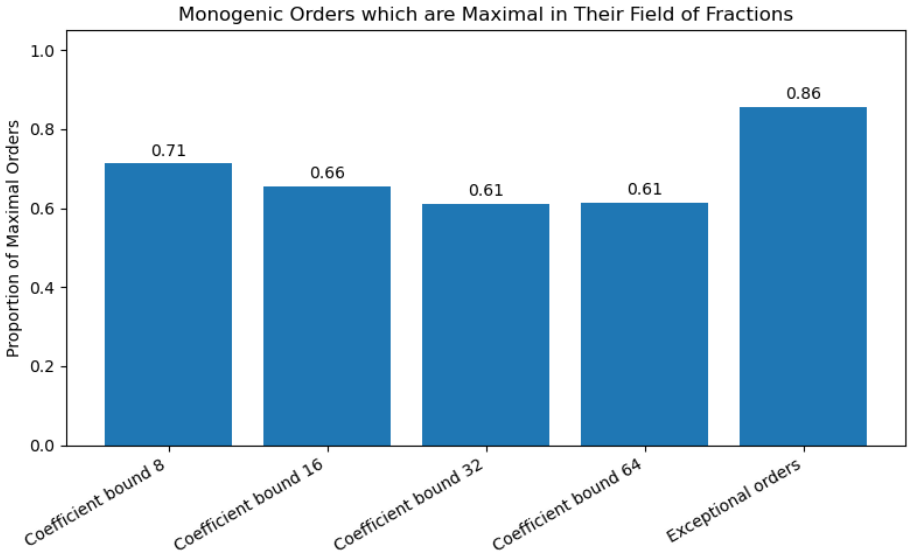

Figure 6.3. Proportion of orders from each sample that are maximal orders in their field of fractions.

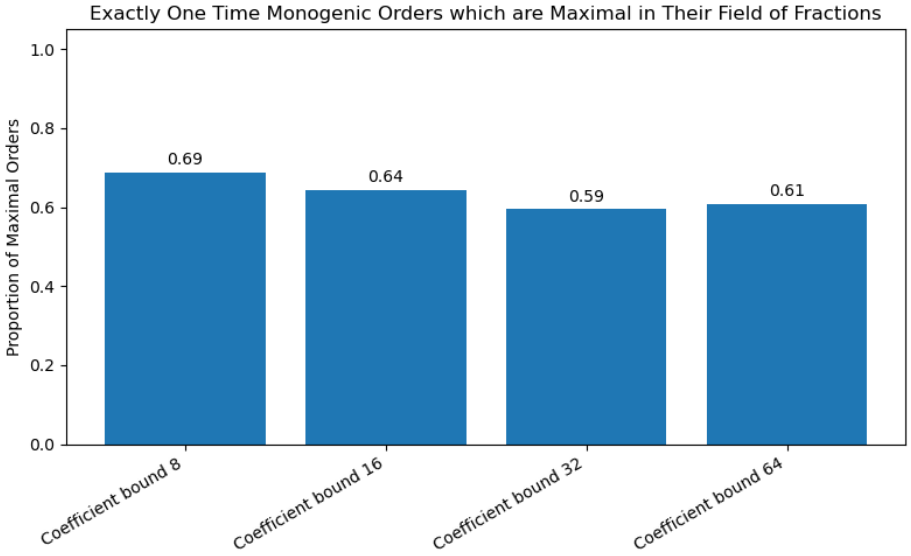

Figure 6.4. The proportion of orders from each coefficient bound with exactly one monogenization that are maximal in their field of fractions.

Figure 6.5. The proportion of two times monogenic orders from each coefficient bound, which are maximal orders in their field of fractions. The far right column is the proportion of exceptional orders that are maximal in their field of fractions.

$f(T)$	Monogenic Signature	Discriminant	Gal(f)
$T^4 - 5T^3 + 5T^2 + 5T - 5$	$\{6, 6\}$	1125	C_4
$T^4 - 5T^3 + 3T^2 + 5T - 3$	$\{0, 2, 3, 5, 2\}$	16357	S_4
$T^4 - 5T^3 6T^2 - 1$	$\{5, 6\}$	725	D_4
$T^4 + T^3 - 8T^2 + 1$	$\{2, 2, 3, 3\}$	58469	S_4
$T^4 - 5T^3 + 5T^2 + 5T - 7$	$\{3, 6, 1\}$	-283	S_4
$T^4 + 6T^3 + T^2 - 3T - 1$	$\{1, 2, 4, 2, 0\}$	2777	S_4
$T^4 - 8T^3 + 16T^2 - 10T + 2$	$\{3, 4\}$	-688	S_4
$T^4 - 5T^3 + 7T^2 - 3T - 1$	$\{4, 2\}$	-1371	S_4
$T^4 - 12T^3 - 2T^2 + 12T + 2$	$\{4, 2\}$	11186432	S_4
$T^4 + T^2 + 13T^2 + 13T + 1$	$\{3, 3\}$	-1153651	S_4

Table 6.3. The polynomials in the total reduced dataset that define orders having the greatest number of monogenizations. See definition 2.37 for the definition of Gal(f), and 6.2 for the definition of monogenic signature

CHAPTER 7

CONCLUSION

In this dissertation, we establish a connection between the structure of solutions to quartic index equations and the type classification of monogenic orders. Our approach was to identify a connection between how the algorithm from [Akh22] groups the monogenizations and how this grouping was connected to the type I algebraic relations. By studying the Diophantine equations attached to the index equations for quartic orders, we were able to prove that every two times monogenic order in a biquadratic field is a type I order. The same techniques also produced partial results, limiting the possible solutions to the index form equation in a field whose normal closure has Galois group C_4 or D_4

Using the Diophantine equation given in the algorithm from [Akh22] for finding monogenizations, we also studied the type II monogenic orders. For type II relations, we provided a complete parametrization of all polynomials that define type II monogenic orders. This parameterization enabled us to give a new infinite family of type II orders. The parameterization also provided an effective way to determine if an order is type II from a defining polynomial in some cases.

We have also created a dataset of 161 exceptional orders, none of which were known. To find these orders, an implementation of the algorithm from [GPP96] with the specialization to monogenic orders from [Akh22] was developed using SageMath and Pari/gp. In addition to the SageMath code to find all monogenizations of a quartic order, several diagnostic functions were also developed. Using this implementation, we were able to do a complete search of irreducible polynomials with coefficients bounded by ± 8, and produce a sample of 5000 polynomials with coefficients bounded by ± 16, ± 32, and ± 64. All the code, as well as the datasets of orders, are available on GitHub (see the Appendix for details on how to access and use the code).

The work in this dissertation provided many new directions for inquiry. Firstly, spurred by the results of Bérczes, Evertse, Győry in [BEG13] on the scarcity of exceptional orders in fields with Galois group S_4, we sought to understand exceptional orders in any quartic number field. To this end, we made progress in fields whose Galois group is V_4, C_4, or D_4, but did not address fields with a Galois group of A_4. Given the scarcity of examples of exceptional orders with a Galois group other than S_4, we suspect that exceptional orders in any quartic number field are rare in some

sense. We hope that future work will extend the partial results on fields with Galois groups C_4 and D_4 using techniques from Diophantine approximations or Diophantine geometry. The approach used for fields with the Galois group V_4, C_4, and D_4 will not work if the Galois group is A_4. To study the case with the three smallest Galois groups, we utilized the reducibility of specific Diophantine equations that arise in the algorithm for solving quartic index equations. For polynomials with Galois group A_4, the specific Diophantine equation is irreducible. Therefore, a new approach will be needed in fields with the Galois group A_4.

Improvements can also be made to the SageMath code used to compute monogenizations of quartic rings. The algorithm used to solve quartic index equations requires solving many Diophantine equations of the form

$$F(T_1, T_2) = \pm 1, \tag{7.1}$$

where F is homogeneous of degree three or four. Fortunately, Pari/gp has an existing function to solve the type of equation shown above, but the run time of this function is roughly proportional to the size of the coefficients of F. When solving quartic index equations for an order $\mathbb{Z}[\alpha]$, we need to solve (7.1) where the left-hand side is the cubic resolvent form of α. If a_m and c_m are the largest absolute values of coefficients of the minimal polynomial of α and the cubic resolvent polynomial of α, respectively, then c_m is typically between a_m^2 and a_m^3. Thus, even for polynomials with coefficients bounded by ± 128, it can take dozens of seconds to solve a quartic index equation for one algebraic integer ξ. Using the action of $\mathrm{GL}_2(\mathbb{Z})$, it may be possible to replace the right-hand side of (7.1) with an equivalent homogeneous polynomial with smaller coefficients, resulting in a faster overall run time. We hope to explore this possible optimization for the algorithm in the future.

In summary, this dissertation contributes to our understanding of monogenic quartic orders by combining techniques from Diophantine equations, Galois Theory, and computational experimentation. Our parameterization of type II orders, along with the existence of over 150 exceptional orders, provided new insights into these rings. While many deep questions remain, particularly for fields with Galois group A_4, the tools and dataset developed will provide a foundation for further inquiry. We hope to build upon the work here in the future to offer a fuller understanding of monogenic quartic orders.

APPENDIX A

THE ALGORITHM USED TO FIND ALL MONOGENIZATIONS OF QUARTIC ORDERS

Here, we will provide an explicit, step-by-step version of the algorithm used to find all monogenizations of a quartic monogenic order, given the minimal polynomial of a monogenizer.

After presenting the general algorithm, we will discuss how to access and utilize the SageMath implementation, as well as provide important information about the datasets of monogenic orders that were generated. All the code and files created for this dissertation can be found in a GitHub repository here: https://github.com/shumakerJ/Thesis_work/tree/main.

A.1 An Algorithm for Solving the Quartic Index Form Equations

Let ξ be a quartic algebraic integer with minimal polynomial $f_\xi(T) = T^4 + a_1T^3 + a_2T^2 + a_3T + a_4$, $K = \mathbb{Q}(\xi)$, and $\mathcal{O} = \mathbb{Z}[\xi]$. Propositions 2.33 outlines an algorithm for reducing the index form equation $\mathcal{I}(X, Y, Z) = \pm 1$, for $\mathbb{Z}[\xi]$ to solving a system of three equations,

$$Q_1(X, Y, Z) = T_1, \qquad Q_2(X, Y, Z) = T_2, \qquad F_\xi(T_1, T_2) = \pm 1, \tag{A.1}$$

where F_ξ is the cubic resolvent form of ξ, defined in 2.27, the quadratic forms Q_1, Q_2 are defined to be

$$Q_1(X, Y, Z) = X^2 - a_1XY + a_2Y^2 + (a_1^2 - 2a_2)XZ + (a_3 - a_1a_2)YZ + (-a_1a_3 + a_2^2 + a_4)Z^2, \tag{A.2}$$

and

$$Q_2(X, Y, Z) = Y^2 - XZ - a_1YZ + a_2Z^2. \tag{A.3}$$

Remark A.1. Since the cubic resolvent form of a quartic algebraic integer is monic, every solution (x, y, z) to (A.1) satisfying $Q_2(x, y, z) = 0$ must satisfy $Q_1(x, y, z) = \pm 1$.

Gaál, Pethő, and Pohst in [GPP96] provided an algorithm for further reducing a system of two trinary quadratics to the task of independently solving a finite set of equations

$$H(T_1, T_2) = \pm m, \tag{A.4}$$

where H is a an integral quartic form, and $m \in \mathbb{Z}$. Computer algorithms for finding all integer solutions to equations of the type in (A.4) have been developed. In particular, the function `thue`(tnf, a, {sol}) in the computer algebra system Pari/gp, finds all solutions to (A.4), [The24], Chapter 3, Section 9.53. Therefore, once we reduce a quartic index form equation to the finite set of equations of the form in (A.4), a complete list of solutions can be produced.

The reduction from [GPP96] of the system

$$Q_1(X, Y, Z) = t_1, \qquad Q_2(X, Y, Z) = t_2, \tag{A.5}$$

is performed by first defining a new form

$$Q_{t_1,t_2}(X, Y, Z) = t_2 Q_1(X, Y, Z) - t_1 Q_2(X, Y, Z), \tag{A.6}$$

and then finding an integer solution to the equation

$$Q_{t_1,t_2}(X, Y, Z) = 0. \tag{A.7}$$

Note that every non-trivial solution to (A.5) will be a solution to (A.7). The form Q_{t_1,t_2} can be rewritten as the sum of three squares, with coefficients a, b, c square-free and satisfying $\gcd(a, b) = \gcd(b, c) = \gcd(a, c) = 1$. Mordell outlines a precise method for performing the change of variables needed to rewrite Q_{t_1,t_2} in Chapter 7, Sections 1 and 2 of [Mor69]. Once we have Q_{t_1,t_2} in the standard form, as given by the following Theorems of Mordell, we can find a non-trivial solution.

Theorem A.2. *([Mor69] Chapter 7 Theorem 3) If $a, b, c \in \mathbb{Z}$ is square free,*

$$\gcd(a, b) = \gcd(b, c) = \gcd(a, c) = 1,$$

and a, b, c are not all of the same sign, then the equation

$$aX^2 + bY^2 + cZ^2 = 0$$

has a non-trivial integer solution if and only if all the following congruences are solvable:

$$\begin{aligned} T^2 + bc &\equiv 0 \pmod{a}, \\ T^2 + ac &\equiv 0 \pmod{b}, \\ T^2 + ab &\equiv 0 \pmod{c}, \\ aX^2 + bY^2 + cZ^2 &\equiv 0 \pmod{8}. \end{aligned}$$

If (A.7) is solvable, the next theorem from Mordell gives bounds for a small solution. Once we have a small solution, we will be able to find all the solutions to (A.7).

Theorem A.3. *([Mor69] Chapter 7 Theorem 5) If* $aX^2+bY^2+cZ^2=0$ *is solvable, with* $a,b,c\in\mathbb{Z}$ *are square free,* $\gcd(a,b)=\gcd(b,c)=\gcd(a,c)=1$*, and* $a,b>0$*,* $c<0$ *then there exists a non-trivial solution satisfying*

$$|x|\leq\sqrt{b|c|},\qquad |y|\leq\sqrt{|c|a},\qquad |z|\leq\sqrt{ab}.$$

With a small solution, we can parametrize all the solutions using the approach laid out in the next theorem.

Theorem A.4. *([Mor69] Chapter 7 Theorem 4) If a non-trivial integer solution exists for the equation*

$$f(X,Y,Z)=0,$$

where f *is an irreducible ternary quadratic form, then the general solution* (x,y,z) *such that* $\gcd(x,y,z)=1$*, is given by a finite number of expressions of the form*

$$\begin{aligned}x=f_x=&a_xp^2+b_xpq+c_xq^2,\\ y=f_y=&a_yp^2+b_ypq+c_yq^2,\\ z=f_z=&a_zp^2+b_zpq+c_zq^2,\end{aligned}$$

where p,q *take all integer values with* $\gcd(p,q)=1$ *and the numbers* a*,* b *and* c *are integer constants.*

The general approach discussed here outlines the process for finding all the monogenization of a monogenic ring. In the next section, we will give the algorithm in detail for finding all monogenizations.

The Algorithm for Finding All Monogenizations in Quartic Monogenic Orders

Input: A quartic algebraic integers ξ and its minimal polynomial f_ξ.
Output: A set of all monogenizations for the ring $\mathbb{Z}[\xi]$, subdivided by the solutions to $F_\xi(T_1,T_2)=\pm1$ where F_ξ is the cubic resolvent form of ξ. Every monogenization $\beta+\mathbb{Z}$ in the output are represented by the coordinates (x,y,z) where $(x\xi+y\xi^2+z\xi^3)+\mathbb{Z}=\beta+\mathbb{Z}$ as monogenizations.

1. Compute the cubic resolvent form of ξ, $F_\xi(T_1, T_2)$.

2. Find all solutions to $F_\xi(T_1, T_2) = \pm 1$, and record each solution in a set S_F.

3. Compute the quadratic forms Q_1 and Q_2 from (A.2) and (A.3).

4. Let $H_\xi(T_2, T_2)$ be the minimal form of ξ, and find all integer solutions to

$$H_\xi(T_1, T_2) = \pm 1. \tag{A.8}$$

5. For each solution (t_1, t_2) to (A.8) use Corollary 3.7 to find the triples (x, y, z) solving (A.1) when $(t_1, t_2) = (\pm 1, 0)$. Record all the found triples (x, y, z) in the set $\mathcal{S}_\xi(1, 0)$.

6. For each $(t_1, t_2) \in S_F$, if $(t_1, t_2) \neq (\pm 1, 0)$ perform the following steps,

   a) Define Q_{t_1,t_2} by

$$Q_{t_1,t_2}(X, Y, Z) = t_2 Q_1(X, Y, Z) - t_1 Q_2(X, Y, Z). \tag{A.9}$$

   Every solution to the system

$$\begin{aligned} Q_1(X, Y, Z) &= t_1, \\ Q_2(X, Y, A) &= t_2 \end{aligned}$$

   will be a solution to (A.9).

   b) Rewrite $Q_{t_1,t_2}(X, Y, Z)$ as the sum of three squares in the variables X', Y' and Z', retain the change of variables.

   c) Using Theorems A.2 and A.3 and the change of variables X', Y' and Z' to find a solution (x_0, y_0, z_0) to (A.9). Note that if $y_0 = 0 = z_0$, then we can see that $x_0 = \pm 1$ from the definition of the equation in the system (A.1). So one of y_0 or z_0 is not 0.

   d) If $z_0 \neq 0$ then following Mordell's proof of Theorem A.4 all solutions (x, y, z) to (A.9) can be represented as

$$x = rx_0 + p, \qquad y = ry_0 + q, \qquad z = rz_0, \tag{A.10}$$

   where r, p and q are rational parameters.

e) substituting (A.10) into (A.9) and perform the simplification resulting from (x_0, y_0, z_0) being a solution to (A.9) to obtain the relations

$$r(c_1p + c_2q) = c_3p^2 + c_3pq + c_5q^2, \tag{A.11}$$

where the c_i are integers for $1 \leq i \leq 5$.

f) Multiply (A.10) by $r(c_1p + c_2q)$, and divide by d, where d is the square of common denominator of p and q. Using the relation (A.11), and dividing by $g = \gcd(p, q)^2$ we get

$$\begin{aligned} kx = f_x(p, q) &= c_{1,1}p^2 + c_{1,2}pq + c_{1,3}q^2, \\ ky = f_y(p, q) &= c_{2,1}p^2 + c_{2,2}pq + c_{2,3}q^2, \\ kz = f_z(p, q) &= c_{3,1}p^2 + c_{3,2}pq + c_{3,3}q^2, \end{aligned} \tag{A.12}$$

where $k \in \mathbb{Z}$ is a positive divisor of d/g, $c_{i,j} \in \mathbb{Z}$ for $1 \leq i, j \leq 3$ and the parameters p and q are coprime. Let D be the set of all positive divisors of d/g

g) Define $H(P, Q) = Q_2(f_x(P, Q), f_y(P, Q), f_z(P, Q))$ and find all integer solutions to the equations

$$H(P, Q) = \pm k, \tag{A.13}$$

for all possible values of k, from step (f).

h) For each solution (p, q) to (A.13), check if $(f_x(p, q), f_y(p, q), f_z(p, q))$ is a solution to (A.1). If $(f_x(p, q), f_y(p, q), f_z(p, q))$ is a solution, then record the value in the set $\mathcal{S}_\xi(t_1, t_2)$.

i) If $z_0 = 0$ then $y_0 \neq 0$, then use the parametrization

$$x = rx_0 + p, \qquad y = ry_0, \qquad z = rz_0 + q, \tag{A.14}$$

to and follow steps (e)-(h).

7. Return the calculated set $\mathcal{S}_\xi(t_1, t_2)$ for $(t_1, t_2) \in S$.

A.2 The Implementation of the Algorithm in SageMath

When implementing the algorithm for finding all monogenizations of a given order, the primary concern was memory use. Early experiments suggested that

many orders would need to be searched to find any that are exceptional. During early tests, we found that storing the necessary data to search thousands of polynomials would require several gigabytes without memory optimizations. For this reason, we designed the code around a custom class `poly`, with attributes including the coefficients of a quartic polynomial and the coefficients of its cubic resolvent, as well as attributes related to the information obtained during the process of finding all the monogenizations. The steps in the algorithm are then implemented as methods in the `poly` class. This design enabled the search of nearly 100,000 orders while using relatively little memory. It had the additional benefit of outputting information which could be recorded in a CSV file.

In addition to implementing the algorithm from Section A.1, we developed several valuable functions. Most important is the function `find_monogens` that takes as input an array of 5 integers $[1, a_1, a_2, a_3, a_4]$ and returns all the monogenizations of the ring defined by the polynomial $f(T) = T^4 + a_1T^3 + a_2T^2 + a_1T + a_4$. An example is shown below.

Example A.5. To find the monogenizations of the order $\mathcal{O}$ defined by the polynomial $f(T) = T^4 + T^3 + T^2 + T + 1$, we use the code shown below. We assume a fixed monogenizer ξ of the order $\mathcal{O}$, where $f(\xi) = 0$ and a basis $\{1, \xi, \xi^2, \xi^3\}$ for $\mathcal{O}$.

```
find_monogens([1,1,1,1,1])
```

Output:

```
(-1, -1)
(1, 0)
[3, 3]
{(-1, -1): {(0, 0, -1), (1, 1, 0), (0, 1, 0)}, (1, 0): {(1, 0,
   0), (1, 0, 1), (1, 1, 1)}}
```

The pairs $(-1, -1)$ and $(1, 0)$ are the solutions to the equations

$$F(T_1, T_2) = \pm 1, \tag{A.15}$$

where $F(T, 1)$ is the cubic resolvent polynomial of f. The array $[3, 3]$ is the monogenic signature, and the set at the end indicates that

$$\mathcal{S}_\xi(1, 0) = \{(1, 0, 0), (1, 0, 1), (1, 1, 1)\} \tag{A.16}$$

$$\mathcal{S}_\xi(1, 1) = \{(0, 0, -1), (1, 1, 0), (0, 1, 0)\} \tag{A.17}$$

All the code can be found in the Jupyter notebook file in the `Monogen_Search_P.ipynb`, which is available in the GitHub repository https://github.com/shumakerJ/Thesis_work.

A.3 Accessing the Code and Datasets

All datasets of quartic monogenic orders created for this project can be found on GitHub here: https://github.com/shumakerJ/Thesis_work/tree/main/Data, in CSV format. The final cleaned and complete version of the dataset can be found in the folder `final_version`. Each of the CSV files has several rows corresponding to non-isomorphic orders. The data is organized into six labeled columns. Below, we provide a brief description of what data in each column represents.

- `coefficients`: Contains an array of integers $[1, a_1, a_2, a_3, a_4]$ which are the coefficients of the quartic polynomial $f(T) = T^4 + a_1T^3 + a_2T^2 + a_3T + a_4$. Every polynomial represented in the dataset has been checked using SageMath to ensure that it is irreducible over $\mathbb{Q}$.
- `signature`: Contains the monogenic signature of each of the orders.
- `discriminant`: Contains the discriminant of the polynomial f.
- `gal_group`: The Galois group of f.
- `disc_ratio`: The quotient of the discriminant of f divided by the discriminant of the field $\mathbb{Q}[T]/(t)$, computed using SageMath.
- `ring_int`: A column of boolean values that indicates if the order represented by each row is a maximal order in its field of fractions. The rings were verified to be the ring of integers by checking if the associated power basis is an integral basis for the field.

REFERENCES CITED

[ABS21a] L. Alpöge, M. Bhargava, and A. Shnidman, *A positive proportion of cubic fields are not monogenic yet have no local obstruction to being so*, arXiv: 2011.01186 [math.NT], 2021.

[ABS21b] ———, *A positive proportion of quartic fields are not monogenic yet have no local obstruction to being so*, arXiv: 2107.05514 [math.NT], 2021.

[Akh22] S. Akhtari, *Quartic index form equations and monogenizations of quartic orders*, Essent. Number Theory **1** (2022), no. 1, 57–72, DOI: 10.2140/ent.2022.1.57, MR4573252.

[BEG13] A. Bérczes, J.-H. Evertse, and K. Győry, *Multiply monogenic orders*, Ann. Sc. Norm. Super. Pisa Cl. Sci. (5) **12** (2013), no. 2, 467–497, MR3114010.

[Ben01] M. A. Bennett, *On the representation of unity by binary cubic forms* (English), Trans. Am. Math. Soc. **353** (2001), no. 4, 1507–1534, DOI: 10.1090/S0002-9947-00-02658-1.

[Bha04] M. Bhargava, *Higher composition laws. III. The parametrization of quartic rings*, Ann. of Math. (2) **159** (2004), no. 3, 1329–1360, DOI: 10.4007/annals.2004.159.1329, MR2113024.

[Bha22] ———, *On the number of monogenizations of a quartic order*, Publ. Math. Debrecen **100** (2022), no. 3-4, 513–531, DOI: 10.5486/pmd.2022.9433, MR4434621, With an appendix by Shabnam Akhtari.

[BM72a] B. J. Birch and J. R. Merriman, *Finiteness Theorems for Binary Forms with Given Discriminant*, Proceedings of the London Mathematical Society **s3-24** (1972), no. 3, 385–394, DOI: 10.1112/plms/s3-24.3.385, eprint: https://academic.oup.com/plms/article-pdf/s3-24/3/385/4272690/s3-24-3-385.pdf.

[BM72b] ———, *Finiteness theorems for binary forms with given discriminant*, Proc. London Math. Soc. (3) **24** (1972), 385–394, DOI: 10.1112/plms/s3-24.3.385, MR306119.

[DF03] D. Dummit and R. Foote, *Abstract Algebra*, Wiley, 2003.

[DF64] B. N. Delone and D. K. Faddeev, *The theory of irrationalities of the third degree, Vol. Vol. 10*, Translations of Mathematical Monographs, American Mathematical Society, Providence, RI, 1964, xvi+509, MR160744.

[Gaá19] I. Gaál, *Diophantine Equations and Power Integral Bases, Theory and Algorithms*, 2nd ed., Translations of Mathematical Monographs, Birkhäuser Cham, 2019, xxii+326.

[GPP93] I. Gaál, A. Pethő, and M. Pohst, *On the resolution of index form equations in quartic number fields*, J. Symbolic Comput. **16** (1993), no. 6, 563–584, DOI: https://doi.org/10.1006/jsco.1993.1064.

[GPP96] ———, *Simultaneous Representation of Integers by a Pair of Ternary Quadratic Forms—With an Application to Index Form Equations in Quartic Number Fields*, J. Number Theory **57** (1996), no. 1, 90–104, DOI: https://doi.org/10.1006/jnth.1996.0035.

[HJ24] J. Harrington and L. Jones, *Monogenic Quartic Polynomials and Their Galois Groups*, Bull. Aust. Math. Soc. **111** (2024), no. 2, 244–259, DOI: 10.1017/s000497272400073x.

[KW89] L.-C. Kappe and B. Warren, *An Elementary Test for the Galois Group of a Quartic Polynomial*, The American Mathematical Monthly **96** (1989), no. 2, 133–137.

[Mil20] J. S. Milne, *Algebraic Number Theory (v3.08)*, Available at www.jmilne.org/math/, 2020.

[Mor69] L. Mordell, *Diophantine Equations: Diophantine Equations*, Pure and Applied Mathematics, Academic Press, 1969.

[The24] The PARI Group, *PARI/GP User's Guide*, Version 2.17.2. https://pari.math.u-bordeaux.fr/doc/, Université de Bordeaux, Bordeaux, France, 2024.

[The25a] The Sage Developers, *SageMath, the Sage Mathematics Software System (Version 10.5)*, available from https://www.sagemath.org, 2025.

[Thu09] A. Thue, *Über Annäherungswerte algebraischer Zahlen.* (ger), Journal für die reine und angewandte Mathematik **135** (1909), 284–305.

[Woo12] M. M. Wood, *Quartic rings associated to binary quartic forms*, Int. Math. Res. Not. IMRN (2012), no. 6, 1300–1320, DOI: 10.1093/imrn/rnr070, MR2899953.