PARAMETRIC FAMILIES OF POLYNOMIALS:
CONSTRUCTION AND APPLICATIONS

by

MELISA JEAN LAVALLEE

B.Sc., The University of British Columbia, 2006
M.Sc., The University of British Columbia, 2008

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

DOCTOR OF PHILOSOPHY

in

THE COLLEGE OF GRADUATE STUDIES
(Mathematics)

THE UNIVERSITY OF BRITISH COLUMBIA
(Okanagan)

June 2013
© Melisa Jean Lavallee, 2013
Abstract

The focus of this thesis is on the study of parametric families of polynomials and in particular, their construction and applications. A method in constructing a family of parametric sextic trinomials defining sextic fields containing any cubic subfield is presented. We then show two applications of our parametrization to obtain already established parameterizations of sextic trinomials defining sextic fields containing either a cyclic or pure cubic subfield. We then present three chapters illustrating the applications obtained from a parametric family of polynomials. Two such chapters illustrate that such families may yield an infinite number of monogenic fields. The other illustrates that such families may yield an infinite number of intersective polynomials.
Preface

This thesis is primarily based on the following four papers:

Published:


Accepted:


Submitted:


For each of these papers with multiple authors, each author contributed equally in terms of acquisition and analysis of data and preparation of papers for publishing purposes.
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.4</td>
<td>Future Research</td>
<td>48</td>
</tr>
<tr>
<td>Chapter 6</td>
<td>Lifting Monogenic Cubic Fields to Sextic Fields</td>
<td>51</td>
</tr>
<tr>
<td>6.1</td>
<td>Preliminaries</td>
<td>51</td>
</tr>
<tr>
<td>6.2</td>
<td>Important Lemmas</td>
<td>55</td>
</tr>
<tr>
<td>6.3</td>
<td>Main Theorem</td>
<td>162</td>
</tr>
<tr>
<td>6.4</td>
<td>Future Research</td>
<td>168</td>
</tr>
<tr>
<td>Chapter 7</td>
<td>Intersective Polynomials with Galois Group $D_5$</td>
<td>171</td>
</tr>
<tr>
<td>7.1</td>
<td>Preliminaries</td>
<td>173</td>
</tr>
<tr>
<td>7.2</td>
<td>Important Lemmas</td>
<td>176</td>
</tr>
<tr>
<td>7.3</td>
<td>Main Theorem</td>
<td>178</td>
</tr>
<tr>
<td>7.4</td>
<td>Future Research</td>
<td>184</td>
</tr>
<tr>
<td>7.5</td>
<td>Conclusion</td>
<td>185</td>
</tr>
<tr>
<td>Bibliography</td>
<td></td>
<td>186</td>
</tr>
<tr>
<td>Appendix A: Maple Code</td>
<td></td>
<td>190</td>
</tr>
</tbody>
</table>
## List of Tables

<table>
<thead>
<tr>
<th>Table</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table 2.1.1</td>
<td>Summary of Galois Groups for Irreducible Polynomials</td>
<td>4</td>
</tr>
<tr>
<td>Table 6.2.2</td>
<td>Lifting Monogenic Cubic Fields - Lemma 6.2.1</td>
<td>86</td>
</tr>
<tr>
<td>Table 6.2.3</td>
<td>Lifting Monogenic Cubic Fields - Lemma 6.2.2</td>
<td>121</td>
</tr>
<tr>
<td>Table 6.2.4</td>
<td>Lifting Monogenic Cubic Fields - Lemma 6.2.4</td>
<td>122</td>
</tr>
<tr>
<td>Table 6.2.5</td>
<td>Lifting Monogenic Cubic Fields - Lemma 6.2.7</td>
<td>149</td>
</tr>
<tr>
<td>Table 6.3.6</td>
<td>Lifting Monogenic Cubic Fields - Theorem 6.3.1</td>
<td>163</td>
</tr>
<tr>
<td>Table 7.3.7</td>
<td>Intersective Polynomials - Example 7.3.2</td>
<td>184</td>
</tr>
</tbody>
</table>
List of Symbols

\(\mathbb{Z}\) ................................ Set of integers
\(\mathbb{Q}\) ................................ Set of rationals
\(\mathbb{R}\) ................................ Set of real numbers
\(\mathbb{C}\) ................................ Set of complex numbers
\(\mathbb{Z}_p\) ................................ Set of integers modulo \(p\)
\(D(f)\) .................................. Discriminant of a polynomial \(f(x)\)
\(N(\alpha)\) ................................ Norm of \(\alpha\)
\(Tr(\alpha)\) ................................ Trace of \(\alpha\)
\(K : \mathbb{Q}\) .............................. Degree of \(K\) over \(\mathbb{Q}\)
\(Gal(K/\mathbb{Q})\) ......................... Galois group of \(K\) over \(\mathbb{Q}\)
\(Gal(f(x))\) .............................. Galois group of the splitting field of \(f(x) \in F[x]\) over \(F\)
\(S_n\) ...................................... Symmetric group of order \(n!\)
\(C_n\) ...................................... Cyclic group of order \(n\)
\(D_n\) ...................................... Dihedral group of order \(2n\)
\(A_n\) ...................................... Alternating group of order \(n!/2\)
\(V = \mathbb{Z}_2 \times \mathbb{Z}_2\) .................. Klein four-group of order 4
\(Tr_{L/K}(\alpha)\) ........................ Relative trace of \(\alpha\)
\(N_{L/K}(\alpha)\) .......................... Relative norm of \(\alpha\)
\(O_K\) ..................................... Ring of integers in the number field \(K\)
\(d(K)\) .................................... Field discriminant of the field \(K\)
\(\Delta(\beta_1, \ldots, \beta_n)\) ............... Discriminant of \(\{\beta_1, \ldots, \beta_n\}\)
\(\text{ind}(\theta)\) .......................... Index of \(\theta\)
\(\langle p \rangle\) ................................ Prime ideal
\(N(I)\) ................................... Norm of ideal \(I\)
\(G(\wp)\) .................................. Decomposition group for prime ideal \(\wp\)
\(\text{irr}_Q(\theta)\) .......................... Minimal polynomial of \(\theta\)
Acknowledgements

Firstly, I would like to thank my supervisors Dr. Blair Spearman and Dr. Qiduan Yang for their guidance and constructive criticism throughout my postgraduate studies. Their advice and constant support have proved invaluable and the completion of this thesis would not have been possible without them. I would also like to thank my committee member Dr. Shawn Wang for his help, not only in the completion of this thesis, but in the completion of my degree as well.

Furthermore, I would like to acknowledge and express my appreciation to Dr. Blair Spearman. The confidence you have instilled in me and the support you have given played a crucial role in the completion of my degree. I know the successes I have obtained throughout these last ten years are because you believed in me and as a result made me believe in myself. Lastly, I would like to thank my family and friends for their constant support and encouragement throughout my post-secondary experience.
Dedication

I would like to dedicate this thesis to my family and friends. The never ceasing love and support you have given me during these years have been invaluable.
Chapter 1

Introduction

In this thesis we examine the construction and applications of parametric families of polynomials. Currently methods exist to determine the Galois group of an irreducible polynomial of specified degree. However, we are often interested in what is known as the Inverse Galois Problem. That is, given a finite group $G$, is it possible to find an explicit polynomial of specified degree over the rational numbers whose Galois group is the prescribed group $G$? Moreover, is it possible to find an explicit formula that gives all irreducible polynomials whose Galois group and degree are specified? In finding such an explicit formula, the construction of parametric families of polynomials was formed.

In the early nineteenth century, the following result known as the Kronecker-Weber Theorem was posed (and later proved).

**Theorem 1.0.1** Any finite abelian group $G$ occurs as a Galois group over $\mathbb{Q}$. Indeed, $G$ is realized as the Galois group of a subfield of the cyclotomic field $\mathbb{Q}(\zeta)$ where $\zeta$ is an $n^{th}$ root of unity for some natural number $n$.

As for the actual polynomials with Galois group $G$ described above, examples were constructed using a certain kind of sum of roots of unity known as Gaussian periods. However, the first systematic approach to the Inverse Galois Problem was first studied by Hilbert in 1892. He established the following result.

**Theorem 1.0.2** For any $n \geq 1$, the symmetric group $S_n$ and the alternating group $A_n$ occur as Galois groups over $\mathbb{Q}$.

In regards to his theorem, Hilbert was able to construct a parametric family of polynomials whose Galois group is $S_n$, however, was unable to construct one for $A_n$ (in
fact, this problem remains open). Over time, more research has been done on the Inverse Galois Problem, showing more different groups $G$, both solvable and nonsolvable, are realizable as a Galois group over $\mathbb{Q}$ by constructing parametric families of polynomials whose Galois group is the prescribed group $G$. The search for parametric families and strategies for their construction is still an active area of research. A more comprehensive survey of the problem of constructing families of polynomials with prescribed Galois group can be found in [13]. Applications of families of polynomials can range into many areas of mathematics involving the study of polynomials as seen in the following studies.

The study of polynomials defining number fields and the problem of determining whether or not these number fields are monogenic (that is, they have a power basis) is an important problem in the area of algebraic number theory. In studying such problems, mathematicians have developed more efficient and algorithmic methods for solving diophantine equations - equations prevalent in not only mathematics but other life sciences such as chemistry. For example, in balancing equations or determining the molecular formula of a compound, one must solve a diophantine equation. Hence, the study of monogenic fields contributes greatly to the constructive theory of diophantine equations. Dedekind first proved in 1878 that not every algebraic number field is monogenic. Moreover, for algebraic number fields of given degree and Galois group of their normal closure, power bases may be quite rare. For instance, there is only one cyclic quintic field with a power basis as shown in [11] and the same phenomenon occurs for octic fields with Galois group 2 elementary abelian as seen in [24]. A more lengthy history of the study of monogenic fields can be found in [10]. Finding monogenic fields using already constructed families of polynomials makes the search for such rare fields more attainable.

The study of intersective polynomials (polynomials with roots modulo every positive integer) is a recent area of study and their existence depends on properties of their
Galois group. Simple conditions exist to determine whether or not a polynomial is intersective (see [2]) as well as methods for constructing them (see [31]), however, examples of such polynomials in general seem to be scarce. Making use of already constructed parametric families of polynomials with certain Galois groups certainly makes finding these intersective polynomials easier.

The contents of this thesis are divided into three major parts. Chapters 2 and 3 begin with some background information and then an introduction to parametric families of polynomials and the reason for their construction. Moreover, we give two important examples of parametric families that will be studied later on. Chapter 4 is devoted to our own construction of parametric families of polynomials. Specifically, we study sextic trinomials of the form $x^6 + ax + b$. Our main goal is to construct a parametrization of the coefficients $a$ and $b$ such that the sextic trinomial $x^6 + ax + b$ defines a sextic field containing a cubic subfield. We then use this parametrization to look at specific cases of the cubic subfield (in particular, when the cubic subfield is a pure cubic field or a cyclic cubic field). We also examine existing parameterizations of sextic trinomials of the form $x^6 + ax + b$ and compare our results. Lastly, we give the reader numerous examples of future research in this area of study. In the remaining Chapters 5, 6 and 7, we show two major applications to constructing parametric families of polynomials. The first application in constructing a parametric family of polynomials is to show that such a family defines monogenic fields. Since monogeneity is not a common occurrence, finding a family of polynomials that yield an infinite number of monogenic fields is an important result in this area of active research. Our second application is using a parametric family of polynomials to construct an infinite family of intersective polynomials. Once again, intersective polynomials are rare and so constructing an infinite number of such polynomials is of great significance. Moreover, we also give the reader more examples of future research in the area of applications of parametric families of polynomials.
Chapter 2

Background

2.1 Possible Galois Groups

The following is a summary of the possible Galois groups for irreducible polynomials of the specified degree (TABLE 2.1.1). Note that for sextic polynomials there are 16 possible Galois groups, up to isomorphism.

Table 2.1.1: Summary of Galois Groups for Irreducible Polynomials

<table>
<thead>
<tr>
<th>Quadratic</th>
<th>Cubic</th>
<th>Quartic</th>
<th>Quintic</th>
</tr>
</thead>
<tbody>
<tr>
<td>$C_2$</td>
<td>$S_3$</td>
<td>$S_4$</td>
<td>$S_5$</td>
</tr>
<tr>
<td>$C_3$</td>
<td>$A_4$</td>
<td>$A_5$</td>
<td></td>
</tr>
<tr>
<td>$V = \mathbb{Z}_2 \times \mathbb{Z}_2$</td>
<td></td>
<td>$F_{20}$</td>
<td></td>
</tr>
<tr>
<td>$C_4$</td>
<td></td>
<td>$C_5$</td>
<td></td>
</tr>
<tr>
<td>$D_4$</td>
<td></td>
<td>$D_5$</td>
<td></td>
</tr>
</tbody>
</table>

A comprehensive study on the computation of Galois groups of irreducible polynomials of degree less than seven can be found in [6] (pp. 322-333).

2.2 Relative Trace and Norm

In order to prove one of our main results, we need to first generalize our concepts of the norm and trace of an algebraic number.

**Definition 2.2.1** Let $K, L$ be number fields satisfying $K \subset L$. Let $\sigma_1, \sigma_2, \ldots, \sigma_n$ be the $n = [L : K]$ embeddings (i.e. injective homomorphisms) of $L$ in $\mathbb{C}$ that fix $K$. Let $\alpha \in L$. Then define the relative trace and relative norm as follows:

\[
T_{L/K}(\alpha) = \sigma_1(\alpha) + \sigma_2(\alpha) + \ldots + \sigma_n(\alpha)
\]

\[
N_{L/K}(\alpha) = \sigma_1(\alpha)\sigma_2(\alpha)\ldots\sigma_n(\alpha).
\]
The following is Proposition 4.3.2(1), p. 162, [6].

**Theorem 2.2.2** Let $\alpha \in L$ and let $f(x) = \sum_{i=0}^{m} a_i x^i$ be the minimal polynomial of $\alpha$ over $K$. Also, let $n = [L : K]$. Then

$$
T_{L/K}(\alpha) = \frac{n}{m} Tr(\alpha) \\
N_{L/K}(\alpha) = N(\alpha)^\frac{n}{m}
$$

where

$$
Tr(\alpha) = -\frac{a_{m-1}}{a_m} \\
N(\alpha) = (-1)^m \frac{a_0}{a_m}.
$$

**Remark 2.2.3** Let $\theta$ be a root of an irreducible sextic trinomial of the form $x^6 + Ax + B$. Since there is no $x^5$ term, $Tr(\theta) = 0$. 


Chapter 3

Parametric Families of Polynomials

3.1 Construction and Applications

A well known, however unsolved, problem in Galois theory is what is known as the Inverse Galois Problem. It is composed of two parts (see [13]):

(1) Determine whether a finite group \( G \) occurs as a Galois group over a field \( K \).

(2) If (1) holds, construct explicit polynomials over \( K \) having \( G \) as a Galois group.

More generally, construct a family of polynomials over \( K \) having \( G \) as a Galois group. We call such a family a parametric family of polynomials.

Ideally, we would like the family of polynomials we construct to give all polynomials having \( G \) as their Galois group. We now give examples of two important parametric families of polynomials.

3.2 Parametric Family of Degree Five

An example of a parametric family of polynomials is the family of quintic polynomials studied by A. Brumer ([4]) and T. Kondo ([14]). This family of quintics is given by

\[
R_{a,b}(x) = x^5 + (a - 3)x^4 + (b - a + 3)x^3 + (a^2 - a - 1 - 2b)x^2 + bx + a
\]

where \( a, b \in \mathbb{Z} \). For our purposes, we set \( a = 1 \), in the above expression, to get

\[
F_b(x) = x^5 - 2x^4 + (b + 2)x^3 - (2b + 1)x^2 + bx + 1
\]
where \( b \in \mathbb{Z} \). If \( 4b^3 + 28b^2 + 24b + 47 \) is squarefree then \( Gal(F_b(x)) \cong D_5 \). It was proved in [18], this family of quintics yields an infinite set of distinct monogenic quintic fields whose normal closure has Galois group isomorphic to the dihedral group \( D_5 \) of order 10.

### 3.3 Parametric Family of Degree Seven

In his paper [16], Samuel E. LaMacchia constructs a family of polynomials of degree seven over \( \mathbb{Q} \) with Galois group isomorphic to \( \text{PSL}(2, 7) \) or \( 7T5 \) - the projective special linear group of \( 2 \times 2 \) matrices whose entries are in the finite field with 7 elements (that is, \( F_7 \)). Note that the group \( \text{PSL}(2, 7) \) is isomorphic to the group \( \text{GL}(3, 2) \) - the general linear group of \( 3 \times 3 \) invertible matrices whose entries are in \( F_2 \).

LaMacchia begins with a certain polynomial

\[
f(x) = f(x, a) = (x + 1) \cdot p_1(x, a) \cdot p_2(x, a)
\]

with

\[
p_1(x, a) = x^3 + 2(1 - 2a)x^2 + 2(-1 + 4a)x - 4a
\]

and

\[
p_2(x, a) = x^3 - (1 + 2a)x^2 + 2ax + 2a^2
\]

where \( a \) is indeterminate. Then, using properties of symmetry, he is able to define

\[
f(a, A, x) = f(x) + Ax^3(1 - x)
\]

where \( A \) is indeterminate. These polynomials have Galois group \( \text{PSL}(2, 7) \) and can be written as the family of polynomials
\[ f(a, A, X) = X^7 + 2(1 - 3a)X^6 + (-3 + 4a + 8a^2)X^5 + (-2 + 6a - 14a^2)X^4 \]
\[ + (2 - 4a + 6a^2 - 8a^3)X^3 + 8(2 + a)a^2X^2 + 4(-3 + 2a)a^2X \]
\[ - 8a^3 + AX^3(1 - X) \]

where \( a \) and \( A \) are parameters and the family of polynomials is in \( \mathbb{Q}(a, A)[X] \). We will examine this family in more detail in a later chapter. We will go on to show that this family gives an infinite set of distinct monogenic septimic fields whose normal closure has Galois group \( \text{PSL}(2, 7) \).
Chapter 4

Sextic Fields Containing any Cubic Subfield

A trinomial is defined to be a polynomial consisting of three terms. There are many properties of trinomials that make them interesting to study as well as make difficult problems easier to solve. For example, finding the discriminant of an $n$th degree polynomial can be nearly impossible to do by hand for large $n$. However, it is an easier task to find the general formula of the discriminant of the trinomial $x^n + Ax + B$ (p. 148, [6]).

In regards to the Inverse Galois Problem, much study has been done on trinomials of smaller degree. In his paper [29], F. Seidelmann presents, for each possible Galois group, explicit formulas of all reduced cubic and quartic polynomials. Hence, cubic or quartic trinomials with prescribed Galois group can be parametrized by adapting Seidelmann’s formula. In 1885, George Paxton Young found a parameterization of solvable quintic trinomials and since then, much study has been devoted to this problem of finding parameterizations of all solvable quintics. Spearman and Williams give a characterization of all solvable quintic trinomials in their paper [35]. Solvable sextic trinomials define sextic fields containing either a quadratic or cubic subfield. Malle gives a parametrization for both cases in [20] and we prove this then characterizes all solvable sextic trinomials.

Specifically, we will be considering irreducible sextic trinomials of the form $f(x) = x^6 + Ax + B$ where $f(x)$ is a polynomial with rational coefficients and $K$ denotes a field extension of finite degree over the rational numbers $\mathbb{Q}$. We say that $f(x)$ defines $K$ if $K = \mathbb{Q}(\theta)$ for some root $\theta$ of $f(x)$. Because the second-highest power coefficient in $f(x)$ is 0 (as we are only considering trinomials of the form $x^6 + Ax + B$), the trace
$T_{K/Q}(\theta) = 0$. It is from this fact that the results in this chapter can be established.

The purpose of this part of the thesis is to illustrate a method that constructs a parametric family of sextic trinomials defining sextic fields containing a cubic subfield. As a result, we are able to give a parametrization of all sextic trinomials of the form $x^6 + ax + b$ defining sextic fields containing a cubic subfield. We then will look at two established results and illustrate that these are just specializations of our parametrization. Existing parameterizations of such trinomials will also be studied as well as topics for future study in this area of mathematics.

4.1 Preliminaries

**Definition 4.1.1** If for a ring $R$ a positive integer $n$ exists such that $n \cdot a = 0$ for all $a \in R$, then the least such positive integer is the characteristic of the ring $R$. If no such positive integer exists, then $R$ is of characteristic 0.

For example, the fields $\mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$ all have characteristic 0. The field $\mathbb{Z}_p$ where $p$ is prime has characteristic equal to $p$. We now wish to introduce the concept of the resultant which will be needed in our calculations for the proof of our main theorem.

**Definition 4.1.2** The resultant of two monic polynomials over a field $K$ is defined as the product of the differences of their roots in an algebraic closure of $K$. That is, for polynomials $P$ and $Q$ over a field $K$, the resultant of $P$ and $Q$ is given by

$$\prod_{(x,y): P(x) = Q(y) = 0} (x - y).$$

Note that the resultant is the determinant of the Sylvester matrix associated to polynomials $P$ and $Q$. Moreover, the resultant is a polynomial expression of the coefficients of polynomials $P$ and $Q$, which is equal to zero if and only if the polynomials have a common root. Lastly, if we take the resultant of the polynomial $f(X)$ and
$f(x - X)$, this then yields a polynomial in terms of the coefficients of the polynomial $f$ whose roots are the sum of pairs of roots of $f$ (see [6], pp. 119-121).

### 4.2 Important Lemmas

**Lemma 4.2.1** Let $K$ be a field of characteristic zero. Suppose that $A$ and $B$ are nonzero elements of $K$ such that $f(x) = x^6 + Ax + B$ is irreducible over $K$, and that for some root $\theta$ of $f(x)$ in an algebraic closure of $K$, $K(\theta)$ is a sextic extension of $K$ containing a cubic subfield $E$. Then there exists a root $\theta' \neq \theta$ of $f(x)$ such that $\theta + \theta'$ is a root of an irreducible cubic polynomial $x^3 + ax + b \in K[x]$ defining $E$.

**Proof.** Let $K(\theta)$ denote the sextic field specified in the statement of the Lemma and let $E$ denote its cubic subfield. Since $[K(\theta) : K] = 6$, the minimal polynomial of $\theta$ over $K$ must be of degree six. Since the degree of the monic polynomial $f(x)$ is also six and $f(\theta) = 0$, we conclude $f(x)$ is the minimal polynomial of $\theta$ over $K$.

Let $h(x)$ denote the minimal polynomial of $\theta$ over $E$. Since $[K(\theta) : K] = 6$ and $[E : K] = 3$, we conclude $[K(\theta) : E] = 2$ and so $h(x)$ must have degree equal to two. Moreover, since $\theta$ is a root of $f(x) \in K[x] \subseteq E[x]$, we also conclude $h(x) \mid f(x)$ in $E[x]$.

Since $K(\theta)/E$ is a separable extension, the minimal polynomial of $\theta$ over $E$, namely $h(x)$, has no multiple zeroes. Hence, there exists a root $\theta' \neq \theta$ of $h(x)$ (and hence of $f(x)$). So

$$h(x) = (x - \theta)(x - \theta') \in E[x]$$

then implies $\theta + \theta' \in E$. Recall $[E : K] = 3$ and so the only subfields of $E$ are itself and $K$. So we have

$$K \subseteq K(\theta + \theta') \subseteq E$$

implies

$$K(\theta + \theta') = K$$
or

\[ K(\theta + \theta') = E. \]

Thus, \( \theta + \theta' \) is either an element of \( K \) or it is a root of an irreducible cubic polynomial in \( K[x] \).

By way of contradiction, assume \( \theta + \theta' \in K \Leftrightarrow \theta + \theta' = r \) for some \( r \in K \). Taking the trace of both sides of the latter equation from \( K(\theta) \) to \( K \) we obtain

\[ Tr_{K(\theta)/K}(\theta + \theta') = Tr_{K(\theta)/K}(r). \]

By properties of trace (p. 163, [6]), we have

\[ Tr_{K(\theta)/K}(\theta + \theta') + Tr_{K(\theta)/K}(\theta') = Tr_{K(\theta)/K}(r). \]

Since the minimal polynomial of \( \theta \) over \( K \) is \( f(x) = x^6 + Ax + B \), we have \( Tr_{K(\theta)/K}(\theta) = 0 \) (as \( f(x) \) has no \( x^5 \) term). We also know that the minimal polynomial of \( \theta' \) over \( K \) must also be \( f(x) \) as \( f(\theta') = 0 \) and is monic and irreducible over \( K \). Hence, \( Tr_{K(\theta)/K}(\theta') = 0 \). So we have

\[ Tr_{K(\theta)/K}(r) = 0. \]

Since \( r \in K \), the minimal polynomial of \( r \) over \( K \) must be \( m(x) = x - r \). By Theorem 2.2.2,

\[ Tr_{K(\theta)/K}(r) = 6 \cdot r \]

and so

\[ 6r = 0 \quad \Rightarrow \quad r = 0 \]

\[ \Rightarrow \theta + \theta' = 0 \]

\[ \Rightarrow \theta' = -\theta. \]
So we deduce that both $\theta$ and $-\theta$ are roots of $f(x)$. We now have

\[
\begin{align*}
\theta^6 + A\theta + B &= 0 \\
\theta^6 - A\theta + B &= 0
\end{align*}
\]

which implies $2A\theta = 0$. Now $\theta \neq 0$ since $f(0) = B \neq 0$. So we must have $A = 0$, a contradiction. So we conclude that $\theta + \theta'$ is a root of an irreducible cubic polynomial in $K[x]$. 

We now calculate $Tr_{E/K}(\theta + \theta')$ using Theorem 2.2.2. We have

\[
Tr_{E/K}(\theta + \theta') = \frac{3}{6} Tr_{K(\theta)/K}(\theta + \theta') = \frac{1}{2} \cdot 0 = 0.
\]

Since $Tr_{E/K}(\theta + \theta')$ represents the $-(n-1)^{st}$ coefficient of the minimal polynomial of $\theta + \theta'$ (as the minimal polynomial is monic, see Theorem 2.2.2), we conclude $\theta + \theta'$ is a root of an irreducible polynomial of the form $x^3 + ax + b$. This polynomial defines $E$ as one of its roots is $\theta + \theta' \in E$ and $[E : K] = 3$. □

### 4.3 Main Theorem

We wish to characterize sextic trinomials over a field $K$ of characteristic equal to zero defining sextic fields containing any cubic subfield. Note that not only are we generalizing the cubic subfield, but we are also considering our polynomial with coefficients in a field $K$ of characteristic equal to zero.

**Theorem 4.3.1** Let $K$ be a field of characteristic zero. Suppose that $A$ and $B$ are nonzero elements of $K$ such that $f(x) = x^6 + Ax + B$ is irreducible over $K$. Then $f(x)$ defines a sextic field containing a cubic subfield if and only if there exist elements
\[ u \text{ and } v \text{ in } K \text{ such that} \]
\[ A = (3u + 23)(u - 9)(u + 9)^2(4u + 39)^3v^5 \]
\[ B = (u + 11)(u - 9)(u^2 + 7u - 19)(u + 9)^2(4u + 39)^3v^6. \]

**Proof.** (\( \Leftarrow \)) Assume \( f(x) = x^6 + Ax + B \in K[x] \) defines a sextic field containing a cubic subfield extension \( E \) of \( K \). Let \( \theta \) be a root of \( f(x) \) in an algebraic closure of \( K \) such that \( K(\theta) \) contains \( E \). By Lemma 4.2.1, there exists a root \( \theta' \neq \theta \) of \( f(x) \) such that \( \theta + \theta' \) is a root of an irreducible trinomial \( g(x) = x^3 + ax + b \in K[x] \) defining \( E \).

We now find a polynomial whose coefficients are a function of \( A \) and \( B \) and which has \( \theta + \theta' \) as a root. We calculate the polynomial, which we denote by \( s(x) \), using

\[
\sqrt{\text{Resultant}(f(x - X), f(X))} / 2^6 f(x/2).
\]

MAPLE\textsuperscript{TM} gives the polynomial as

\[
s(x) = x^{15} - 10Ax^{10} - 26Bx^9 - 12A^2x^5 + 18ABx^4 - 27B^2x^3 - A^3.
\]

The minimal polynomial of \( \theta + \theta' \), namely \( g(x) \), must divide \( s(x) \) as \( s(\theta + \theta') = 0 \).

We formally divide \( s(x) \) by \( g(x) \) using MAPLE\textsuperscript{TM} and equate each of the coefficients of \( x^2, x \) and the constant term to zero. This gives us the following three equations:

\[
78a^2bB - 10a^2b^3 - 10a^4A + 30ab^2A - 18aAB + 12bA^2 + 6a^5b = 0, \quad (1)
\]
\[
15a^4b^2 - 40a^3bA - 5ab^4 - 26a^4B + 78ab^2B - 12a^2A^2 - a^7 + 27aB^2 - 18bAB + 10b^3A = 0, \quad (2)
\]
\[
-A^3 - a^6b - 26a^3bB + 26b^3B + 10a^3b^3 - b^5 - 30a^2b^2A + 27bB^2 - 12abA^2 = 0. \quad (3)
\]

We will solve these equations for \( A \) and \( B \).
First assume \( a = 0 \). Then equation (1) reduces to

\[
12bA^2 = 0.
\]

Now \( A \neq 0 \) as we are assuming \( f(x) \) is a trinomial. Hence, \( b = 0 \). But this then implies \( g(x) = x^3 \), a reducible cubic over \( K \) and hence a contradiction. Thus, we may assume \( a \neq 0 \).

Now assume \( A = \frac{12}{3}ab \). Then equation (1) becomes

\[
-\frac{28}{3}a^2b(-37b^2 + 4a^3) = 0.
\]

As seen previously, we know \( a \neq 0 \). If \( b = 0 \) then \( g(x) = x^3 + ax = x(x^2 + a) \), a reducible cubic and hence a contradiction. This then implies

\[
-37b^2 + 4a^3 = 0.
\]

The solutions to this equation, in \( K \), are

\[
(a, b) = (37k^2, 74k^3)
\]

where \( k \in K \). Furthermore, \( k \) is nonzero since \( a \) and \( b \) are the coefficients of an irreducible cubic over \( K \). Substituting these values of \( a \) and \( b \) in equations (1), (2) and (3) and solving for \( A \) and \( B \) yields

\[
A = \frac{35594k^5}{3}
\]

\[
B = \frac{2487473k^6}{27}
\]
or

\[ A = 814k^5 \]
\[ B = -2109k^6. \]

These values of \( A \) and \( B \) then give rise to trinomials

\[ x^6 + \frac{35594k^5}{3}x + \frac{2487473k^6}{27} \]

and

\[ x^6 + 814k^5x - 2109k^6 \]

both of which define sextic fields containing a cubic subfield (as their Galois group is isomorphic to \( 6T11 \) or \( S_4 \times C_2 \)). Both of these trinomials are accounted for in our theorem by choosing

\[ (u, v) = \left( \frac{93}{2}, \frac{2k}{225} \right) \]
\[ (u, v) = \left( -\frac{19}{2}, 2k \right), \]

respectively.

Henceforth, we may assume \( a \neq 0 \) and \( A \neq \frac{13}{3}ab \). So solving for \( B \) in equation (1) yields

\[ B = \frac{1}{3} \frac{-5a^2b^3 - 5a^4A + 15ab^2A + 6bA^2 + 3a^5b}{a(-13ab + 3A)}. \]

We substitute \( B \) into equation (2) giving

\[ -\frac{1}{3} \frac{FG}{(-13ab + 3A)^2} = 0 \]  \hspace{1cm} (4)

where

\[ F = 3a^2A^2 - 10a^3bA - 36b^3A + 3a^4b^2 + 8ab^4 \]
\[ G = 108A^2 - 196a^5 + 30abA - 345a^2b^2. \]
In order for equation (4) to hold, either $F = 0$ or $G = 0$. Suppose first that $G = 0$. Viewing this equation as a quadratic in $A$ we see that its discriminant must be equal to a perfect square in $K$. This discriminant is equal to

$$1764a^2(48a^3 + 85b^2).$$

Using standard parametrization methods we find that

$$b = \frac{1}{48} \frac{-85 + w^2}{t^3}$$

and

$$a = bt = \frac{1}{48} \frac{-85 + w^2}{t^2}$$

for some elements $t$ and $w$ in $K$ with $t \neq 0$. Substituting equations (5) and (6) into $G = 0$ and solving for $A$ gives two solutions for $A$ in terms of $w$ and $t$. Since the second solution is equivalent to the first under the transformation $w \rightarrow -w$, we may choose the first solution which is given by

$$A = \frac{(7w - 5)(w^2 - 85)^2}{82944t^5}. \quad (7)$$

Substituting the equations (5), (6) and (7) into (1) gives

$$B = -\frac{5(w^2 - 85)^2(w^2 + 8w - 29)}{995328t^6}. \quad (8)$$

These values of $a$, $b$, $A$ and $B$ given in equations (5), (6), (7) and (8) do not satisfy equation (3) so we do not consider them further.

Now we turn to the equation $F = 0$. Again, viewing this equation as a quadratic in $A$ we see that its discriminant must be equal to a perfect square in $K$. This discriminant is equal to

$$16b^2(27b^2 + 4a^3)(3b^2 + a^3).$$
Substituting $a = bt$ in this discriminant, taking the squarefree part and equating to $z^2$, for $z \in K$, gives

$$(27 + 4bt^3)(3 + bt^3) = z^2.$$  

If we now set $z = w \left( b + \frac{3}{t^3} \right)$ for $w \in K$ in this equation and solve for $b$ we obtain

$$b = -\frac{3}{t^3}$$

or

$$b = \frac{-3(-w^2 + 9t^6)}{t^3(-w^2 + 4t^6)}.$$  

First we consider the case where $b = -\frac{3}{t^3}$. Thus, $a = bt = -\frac{3}{t^3}$. So from $F = 0$ we obtain $A = -\frac{3}{t^3}$. Substituting these values into equation (1), we obtain $B = \frac{5}{t^6}$. The resulting trinomial is then

$$f(x) = x^6 - \frac{3}{t^5}x + \frac{5}{t^6}$$

which defines a sextic field containing a cubic subfield (as its Galois group is isomorphic to $6T11$). This trinomial is accounted for in our theorem by choosing

$$(u, v) = \left(-6, \frac{1}{15t}\right).$$

Let’s now consider the case where $b = \frac{-3(-w^2 + 9t^6)}{t^3(-w^2 + 4t^6)}$. For convenience, we set $w = \frac{t^3(2u+27)}{u+6}$, for some elements $t, u \in K$. Note that the special case where $u = -6$ is considered above. So we obtain

$$b = \frac{(u - 9)(u + 9)}{t^3(4u + 39)} \quad (9)$$

and so

$$a = bt = \frac{(u - 9)(u + 9)}{t^2(4u + 39)}. \quad (10)$$
We note that the special case where $4u + 39 = 0$ does not lead to any trinomials defining sextic fields containing a cubic subfield. We now substitute equations (9) and (10) into $F = 0$ and solve for $A$. We obtain two solutions for $A$ in terms of $u$ and $t$. Since the second solution is equivalent to the first under the transformation $u \rightarrow -\frac{3(13u + 108)}{4u + 39}$, we may choose the first solution which is given by

$$A = \frac{(3u + 23)(u - 9)(u + 9)^2}{(4u + 39)^2t^5}. \quad (11)$$

Substituting equations (9), (10) and (11) into (2) yields

$$B = \frac{(u + 11)(u - 9)(u^2 + 7u - 19)(u + 9)^2}{(4u + 39)^3t^6}. \quad (12)$$

The pair $(A, B)$ given by equations (11) and (12) satisfy all three equations (1), (2) and (3) so we have indeed found all rational solutions to these three equations and hence the set of all trinomials $x^6 + Ax + B$ defining sextic fields containing a cubic subfield. To obtain the final values of $A$ and $B$ as stated in the theorem, we introduce a scaling factor $v$ and a scaling $x \rightarrow \frac{x}{tv(4u + 39)}$, yielding

$$A = (3u + 23)(u - 9)(u + 9)^2(4u + 39)^3v^5$$
$$B = (u + 11)(u - 9)(u^2 + 7u - 19)(u + 9)^2(4u + 39)^3v^6,$$

as required.

$(\Rightarrow)$ Assume $f(x) = x^6 + Ax + B \in K[x]$ is irreducible over $K$ where

$$A = (3u + 23)(u - 9)(u + 9)^2(4u + 39)^3v^5$$
$$B = (u + 11)(u - 9)(u^2 + 7u - 19)(u + 9)^2(4u + 39)^3v^6,$$

for some numbers $u$ and $v$ in $K$. We need to show $f(x)$ defines a sextic field containing a cubic subfield. For convenience, we choose our scaling factor to be $v = 1$ in $f(x)$. 

19
Let \( \theta \) denote a root of \( f(x) \) in an algebraic closure \( C \) of \( K \) and set \( F = K(\theta) \). Since \( f(x) \) is irreducible over \( K \) we have \([F : K] = 6\). Next we give explicitly a cubic polynomial \( g(x) \in K[x] \) which we will use to show that \( F \) has a cubic subfield over \( K \). Define \( g(x) \) by

\[
g(x) = x^3 + (u + 9)(4u + 39)(u - 9)x + (u - 9)(u + 9)(4u + 39)^2.
\]

Let \( \alpha \) denote a root of \( g(x) \) in \( C \). Define the quadratic polynomial \( q(x) \) in \( K(\alpha)[x] \) by

\[
q(x) = (2u + 27)x^2 - (2u + 27)\alpha x + \\
+(4u + 39)\alpha^2 - (20u^2 + 375u + 1755)\alpha + (u + 9)(4u + 39)(2u + 17)(u - 9).
\]

A MAPLE\textsuperscript{TM} calculation shows that

\[
\text{Resultant}(f(x), q(x), x) = (4u + 39)^3 g(\alpha)^2 h(\alpha)
\]

where \( h(\alpha) \) is a quadratic polynomial in terms of \( \alpha \). Recall \( \alpha \) is a root of \( g(x) \) and so

\[
\text{Resultant}(f(x), q(x), x) = 0.
\]

Therefore, there exists a conjugate \( \theta' \) of \( \theta \) over \( K \) such that \( q(\theta') = 0 \). Next we evaluate the field extension degrees \([K(\theta', \alpha) : K]\) and \([K(\alpha) : K]\). Note that

\[
[K(\theta', \alpha) : K] = [K(\theta', \alpha) : K(\alpha)][K(\alpha) : K] \leq 2 \cdot 3 = 6 \quad (13)
\]

since \( \theta' \) satisfies a quadratic polynomial (namely, \( q(x) \)) over \( K(\alpha) \) and \( \alpha \) is a root of a cubic polynomial (namely, \( g(x) \)) in \( K[x] \). Since \( \theta' \) is a conjugate of \( \theta \) over \( K \), it too
must be a root of $f(x)$. Thus $[K(\theta') : K] = [F : K] = 6$. So we obtain

$$[K(\theta', \alpha) : K] = [K(\theta', \alpha) : K(\theta')][K(\theta') : K] \geq 1 \cdot 6 = 6. \quad (14)$$

Combining equations (13) and (14) gives the following:

$$[K(\theta', \alpha) : K] = 6 = [K(\theta') : K].$$

And so we conclude

$$[K(\theta', \alpha) : K(\theta')] = 1 \quad (15)$$

and

$$[K(\alpha) : K] = 3. \quad (16)$$

Equation (15) shows that $\alpha \in K(\theta')$ so that $K(\alpha)$ is a subfield of $K(\theta')$. Furthermore, equation (16) shows that $g(x)$ is irreducible over $K$ so that $K(\alpha)$ is a cubic subfield of $K(\theta')$. Finally, since $K(\theta')$ is isomorphic to the field $F = K(\theta)$, $F$ contains a cubic subfield as well, which completes the proof. \qed

### 4.4 Specializations of Theorem 4.3.1

We will show, using Theorem 4.3.1, we obtain two established results that are just special cases of the cubic subfield. First, we begin with some definitions.

**Definition 4.4.1** A cyclic cubic field is a normal extension of $\mathbb{Q}$ of degree three with Galois group isomorphic to the cyclic group of order three.

**Remark 4.4.2** A cubic polynomial with rational coefficients defines a cyclic cubic field if and only if it is irreducible and its discriminant is of the form $d^2$ for some $d \in \mathbb{Q}$ (see p. 336, [6]).
An example of a cyclic cubic field is the field defined by the polynomial \( g(x) = x^3 + x^2 - 2x - 1 \), whose discriminant is equal to \( 49 = 7^2 \).

The following Theorem was taken from [33] and is a rational parametrization of all sextic trinomials \( x^6 + Ax + B \) defining sextic fields with a cyclic cubic subfield, a special case of Theorem 4.3.1. The author gives a similar method in his derivation of results but we will show how this parametrization can be obtained from our parametrization given in Theorem 4.3.1 by making a simple substitution.

**Theorem 4.4.3** Let \( A \) and \( B \) denote nonzero rational numbers such that \( f(x) = x^6 + Ax + B \) is irreducible. Then \( f(x) \) defines a sextic field containing a cyclic cubic subfield if and only if there exist rational numbers \( u \) and \( v \) such that

\[
A = 4u(u^2 + 3)(3u^2 + 1)(3u^2 + 25)^2v^5 \\
B = (u^2 - 5)(3u^2 + 1)(u^4 + 10u^2 + 5)(3u^2 + 25)^2v^6.
\]

**Proof.** If we let

\[
u = -\frac{1}{4}\left(\frac{25 + 39w^2}{w^2}\right) \\
v = -\frac{4}{25}ew^3
\]

in our formulas for \( A \) and \( B \) in Theorem 4.3.1, we obtain

\[
A = 4w(w^2 + 3)(3w^2 + 1)(3w^2 + 25)^2e^5 \\
B = (w^2 - 5)(3w^2 + 1)(w^4 + 10w^2 + 5)(3w^2 + 25)^2e^6.
\]

Renaming \( w = u \) and \( e = v \) we obtain the parametrization given in this theorem

\[
A = 4u(u^2 + 3)(3u^2 + 1)(3u^2 + 25)^2v^5 \\
B = (u^2 - 5)(3u^2 + 1)(u^4 + 10u^2 + 5)(3u^2 + 25)^2v^6.
\]
We now introduce another definition that will be used to obtain another special case of Theorem 4.3.1.

**Definition 4.4.4** A cubic field is called pure if it can be obtained by adjoining the real cube root $\sqrt[3]{m}$ of a cubefree positive integer $m$ to the rational number field $\mathbb{Q}$.

**Remark 4.4.5** A cubic polynomial with rational coefficients defines a pure cubic field if and only if it is irreducible and its discriminant is of the form $-3d^2$ for some $d \in \mathbb{Q}$ (see p. 343, [6]).

An example of a pure cubic field is $\mathbb{Q}(\sqrt[3]{2})$. It is defined by the polynomial $g(x) = x^3 - 2$ whose discriminant is equal to $-108 = -3 \cdot 6^2$.

The following theorem was taken from [17] and is a rational parametrization of all sextic trinomials $x^6 + Ax + B$ defining sextic fields with a pure cubic subfield. We will show the same results can be obtained by using Theorem 4.3.1.

**Theorem 4.4.6** Let $A$ and $B$ denote nonzero rational numbers such that $f(x) = x^6 + Ax + B$ is irreducible. Then $f(x)$ defines a sextic field containing a pure cubic subfield if and only if there exist rational numbers $u$ and $v$ such that

\[
A = 12u(u^2 - 1)(u^2 - 9)(u^2 - 25)^2v^5 \\
B = -(u^2 - 1)(u^2 - 25)^2(u^2 + 15)(u^4 - 30u^2 + 45)v^6.
\]

**Proof.** If we let

\[
u = \frac{3}{4} \left( \frac{-25 + 13w^2}{w^2} \right) \\
v = \frac{4}{75}ew^3
\]

\]
in our formulas for $A$ and $B$ in Theorem 4.3.1, we obtain

\[ A = 12w(w^2 - 1)(w^2 - 9)(w - 5)^2(w + 5)^2e^5 \]
\[ B = -(w^2 - 1)(w - 5)^2(w + 5)^2(w^2 + 15)(w^4 - 30w^2 + 45)e^6. \]

Renaming $w = u$ and $e = v$ we obtain the parametrization given in this theorem

\[ A = 12u(u^2 - 1)(u^2 - 9)(u^2 - 25)v^5 \]
\[ B = -(u^2 - 1)(u^2 - 25)^2(u^2 + 15)(u^4 - 30u^2 + 45)v^6. \]

\[ \blacksquare \]

### 4.5 Solvable Sextic Trinomials $x^6 + Ax + B$

The notion of a solvable group in group theory allows one to determine whether a polynomial is solvable in radicals, depending on whether its Galois group has the property of solvability. For solvable sextic polynomials defining a sextic field, Galois theory implies that this sextic field contains either a quadratic or cubic subfield. Theorem 4.3.1 gives a parametrization of sextic trinomials defining sextic fields containing a cubic subfield. In order to parametrize all solvable sextic trinomials, we only need to provide now a parametrization of sextic trinomials defining sextic fields containing a quadratic subfield. This calculation is straightforward and provided in the following Remark.

**Remark 4.5.1** *Irreducible sextic trinomials $f(x) = x^6 + Ax + B \in K[x]$ defining sextic fields containing a quadratic subfield are easier to completely parameterize. To begin with, $f(x)$ must be equal to the product of two conjugate cubics (see [15]), with coefficients in a quadratic extension field $K(\sqrt{t})$ of $K$ where $t$ is a nonsquare integer.*
Such cubics have the form

\[ x^3 + (a + b\sqrt{t})x^2 + (c + d\sqrt{t})x + (e + k\sqrt{t}) \]

and

\[ x^3 + (a - b\sqrt{t})x^2 + (c - d\sqrt{t})x + (e - k\sqrt{t}) \]

where \(a, b, c, d, e, k \in K\). Equating the coefficients of \(f(x)\) with the product of these two cubics and solving the resulting system of equations for \(A\) and \(B\) gives a characterization of these sextic trinomials to be

\[ f(x) = x^6 + 4u(3u + 1)v^5x - u(u^2 - 18u + 1)v^6 \tag{17} \]

with \(u, v \in K\).

### 4.6 Malle’s Sextic Trinomials

In [20], Gunter Malle gives a parametric family of sextic trinomials over \(\mathbb{Q}(z)\) defining sextic fields with a cubic subfield. This family is

\[ g_z(x) = x^6 - 6x^5 + \frac{4z^5(z^2 - 45)^5}{27(2z + 15)^2(z - 6)(z^2 - 2z - 15)^3}. \]

Now we wish to compare his family of trinomials with our family of sextics given in Theorem 4.3.1. We first invert and scale \(g_z(x)\) to change the \(x^5\) term to an \(x\) term. Doing so, we obtain the following:

\[ h_z(x) = x^6 - \frac{81}{2}(2z+15)^2(z-6)(z^2-2z-15)^3x + \frac{27}{4}(2z+15)^2(z-6)(z^2-2z-15)^3z(z^2-45). \]

Equating the coefficients of \(h_z(x)\) with our \(A\) and \(B\) values in Theorem 4.3.1 yields
the following solution:

\[
\begin{align*}
  u &= -\frac{1}{3}\frac{(23z-165)}{z-5} \\
v &= \frac{9}{50}(z-5)^2.
\end{align*}
\]

To conclude, when the above \(u\) and \(v\) values are substituted into \(f(x) = x^6 + Ax + B\) where \(A\) and \(B\) are given in Theorem 4.3.1, we obtain \(h_z(x)\). Reversing our "inverting" steps above, we then obtain \(g_z(x)\). Thus our theorem shows that Malle’s trinomials, converted to the form \(x^6 + ax + b\) comprise all trinomials defining sextic fields with a cubic subfield over \(K\).

Malle also gives a family of sextic trinomials over \(\mathbb{Q}(y)\) defining sextic fields with a quadratic subfield. This family is

\[
g_y(x) = x^6 - 6x^5 + \frac{(y^2 - 14y + 4)^5}{27(y - 16)y^3}.
\]

Again, if we invert and scale \(g_y(x)\) to obtain

\[
h_y(x) = x^6 - 162(y - 16)y^3x + 27(y - 16)y^3(y^2 - 14y + 4)
\]

and equate the coefficients of \(h_y(x)\) with our \(A\) and \(B\) values in Remark 4.5.1, we obtain the following solution:

\[
\begin{align*}
  u &= -\frac{1}{3}\frac{y-16}{y} \\
v &= \frac{3}{2}y.
\end{align*}
\]

We now conclude all solvable sextic trinomials have now been characterized.

**4.7 Future Research**

We now have the characterization of sextic trinomials defining sextic fields with either a cubic (Theorem 4.3.1) or quadratic (equation (17)) subfield. Hence, we can try to characterize sextic trinomials defining sextic fields that contain both a cubic and quadratic subfield.
Also, recall from the method used to prove Theorem 4.3.1, we have a system of three equations (equations (1), (2) and (3)). However, in these equations, there are only two unknowns $A$ and $B$. Thus, we can introduce one more unknown, say $C$, into this system of equations and still possibly have a solution. That is, we consider sextic quadrinomials of the form $x^6 + Ax^2 + Bx + C$ defining sextic fields containing a cubic subfield. Thanks to a private communication with A. Bremner, we are confident that we will be able to classify all sextic quadrinomials of the form $x^6 + Ax^2 + Bx + C$ defining a sextic field containing a cyclic cubic subfield and hence, yield results similar to the ones found in Theorem 4.3.1. We then try to generalize these results to sextic fields containing any cubic subfield. More generally, we can extend our method to octic (degree 8) trinomials and quadrinomials that define octic fields containing a quartic subfield to produce similar results.
Chapter 5

PSL(2,7) Monogenic Fields

We now illustrate some applications that can be obtained from a parametric family of polynomials (using both our own and already established constructions). Firstly, such a family may yield an infinite number of monogenic fields. Such a characterization is rare and obtaining an infinite number of such polynomials proves to be of great significance in studies with a long history.

It is a nontrivial problem to decide whether an algebraic number field has a power basis. In fact, for algebraic number fields of given degree and Galois group of their normal closure, power bases may be quite rare. For example, for quintic fields with Galois group isomorphic to the cyclic group of order 5, there is only one such field that has a power basis ([11]). Similarly, for octic fields with Galois group isomorphic to the 2 elementary abelian group (that is, $C_2 \times C_2 \times C_2$), there is only one such group with a power basis ([24]). On the other hand, there are infinitely many quintic fields with Galois group isomorphic to the dihedral group of order 10 that have a power basis ([18]) as well as infinitely many sextic fields with Galois group isomorphic to PSL(2,5) with a power basis ([34]).

We will look at field extensions of $\mathbb{Q}$ of degree seven, also known as septimic fields. Specifically, we study septimic fields whose normal closure has Galois group isomorphic to PSL(2,7), the projective special linear group of $2 \times 2$ matrices over $F_7$. We do so by looking at a parametric family of polynomials, specifically LaMacchia’s parametric family of septimic polynomials, that define septimic fields whose normal closure has Galois group isomorphic to PSL(2,7). The purpose of this chapter is to show that there are infinitely many of these septimic fields with Galois group isomorphic to PSL(2,7) that have a power basis. Presently, our family of septimic monogenic fields is the only degree seven family of monogenic fields in existence.
5.1 Preliminaries

We first introduce some important definitions and theorems.

Definition 5.1.1 The set of all algebraic integers that lie in the algebraic number field $K$ is denoted by $O_K$.

In fact, $O_K$ forms a ring and thus is called the ring of integers of the algebraic number field $K$. Moreover, $O_K$ is an integral domain. The ring of integers of an algebraic number field $K$ consists of those numbers in $K$ whose monic minimal polynomials have integer coefficients.

Definition 5.1.2 An integral basis of an algebraic number field $K$ of degree $n$ is a set $\{\beta_1, \ldots, \beta_n\}$ of $n$ algebraic integers in $K$ such that every element in $O_K$ can be written uniquely in the form $c_1\beta_1 + \ldots + c_n\beta_n$ where $c_i \in \mathbb{Z}$ for $i = 1, \ldots, n$.

Note that a basis of $O_K$ is an integral basis of $K$. Now we can always make a slight adjustment in an integral basis of $K$ so that $\beta_1 = 1$ (Theorem 13, pp. 36-38, [21]). Another result worth mentioning is that every algebraic number field has an integral basis (Theorem 2.10, p. 55, [27]). However, these bases are hard to find. We can explicitly compute such a basis but it is now standard for computer algebra systems such as MAPLE™ to have built-in programs to do this.

We now wish to define the discriminant of an algebraic number field but first, we must describe the discriminant of a set of elements of an algebraic number field $K$.

Definition 5.1.3 Let $K$ be an algebraic number field of degree $n$. If $\{\beta_1, \ldots, \beta_n\}$ is a subset of the field $K$ then we may define a symmetric integral matrix $M$ whose $(i, j)$-entry is defined to be $\text{Tr}(\beta_i \cdot \beta_j)$. The discriminant of $\{\beta_1, \ldots, \beta_n\}$ is then defined as

$$\Delta(\beta_1, \ldots, \beta_n) = \det(M).$$
Definition 5.1.4 Let $K$ be an algebraic number field of degree $n$. If $\{\beta_1, \ldots, \beta_n\}$ is an integral basis of the field $K$ then the field discriminant $d(K)$ of $K$ is defined as

$$d(K) = \Delta(\beta_1, \ldots, \beta_n).$$

Remark 5.1.5 It is important to note that the value of the field discriminant is independent of the integral basis that you choose (see Proposition 2.4, p. 16, [5]).

We have two different discriminants - the discriminant of a polynomial $f(x)$ and the discriminant of an algebraic number field $K$. Using these two discriminants, we introduce the following definition.

Definition 5.1.6 The index of an algebraic number $\theta$ is defined by

$$\text{ind}(\theta) = \frac{\sqrt{D(f)}}{d(K)},$$

where $f$ is the minimal polynomial of $\theta$ and $d(K)$ is the field discriminant of the algebraic number field $K = \mathbb{Q}(\theta)$. Note that the index of an algebraic number $\theta$ is a nonzero integer.

Equivalently, we have

$$D(f) = (\text{ind}(\theta))^2 d(K). \quad (18)$$

As stated before, an integral basis for an algebraic number field $K$ is a basis for $O_K$. Moreover, there is a special case in which the basis is known as a power basis. These specific bases are very rare and also hard to find.

Definition 5.1.7 Let $K$ be an algebraic number field (not necessarily equal to $\mathbb{Q}(\theta)$) of degree $n$. If there exists an element $\theta \in O_K$ such that $\{1, \theta, \theta^2, \ldots, \theta^{n-1}\}$ is an integral basis for $K$ then $K$ is said to be monogenic and the integral basis $\{1, \theta, \theta^2, \ldots, \theta^{n-1}\}$ is called a power basis for $K$. 

30
Now we can find power bases based on the index of the element $\theta$ as seen in the following theorem.

**Theorem 5.1.8** Let $K$ be an algebraic number field of degree $n$. Let $\theta \in O_K$ such that $K = \mathbb{Q}(\theta)$. Then $\{1, \theta, \theta^2, \ldots, \theta^{n-1}\}$ is an integral basis for $K$ if and only if $\text{ind}(\theta) = \pm 1$.

**Remark 5.1.9** If $\text{ind}(\theta) = 1$ then $\{1, \theta, \theta^2, \ldots, \theta^{n-1}\}$ is a power basis for $K$.

Now we introduce a few basic definitions from Ideal theory.

**Definition 5.1.10** Let $K$ be an algebraic number field and $O_K$ its ring of integers. An ideal $I$ of $O_K$ is a subring of $O_K$ with the property

$$\forall a \in O_K, aI \subseteq I.$$ 

An ideal $I$ of $O_K$ is called a proper ideal of $O_K$ if $\{0\} \subset I \subset O_K$.

We say an ideal $I$ of $O_K$ is closed under external multiplication by elements of $O_K$.

**Definition 5.1.11** A proper ideal $I$ of $O_K$ is called a prime ideal if

$$a, b \in O_K \text{ and } ab \in I \Rightarrow a \in I \text{ or } b \in I.$$ 

**Definition 5.1.12** A principal ideal is an ideal $I$ of $O_K$ that is generated by a single element $\alpha \in O_K$.

We can generalize our definition of the norm of an algebraic element to the norm of an ideal.

**Definition 5.1.13** Let $K$ be an algebraic number field and $O_K$ its ring of integers. Let $I$ be a nonzero ideal of $O_K$. Then the norm of $I$ is defined to be

$$N(I) = [O_K : I].$$
We can simplify this definition if the ideal is principal (see Theorem 22(c), p. 65, [21]).

**Proposition 5.1.14** Let $\alpha$ be a nonzero element of an algebraic number field $K$ such that $\langle \alpha \rangle$ is a principal ideal of $O_K$. Then

$$N(\langle \alpha \rangle) = |N(\alpha)|.$$

In other words, the norm of a principal ideal is equal to the absolute value of the norm of a generating element.

The norm is also completely multiplicative (see Theorem 22(a), p. 65, [21]).

**Proposition 5.1.15** Assume $I, J$ are ideals of $O_K$. Then

$$N(I \cdot J) = N(I) \cdot N(J).$$

Lastly, a prime number $p$ is said to be **ramified** in an algebraic number field $K$ if the prime ideal factorization

$$\langle p \rangle = \mathfrak{p}_1^{e_1} \mathfrak{p}_2^{e_2} \cdots \mathfrak{p}_r^{e_r},$$

for prime ideals $\mathfrak{p}_1, \mathfrak{p}_2, ..., \mathfrak{p}_r$ in $O_K$, has some $e_i$ greater than 1. If every $e_i$ equals 1 then we say $p$ is unramified in $K$.

We have the following result which characterizes the prime numbers that ramify in an algebraic number field $K$ in terms of the field discriminant $d(K)$ (see Theorem 4.8.8, p. 197, [6]).

**Theorem 5.1.16** For an algebraic number field $K$, the primes which ramify are those dividing the field discriminant $d(K)$ of $K$. 
5.2 Important Lemmas

We first recall LaMacchia’s parametric family of septimic polynomials:

\[
f(a, A, X) = X^7 + 2(1 - 3a)X^6 + (-3 + 4a + 8a^2)X^5 + (-2 + 6a - 14a^2)X^4 \\
+ (2 - 4a + 6a^2 - 8a^3)X^3 + 8(2 + a)a^2X^2 + 4(-3 + 2a)a^2X \\
- 8a^3 + AX^3(1 - X).
\]

This polynomial is irreducible over \( \mathbb{Q} \) and its Galois group over \( \mathbb{Q}(a, A) \) is isomorphic to \( \text{PSL}(2, 7) \).

Let \( b \in \mathbb{Z} \). Substituting for the value of the parameters \( a = \frac{1}{2} \) and \( A = b - \frac{5}{2} \) we obtain the following one-parameter polynomial:

\[
g_b(x) = x^7 - x^6 + x^5 - bx^4 + (-2 + b)x^3 + 5x^2 - 2x - 1.
\]

We now make one scaling adjustment by replacing \( x \) by \(-x\) and then multiply through by \(-1\) to obtain

\[
f_b(x) = x^7 + x^6 + x^5 + bx^4 + (b - 2)x^3 - 5x^2 - 2x + 1.
\]

Such adjustments should not change the irreducibility and Galois group of the polynomial over \( \mathbb{Q} \) and so it is expected that \( f_b(x) \) will also be irreducible over \( \mathbb{Q} \) and have Galois group isomorphic to \( \text{PSL}(2, 7) \). However, this is not guaranteed and so we must confirm these properties.

**Lemma 5.2.1** If \( b \in \mathbb{Z} \) then \( f_b(x) \) is irreducible over \( \mathbb{Q} \).

**Proof.** Let’s consider two cases for the value of \( b \). Assume \( b \) is even and so \( b = 2n \) for some integer \( n \). Then

\[
f_{2n}(x) = x^7 + x^6 + x^5 + 2nx^4 + (2n - 2)x^3 - 5x^2 - 2x + 1.
\]
Modulo 2, this polynomial becomes
\[ f_{2n}(x) \pmod{2} \equiv x^7 + x^6 + x^5 + x^2 + 1 \]
which is an irreducible polynomial modulo 2. Hence, when \( b \) is even, \( f_b(x) \) is irreducible over \( \mathbb{Z} \) and hence over \( \mathbb{Q} \) (by Gauss’ Lemma). Now assume \( b \) is odd and so \( b = 2n + 1 \) for some integer \( n \). Then
\[ f_{2n+1}(x) = x^7 + x^6 + x^5 + (2n+1)x^4 + (2n-1)x^3 - 5x^2 - 2x + 1. \]
Modulo 2, this polynomial becomes
\[ f_{2n+1}(x) \pmod{2} \equiv x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + 1 \]
which is an irreducible polynomial modulo 2. Hence, when \( b \) is odd, \( f_b(x) \) is irreducible over \( \mathbb{Z} \) and hence over \( \mathbb{Q} \) (by Gauss’ Lemma). Thus, \( f_b(x) \) is irreducible over \( \mathbb{Q} \) for all \( b \in \mathbb{Z} \).

We first need to prove the following two Lemmas before we can show the Galois group of \( f_b(x) \) is isomorphic to \( \text{PSL}(2,7) \).

**Lemma 5.2.2** If \( b \in \mathbb{Z} \) then the discriminant of the polynomial \( f_b(x) \) is
\[ (b^2 - 5b - 25)^2(27b^2 - 135b + 769)^2. \]

**Proof.** This calculation was carried out using Maple.

In order to prove the next lemma, we first recall an extended version of Rolle’s Theorem.

**Theorem 5.2.3** Suppose that the function \( f \) is \( n-1 \) times continuously differentiable on the closed interval \([a, b]\) and the \( n^{\text{th}} \) derivative exists on the open interval \((a, b)\) and there are \( n \) intervals given by \( a_1 < b_1 \leq a_2 < b_2 \leq \ldots \leq a_n < b_n \) in \([a, b]\) such that
\( f(a_k) = f(b_k) \) for every \( k \) from 1 to \( n \). Then there is a number \( c \) in \( (a, b) \) such that the \( n^{th} \) derivative of \( f \) at \( c \) is zero.

**Lemma 5.2.4** If \( b \in \mathbb{Z} \) then not all the roots of the polynomial \( f_b(x) \) are real.

**Proof.** By Lemma 5.2.2, the discriminant of \( f_b(x) \) is \((b^2 - 5b - 25)(27b^2 - 135b + 769)^2\) which is nonzero (as \( b \in \mathbb{Z} \)). Therefore, the roots of \( f_b(x) \) are distinct.

Assume, by way of contradiction, that all the roots of \( f_b(x) \) are real. The 5\(^{th} \) derivative of \( f_b(x) \) is

\[
    f_b^{(5)}(x) = 2520x^2 + 720x + 120,
\]

which has no real roots (as its discriminant is negative). However, by Rolle’s Theorem (Theorem 5.2.3 with \( n = 5 \)), there is a number \( c \in \mathbb{R} \) such that \( f_b^{(5)}(c) = 0 \). This is a contradiction and thus, the roots of \( f_b(x) \) are not all real. ■

We are now able to prove the following Lemma.

**Lemma 5.2.5** If \( b \in \mathbb{Z} \) then the Galois group of the polynomial \( f_b(x) \) is isomorphic to \( PSL(2, 7) \).

**Proof.** By Lemma 5.2.2, the discriminant of \( f_b(x) \) is equal to a perfect square in \( \mathbb{Q} \). A list of possible Galois groups for a septimic polynomial is given by Cohen ([6]). Those which correspond to a square discriminant are

\[
\begin{cases}
    C_7 - \text{the Cyclic group of order 7} \\
    M_{21} \text{ or } F_{21} - \text{the Frobenius group of order 21} \\
    PSL(2, 7) - \text{the projective special linear group of } 2 \times 2 \text{ matrices over } \mathbb{F}_7 \text{ of order 168} \\
    A_7 - \text{the Alternating group of order 2520}.
\end{cases}
\]

By Lemma 5.2.4, \( f_b(x) \) has at least some complex roots. Thus, complex conjugation is a nontrivial element of the automorphism group of the splitting field of \( f_b(x) \) and so the order of the Galois group of \( f_b(x) \) must be divisible by two. This eliminates \( C_7 \).
and $F_{21}$ as possible Galois groups of $f_b(x)$. To eliminate $A_7$, we adapt the argument given on p. 55, [13]. The polynomial identity given is

$$y^3(1 - y) \cdot f(a, A, x) + x^3(1 - x) \cdot f(a, -A, y) = p(x, y) \cdot q(x, y)$$

for some polynomials $p(x, y)$ and $q(x, y)$ of degree 3 and 4 in $x$, respectively. In order to adapt this identity for our polynomial $f_b(x)$, we must make the same substitutions and scalings we did before to transform $f(a, A, x)$ into $f_b(x)$. Thus, we substitute $a = \frac{1}{2}, A = b - \frac{5}{2}, x = -x, y = -y$ into this polynomial identity and then multiply by $-1$ throughout to obtain the polynomial identity

$$y^3(1 + y) \cdot f_b(x) + x^3(1 + x) \cdot f_{-b+5}(y) = p(x, y) \cdot q(x, y)$$

(19)

for polynomials $p(x, y)$ and $q(x, y)$ of degree 3 and 4 in $x$, respectively, which are given by

$$p(x, y) = yx^3 + (1 - y^2)x^2 + (1 + y^3)x + y + y^2$$

and

$$q(x, y) = (y^3 + y^2)x^4 + (y^4 + 2y^3 - y)x^3 + (y^4 - 3y^2 - y + 1)x^2 + (-y^3 - y^2 - y)x + y^2.$$ 

Let $\beta$ be a root of $f_{-b+5}(x)$. The possible roots of $f_{-b+5}(x)$ are ±1. However, by Lemma 5.2.1, $f_{-b+5}(x)$ is irreducible over $\mathbb{Q}$. Thus, $\beta \neq \pm 1$. Also, $f_{-b+5}(0) = 1$ and so $\beta \neq 0$. If we set $y = \beta$ in equation [19], we have

$$\beta^3(1 + \beta) \cdot f_b(x) = p(x, \beta) \cdot q(x, \beta).$$

Thus

$$f_b(x) = \frac{p(x, \beta) \cdot q(x, \beta)}{\beta^3(1 + \beta)}$$

as $\beta \neq 0, -1$. This gives a factorization of $f_b(x)$ into factors of degree 3 and 4,
respectively, over \( \mathbb{Q}(\beta) \). We know that the Galois group of these cubic and quartic factors will have at most degree equal to that of \( S_3 \) and \( S_4 \), respectively. Moreover, since \( \beta \) is a root of the monic and irreducible polynomial \( f_{-b+5}(x) \), it follows that \( \mathbb{Q}(\beta) \) is a degree 7 extension of \( \mathbb{Q} \). So it follows that the degree of the splitting field of \( f_b(x) \) over \( \mathbb{Q} \) is a divisor of \( 7 \cdot 3! \cdot 4! = 1008 \). However, this degree is not divisible by 5 and so the possibility of \( A_7 \) as the Galois group of \( f_b(x) \) is now eliminated and so the Galois group must be isomorphic to \( \text{PSL}(2,7) \). ■

We have now established that the polynomial \( f_b(x) \) is irreducible over \( \mathbb{Q} \) and the Galois group is isomorphic to \( \text{PSL}(2,7) \). Our next step is to establish the field discriminant \( d(K) \) of \( K = \mathbb{Q}(\theta) \), where \( \theta \) is a root of \( f_b(x) \). We begin with a series of lemmas that will aid us in finding \( d(K) \).

**Lemma 5.2.6** Let \( f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0 \in \mathbb{Z}[x] \) be irreducible over \( \mathbb{Q} \). Suppose that \( \alpha \) is a root of \( f(x) \) and \( K = \mathbb{Q}(\alpha) \). If \( p \) is a prime number and \( k \) is a positive integer with \( k < n \) such that \( p^k \mid a_0 \) and \( p^{k+1-i} \mid a_i \) for \( 1 \leq i \leq k \) then \( p \) ramifies in \( K \).

**Proof.** By way of contradiction, assume \( p \), a prime number satisfying the hypothesis of the lemma, does not ramify in \( K \). Then there exist distinct prime ideals \( \varphi_1, \varphi_2, \ldots, \varphi_r \) in \( O_K \) such that

\[
\langle p \rangle = \varphi_1 \varphi_2 \cdots \varphi_r.
\]

Since \( p^k \mid a_0 \) for a positive integer \( k < n \), we have as ideals in \( O_K \),

\[
\langle a_0 \rangle = \varphi_1^k \varphi_2^k \cdots \varphi_r^k \cdot \langle c \rangle,
\]

for some \( c \in \mathbb{Z} \) with \( p \nmid c \). Thus, \( \varphi_i \nmid \langle c \rangle \) for \( i = 1, 2, \ldots, r \). Since \( p^k \mid a_0 \) implies \( p \mid a_0 \), we have

\[
N(\alpha) = \pm a_0 \equiv 0(\text{mod } p).
\]
By Proposition 5.1.14, we have

$$N(\langle \alpha \rangle) = |N(\alpha)| = |a_0| \equiv 0 (\text{mod } p).$$

Now we can write

$$\langle \alpha \rangle = \mathfrak{R}_1 \mathfrak{R}_2 \cdots \mathfrak{R}_t$$

for prime ideals $\mathfrak{R}_1, \mathfrak{R}_2, \ldots, \mathfrak{R}_t$. By Proposition 5.1.15, we have

$$N(\langle \alpha \rangle) = N(\mathfrak{R}_1)N(\mathfrak{R}_2) \cdots N(\mathfrak{R}_t).$$

Since $p \mid N(\langle \alpha \rangle)$, we must have one of $N(\mathfrak{R}_1), N(\mathfrak{R}_2), \ldots, N(\mathfrak{R}_t)$ divisible by $p$ as well, say $N(\mathfrak{R}_1)$. Thus

$$N(\mathfrak{R}_1) = p^u$$

for some $u \in \mathbb{Z}^+$. Recall

$$\langle p \rangle = \mathfrak{p}_1 \mathfrak{p}_2 \cdots \mathfrak{p}_r$$

and these are precisely the prime ideals that have norms equal to a power of $p$. Thus $\mathfrak{R}_1$ has to be one of $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_r$. Therefore, the ideal $\langle \alpha \rangle$ must be divisible by at least one $\mathfrak{p}_i$, say $\mathfrak{p}$.

As $p^{k+1-i} \mid a_i$ for $1 \leq i \leq k$, we have

$$\langle p^{k+1-i} \rangle \mid \langle a_i \rangle.$$  

Moreover, since $\mathfrak{p} \mid \langle p \rangle$, by transitivity, we have

$$\mathfrak{p}^{k+1-i} \mid \langle a_i \rangle.$$
Now

\[
\langle a_0 \rangle = \langle a_0 - f(\alpha) \rangle = \langle -(a_1\alpha + \ldots + a_k\alpha^k) - (a_{k+1}\alpha^{k+1} + \ldots + \alpha^n) \rangle.
\]

Consider each term inside the first pair of brackets \((a_1\alpha + \ldots + a_k\alpha^k)\). First, we consider \(\langle a_1\alpha \rangle\). By assumption, we know \(\varphi^k | \langle a_1 \rangle\) and \(\varphi | \langle \alpha \rangle\) and so

\[\varphi^{k+1} | \langle a_1\alpha \rangle\].

Similarly, we have \(\varphi | \langle a_k \rangle\) and \(\varphi^k | \langle \alpha^k \rangle\) and so

\[\varphi^{k+1} | \langle a_k\alpha^k \rangle\].

Thus, \(\varphi^{k+1}\) divides each term in the first pair of brackets.

Now consider each term inside the second pair of brackets \((a_{k+1}\alpha^{k+1} + \ldots + \alpha^n)\). Since \(\varphi^{k+1} | \langle \alpha^{k+1} \rangle\) and each term contains \(\alpha^{k+1}\), we conclude \(\varphi^{k+1}\) divides each term in the second pair of brackets. Thus

\[\langle a_0 \rangle \equiv 0 \pmod{\varphi^{k+1}}\]

or equivalently,

\[\varphi^{k+1} | \langle a_0 \rangle\].

This implies \(p^{k+1} | a_0\) (as \(a_0 \in \mathbb{Z}\)) which contradicts \(p^k \parallel a_0\). Thus, \(p\) ramifies in \(K\).

\[\blacksquare\]

Let \(\theta\) be a root of \(f_b(x)\) and define the field \(K = \mathbb{Q}(\theta)\). Set

\[g(b) = g_1(b)g_2(b)\]
where
\[ g_1(b) = b^2 - 5b - 25 \]
and
\[ g_2(b) = 27b^2 - 135b + 769. \]

We will be working under the assumption that \( g(b) \) is squarefree and wish to calculate the field discriminant \( d(K) \). The following two lemmas determine the ramified primes in \( K = \mathbb{Q}(\theta) \). To do this, we give two elements in \( K \) and their monic minimal polynomials in \( \mathbb{Q}[x] \) to which we can apply the previous lemma. To experimentally find candidates for these elements, we formally solve the polynomial equation \( f_b(\theta) = 0 \) for \( b \). From this, we obtain
\[
b = -\frac{\theta^7 + \theta^6 + \theta^5 - 2\theta^3 - 5\theta^2 - 2\theta + 1}{\theta^3(1 + \theta)}.
\]

We first calculate \( g_1(b) = b^2 - 5b - 25 \) using our value of \( b \) in equation (20). We obtain
\[
g_1(b) = \frac{1}{\theta^6(1 + \theta)^2} \cdot (\theta^2 - \theta - 1)(\theta^4 - \theta^3 + 3\theta^2 + 3\theta - 1)(-\theta^4 - 2\theta^3 - 2\theta^2 - \theta + 1)^2.
\]

We choose \( \theta_1 \) to be a factor of this expression and so
\[ \theta_1 = -\theta^4 - 2\theta^3 - 2\theta^2 - \theta + 1. \]

Similarly, we now calculate \( g_2(b) = 27b^2 - 135b + 769 \) using our value of \( b \) in equation (20). We obtain
\[
g_2(b) = \frac{1}{\theta^6(1 + \theta)^2} \cdot (\theta^2 + 3\theta + 3)(3\theta^4 - 3\theta^3 + 13\theta^2 - 7\theta + 1)(-3\theta^4 + 2\theta^3 - 3\theta - 3)^2.
\]

\[ 40 \]
We choose $\theta_2$ to be a factor of this expression and so

$$\theta_2 = -3\theta^4 + 2\theta^2 - 3\theta - 3.$$ 

We obtain two elements of $K$, namely $\theta_1$ and $\theta_2$. We now wish to calculate their minimal polynomials in $\mathbb{Q}[x]$. Since both $\theta_1$ and $\theta_2$ are in $K$, a septimic field, the degree of their minimal polynomials must be equal to or less than the degree of $K$, and in fact, must divide the degree of $K$. Thus, as $\theta_1$ and $\theta_2$ do not belong to $\mathbb{Q}$, the degree of their minimal polynomials must be seven. Starting with $\theta_1$, its minimal polynomial has the form

$$h_b(x) = x^7 + Ax^6 + Bx^5 + Cx^4 + Dx^3 + Ex^2 + Fx + G$$

where $A, B, C, D, E, F, G \in \mathbb{Q}$. We know $\theta_1 = -\theta^4 - 2\theta^3 - 2\theta^2 - \theta + 1$ is a root of its minimal polynomial and so

$$h_b(\theta_1) = \theta_1^7 + A\theta_1^6 + B\theta_1^5 + C\theta_1^4 + D\theta_1^3 + E\theta_1^2 + F\theta_1 + G = 0$$

which, after the substitution $\theta_1 = -\theta^4 - 2\theta^3 - 2\theta^2 - \theta + 1$, simplifies to a polynomial of which $\theta$ is a root. Since $f_b(x)$ is the minimal polynomial of $\theta$, it must divide any polynomial of which $\theta$ is a root. Using MAPLE$^\text{TM}$, we compute the remainder of
this division and set each of its coefficients equal to zero. This gives

\[
\begin{align*}
A &= -6b + 1 \\
B &= 10b^2 + 29b - 40 \\
C &= b^4 - 5b^3 - 54b^2 + 60b + 475 \\
D &= -(4b^2 - 9b - 78)(b^2 - 5b - 25) = -(4b^2 - 9b - 78)g_1(b) \\
E &= 3(b^2 - 5b - 25)(2b^2 - 8b - 45) = 3(2b^2 - 8b - 45)g_1(b) \\
F &= -4(b^2 - 5b - 25)^2 = -4g_1(b)^2 \\
G &= (b^2 - 5b - 25)^2 = g_1(b)^2.
\end{align*}
\]

Thus, the minimal polynomial of \( \theta_1 \) is

\[
h_b(x) = x^7 + (1 - 6b)x^6 + (10b^2 + 29b - 40)x^5 + (b^4 - 5b^3 - 54b^2 + 60b + 475)x^4 \
- (4b^2 - 9b - 78)g_1(b)x^3 + 3(2b^2 - 8b - 45)g_1(b)x^2 - 4g_1(b)^2x + g_1(b)^2.
\]

We perform a similar calculation for \( \theta_2 = -3\theta^4 + 2\theta^2 - 3\theta - 3 \) to obtain

\[
\begin{align*}
A &= 41 \\
B &= 54b^2 - 27b + 318 \\
C &= 27b^4 - 189b^3 + 1066b^2 - 782b - 4325 \\
D &= (10b^2 - 21b - 50)(27b^2 - 135b + 769) = (10b^2 - 21b - 50)g_2(b) \\
E &= (36b^2 - 114b + 263)(27b^2 - 135b + 769) = (36b^2 - 114b + 263)g_2(b) \\
F &= 2(27b^2 - 135b + 769)^2 = 2g_2(b)^2 \\
G &= (27b^2 - 135b + 769)^2 = g_2(b)^2
\end{align*}
\]
and so its minimal polynomial \( m_b(x) \) is

\[
m_b(x) = x^7 + 41x^6 + (54b^2 - 27b + 318)x^5 + (27b^4 - 189b^3 + 1066b^2 - 782b - 4325)x^4
\]
\[
+ (10b^2 - 21b - 50)g_2(b)x^3 + (36b^2 - 114b + 263)g_2(b)x^2 + 2g_2(b)^2x + g_2(b)^2.
\]

Using the above, we are now able to prove the following two lemmas.

**Lemma 5.2.7** Let \( b \in \mathbb{Z} \) be such that \( g_1(b) \) is squarefree. Let \( p \) be a prime such that \( p \mid g_1(b) \). Then \( p \mid d(K) \).

**Proof.** We know \( \theta_1 \in K \) and so \( \mathbb{Q}(\theta_1) \subseteq \mathbb{Q}(\theta) \). On the other hand, we also know that the monic minimal polynomial of \( \theta_1 \) is of degree seven and so \( \mathbb{Q}(\theta_1) \) is a degree seven extension of \( \mathbb{Q} \). Hence, \( K = \mathbb{Q}(\theta) = \mathbb{Q}(\theta_1) \) and so \( \theta_1 \) is a primitive element of \( K \).

Recall, the monic minimal polynomial \( h_b(x) \) of \( \theta_1 \) in \( \mathbb{Q}[x] \) is given by

\[
h_b(x) = x^7 + (1 - 6b)x^6 + (10b^2 + 29b - 40)x^5 + (b^4 - 5b^3 - 54b^2 + 60b + 475)x^4
\]
\[
- (4b^2 - 9b - 78)g_1(b)x^3 + 3(2b^2 - 8b - 45)g_1(b)x^2 - 4g_1(b)^2x + g_1(b)^2.
\]

By assumption, \( p \mid g_1(b) \) and so \( p^2 \mid g_1(b)^2 \). As \( g_1(b) \) is squarefree, it follows that \( p^2 \parallel g_1(b)^2 \). Considering the polynomial \( h_b(x) \) above, we are now able to conclude

\[
\begin{align*}
p^2 & \parallel a_0 = g_1(b)^2 \\
p^2 & \mid a_1 = -4g_1(b)^2 \\
p & \mid a_2 = 3(2b^2 - 8b - 45)g_1(b).
\end{align*}
\]

So we may apply Lemma 5.2.6 to the irreducible polynomial \( h_b(x) \) with \( k = 2 \) of which \( \theta_1 \) is a root which defines \( K = \mathbb{Q}(\theta) \). We conclude \( p \) ramifies in \( K \). So by Theorem 5.1.16, we have \( p \mid d(K) \). \( \blacksquare \)

**Lemma 5.2.8** Let \( b \in \mathbb{Z} \) be such that \( g_2(b) \) is squarefree. Let \( p \) be a prime such that \( p \mid g_2(b) \). Then \( p \mid d(K) \).
Proof. We know $\theta_2 \in K$ and so $\mathbb{Q}(\theta_2) \subseteq \mathbb{Q}(\theta)$. On the other hand, we also know that the monic minimal polynomial of $\theta_2$ is of degree seven and so $\mathbb{Q}(\theta_2)$ is a degree seven extension of $\mathbb{Q}$. Hence, $K = \mathbb{Q}(\theta) = \mathbb{Q}(\theta_2)$ and so $\theta_2$ is a primitive element of $K$.

Recall, the monic minimal polynomial $m_b(x)$ of $\theta_2$ in $\mathbb{Q}[x]$ is given by

$$m_b(x) = x^7 + 41x^6 + (54b^2 - 27b + 318)x^5 + (27b^4 - 189b^3 + 1066b^2 - 782b - 4325)x^4$$

$$+ (10b^2 - 21b - 50)g_2(b)x^3 + (36b^2 - 114b + 263)g_2(b)x^2 + 2g_2(b)^2x + g_2(b)^2.$$  

By assumption, $p \mid g_2(b)$ and so $p^2 \mid g_2(b)^2$. As $g_2(b)$ is squarefree, it follows that $p^2 \parallel g_2(b)^2$. Considering the polynomial $m_b(x)$ above, we are now able to conclude

$$\begin{cases} 
p^2 \parallel a_0 = g_2(b)^2 \\
p^2 \mid a_1 = 2g_2(b)^2 \\
p \mid a_2 = (36b^2 - 114b + 263)g_2(b).\end{cases}$$

So we may apply Lemma 5.2.6 to the irreducible polynomial $m_b(x)$ with $k = 2$ of which $\theta_2$ is a root which defines $K = \mathbb{Q}(\theta)$. We conclude $p$ ramifies in $K$. So by Theorem 5.1.16, we have $p \mid d(K)$. ■

Lemma 5.2.9 If $g(b)$ is squarefree then $d(K) = g(b)^2$.

Proof. We know the field discriminant $d(K)$ divides the polynomial discriminant of $f_b(x)$, namely $g(b)^2$. Moreover, from equation (18), we conclude

$$g(b)^2 = c^2d(K)$$

for some nonzero integer $c$. On the other hand, Lemma 5.2.7 and Lemma 5.2.8 imply each prime number $p$ dividing $g(b)$ also divides $d(K)$. Since $g(b)$ is squarefree, we deduce $p \nmid c^2$ and so $c^2 = 1$. Thus $d(K) = g(b)^2$. ■
Our previous lemmas have assumed $g(b)$ is squarefree. Moreover, for our main theorem to hold, we will require the polynomial $g(b)$ assume squarefree values for infinitely many positive integers $b$. Since the polynomial $g(b)$ is reducible over $\mathbb{Z}$, we can use a proposition by M. Nair (see pp. 181-182, [26]) to help us prove this. In order to state this proposition, we first define

$$ N_k(f, x, h) = N_k(x, h) = |\{n : x < n \leq x + h, f(n) \text{ is } k\text{-free}\}|. $$

**Proposition 5.2.10** If

$$ f(x) = \prod_{i=1}^{m} (f_i(x))^{\alpha_i} $$

where each $f_i$ is irreducible, $\alpha = \max \alpha_i$ and $\deg(f_i(x)) = g_i$ then

$$ N_k(x, h) = \Lambda_k h + O \left( \frac{h}{(\log h)^{\lambda-1}} \right) \tag{21} $$

for $h = x^\theta$ where $0 < \theta < 1$ and $k \geq \max \{\lambda g_i, \alpha_i\}$, $(\lambda = \sqrt{2} - 1/2)$ provided that at least one $g_i \geq 2$ (the constant $\Lambda_k$ is positive).

**Lemma 5.2.11** There exist infinitely many positive integers $b$ such that $g(b)$ is squarefree.

**Proof.** The quartic polynomial

$$ g(b) = (b^2 - 5b - 25)(27b^2 - 135b + 769) $$

is equal to the product of two irreducible quadratic polynomials over $\mathbb{Q}$. Also, we see that

$$ g_1(1) = -29 = \text{prime} $$
$$ g_2(1) = 661 = \text{prime} $$
and so the polynomial \( g(b) \) has no fixed square divisors. To apply the previous proposition, we note that

\[
f_1(b) = b^2 - 5b - 25 \\
f_2(b) = 27b^2 - 135b + 769
\]

and so

\[
\alpha_1 = 1 \\
g_1 = \deg(f_1(b)) = 2
\]

and

\[
\alpha_2 = 1 \\
g_2 = \deg(f_2(b)) = 2.
\]

Thus, \( k \geq \max \{ \lambda g, \alpha_i \} \), where \( \lambda = \sqrt{2} - 1/2 \), simplifies to \( k \geq 2 \) so that we can set \( k = 2 \). So by equation (21), we conclude

\[
N_2(g, x, h) = \Lambda_2 h + O \left( \frac{h}{\log h} \right) = \Lambda_2 x^\theta + O \left( \frac{x^\theta}{\log x^\theta} \right)
\]

where \( 0 < \theta < 1 \). This then implies

\[
N_2(g, x, h) \to \infty \text{ as } x \to \infty
\]

and so

\[
\{b : x < b \leq x + h, g(b) \text{ is squarefree}\} \to \infty \text{ as } x \to \infty.
\]

It follows that there exist infinitely many positive integers \( b \) such that \( g(b) \) is square-free. \( \blacksquare \)
5.3 Main Theorem

We are now able to prove the following theorem.

**Theorem 5.3.1** There are infinitely many integers $b$ such that the polynomials

$$f_b(x) = x^7 + x^6 + x^5 + bx^4 + (b - 2)x^3 - 5x^2 - 2x + 1$$

define distinct monogenic PSL(2,7) septimic fields.

**Proof.** By Lemma 5.2.2, the polynomial $f_b(x)$ has discriminant equal to

$$g(b)^2 = (b^2 - 5b - 25)^2(27b^2 - 135b + 769)^2.$$  

Moreover, by Lemmas 5.2.1 and 5.2.5, if $\theta$ is a root of $f_b(x)$ then the field $K = \mathbb{Q}(\theta)$ is a PSL(2,7) septimic extension of $\mathbb{Q}$. By Lemma 5.2.11, there exist infinitely many positive integers $b$ such that $g(b)$ is squarefree. For these values of $b$, by Lemma 5.2.9, the field discriminant $d(K)$ of $K = \mathbb{Q}(\theta)$ is equal to $g(b)^2$. Hence,

$$\text{ind}(\theta) = \pm 1$$

and so by Theorem 5.1.8, it follows that

$$\{1, \theta, \theta^2, \theta^3, \theta^4, \theta^5, \theta^6\}$$

is a power basis for $K = \mathbb{Q}(\theta)$, proving that $K$ is monogenic. So we have shown that there are infinitely many positive integers $b$ such that the PSL(2,7) septimic fields $K = \mathbb{Q}(\theta)$ are monogenic. It remains to show that these fields are distinct.

Two fields are equal if they have the same field discriminant. Since

$$d(K) = (b^2 - 5b - 25)^2(27b^2 - 135b + 769)^2,$$
we wish to know how many possible values of $b$ satisfy the given equation for fixed $t \in \mathbb{Z}$

$$(b^2 - 5b - 25)^2(27b^2 - 135b + 769)^2 = (t^2 - 5t - 25)^2(27t^2 - 135t + 769)^2, \quad (22)$$

or equivalently,

$$(b^2 - 5b - 25)(27b^2 - 135b + 769) = \pm (t^2 - 5t - 25)(27t^2 - 135t + 769).$$

Since $t$ is fixed and $(b^2 - 5b - 25)(27b^2 - 135b + 769)$ is a quartic polynomial in terms of $b$, there can be at most four solutions to the equation

$$(b^2 - 5b - 25)(27b^2 - 135b + 769) - (t^2 - 5t - 25)(27t^2 - 135t + 769) = 0$$

and four solutions to the equation

$$(b^2 - 5b - 25)(27b^2 - 135b + 769) + (t^2 - 5t - 25)(27t^2 - 135t + 769) = 0.$$

Thus, there are at most eight solutions for a given integer $t$ to equation (22). Since we have an infinite sequence of the integers $b$ such that $(b^2 - 5b - 25)^2(27b^2 - 135b + 769)^2$ is squarefree, we can choose an infinite subsequence of this sequence such that the fields $K = \mathbb{Q}(\theta)$ will have different discriminants (as we can have at most eight duplications). Thus we will have an infinite number of distinct fields which completes the proof. ■

5.4 Future Research

One topic for future research is to see if the fields $K = \mathbb{Q}(\theta)$ possess any other power bases other than \{1, $\theta$, $\theta^2$, $\theta^3$, $\theta^4$, $\theta^5$, $\theta^6$\}. For instance, if we take the simpler case
\( b = 2 \), we have
\[
g(b) = -18817 = -31 \cdot 607
\]
is squarefree and so by Theorem 5.3.1, the polynomial
\[
f_2(x) = x^7 + x^6 + x^5 + 2x^4 - 5x^2 - 2x + 1
\]
defines a monogenic \( \text{PSL}(2,7) \) septimic field \( K = \mathbb{Q}(\theta) \) where \( \theta \) is a root of \( f_2(x) \).
Moreover, a power basis of \( K = \mathbb{Q}(\theta) \) is \( \{1, \theta, \theta^2, \theta^3, \theta^4, \theta^5, \theta^6\} \). To see if \( K \) possesses any other power bases, we begin with a typical element in \( \mathcal{O}_K \), say \( \alpha \), and find its minimal polynomial \( A(x) \). Since \( \{1, \theta, \theta^2, \theta^3, \theta^4, \theta^5, \theta^6\} \) is a power basis, we have
\[
\alpha = S + T\theta + U\theta^2 + V\theta^3 + W\theta^4 + X\theta^5 + Y\theta^6
\]
where \( S, T, U, V, W, X, Y \in \mathbb{Z} \). Because power bases are defined to be equivalent if they differ by an integer \( (p. 80, [27]) \), we can actually drop the \( S \) term and write
\[
\alpha = T\theta + U\theta^2 + V\theta^3 + W\theta^4 + X\theta^5 + Y\theta^6.
\]
Using a similar procedure to that of finding the minimal polynomials of \( \theta_1 \) and \( \theta_2 \), we find the minimal polynomial \( A(x) \) of \( \alpha \). We then find and factor the discriminant of \( A(x) \), denoted as \( D(A(x)) \).
We know
\[
D(A(x)) = d(K) \cdot (\text{ind}(\alpha))^2.
\]
From before,
\[
d(K) = (b^2 - 5b - 25)^2(27b^2 - 135b + 769)^2
\]
and so for \( b = 2 \) we have
\[
d(K) = (31)^2(607)^2.
\]
Thus

\[ ind(\alpha) = \pm \sqrt{\frac{D(A(x))}{(31)^2(607)^2}} = \pm \frac{\sqrt{D(A(x))}}{31 \cdot 607}. \]

In order to find additional power bases, we wish to solve

\[ ind(\alpha) = \pm \frac{\sqrt{D(A(x))}}{31 \cdot 607} = \pm 1 \]

which is an equation in the six variables \( T, U, V, W, X \) and \( Y \). Unfortunately, even these calculations seem to be too much for computer programs such as MAPLE\textsuperscript{TM}. Perhaps, more efficient and powerful programs may be used to solve such a problem. In this paper, we have shown an infinite family of monogenic \( \text{PSL}(2, 7) \) septimic fields. For future research, one might continue exhibiting infinite families of monogenic fields of given Galois group and degree. Although there has been some research done in the area of monogenic fields, some problems remain open. For example, it is not known if there are infinitely many monogenic cyclic quartic fields. Moreover, since higher degrees make these problems more challenging, such fields remain to be studied.
Chapter 6

Lifting Monogenic Cubic Fields to Sextic Fields

For sextic fields $K$ containing a cubic subfield, there are eight possible Galois groups for $K$ over $\mathbb{Q}$. In this chapter, we construct infinitely many monogenic sextic fields for five of these eight Galois groups. We do so by elevating or lifting monogenic cubic fields into monogenic sextic fields. That is, suppose we have a monogenic cubic field $C$ defined by the cubic polynomial

$$g(x) = x^3 + ax^2 + bx + 1 \in \mathbb{Z}[x].$$

We then investigate conditions on $a$ and $b$ such that the sextic polynomial

$$f(x) = x^6 + ax^4 + bx^2 + 1 \in \mathbb{Z}[x]$$

defines a monogenic sextic field $K$. We discover that for five of the eight possible Galois groups of $f$, there are infinitely many monogenic sextic fields which can be obtained in this way (i.e. via lifting). Moreover, for the remaining three possible Galois groups, we show that there are at most finitely many such monogenic sextic fields. This process shows one application in constructing parametric families of polynomials.

6.1 Preliminaries

We first will go over some theory regarding minimal integers which will be used to find an integral basis of $K$. Further information regarding proofs of theorems and
derivations can be found on pp. 160-170, [1].

First, let $K$ be an algebraic number field of degree $n$ and let $\theta \in O_K$ such that $K = \mathbb{Q}(\theta)$. Thus, every $\alpha \in O_K$ can be expressed of the form

$$\alpha = a_0 + a_1 \theta + a_2 \theta^2 + \ldots + a_{n-1} \theta^{n-1}$$

where $a_0, a_1, \ldots, a_{n-1} \in \mathbb{Q}$ and are uniquely determined by $\alpha$ and $\theta$.

If $k \in \{0, 1, 2, \ldots, n-1\}$ such that

$$a_k \neq 0 \text{ and } a_{k+1} = a_{k+2} = \ldots = a_{n-1} = 0$$

(which implies $\alpha = a_0 + a_1 \theta + a_2 \theta^2 + \ldots + a_k \theta^k$) then $\alpha$ is called an integer of degree $k$ in $\theta$. A specific case is when $a_1 = a_2 = \ldots = a_{n-1} = 0$ (i.e. $k = 0$). This implies that $\alpha = a_0$ and we say that $\alpha$ is an integer of degree 0 in $\theta$. Now for $k \in \{0, 1, 2, \ldots, n-1\}$, define the set $S_k$ by

$$S_k = \{a_k \in \mathbb{Q} \mid a_0 + a_1 \theta + \ldots + a_k \theta^k \in O_K \text{ for some } a_0, a_1, \ldots, a_{k-1} \in \mathbb{Q}\}.$$

So we have

$$S_0 = \{a_0 \in \mathbb{Q} \mid a_0 \in O_K\} = \mathbb{Z}$$

and

$$\mathbb{Z} \subseteq S_k$$

for $k = 0, 1, 2, \ldots, n-1$. Also, it can be shown that $S_k$ has a least positive element, say $a_k^*$. Since $S_0 = \mathbb{Z}$, we know $a_0^* = 1$.

**Definition 6.1.1** With the preceding notation, any integer of $K$ that is of the form

$$a_0 + a_1 \theta + a_2 \theta^2 + \ldots + a_{k-1} \theta^{k-1} + a_k^* \theta^k,$$
where \( a_0, a_1, \ldots, a_{k-1} \in \mathbb{Q} \), is called a minimal integer of degree \( k \) in \( \theta \).

Now the following theorem gives the form of the element \( a_k^* \).

**Theorem 6.1.2** For \( k \in \{0, 1, 2, \ldots, n-1\} \)

\[
a_k^* = \frac{1}{d_k}
\]

for some \( d_k \in \mathbb{N} \).

There exists a property for the numbers \( d_k \) as seen in the following theorem.

**Theorem 6.1.3** For \( k = 1, 2, \ldots, n-1 \)

\[
d_{k-1} \mid d_k.
\]

We are now able to give the form of an integer of degree \( k \) in \( \theta \) for \( k = 0, 1, 2, \ldots, n-1 \) and as a result, the form of a minimal integer of degree \( k \) in \( \theta \).

**Theorem 6.1.4** If \( \alpha \) is an integer of degree \( k \) in \( \theta \) then there exists \( b_0, b_1, \ldots, b_k \in \mathbb{Z} \) such that

\[
\alpha = \frac{b_0 + b_1 \theta + b_2 \theta^2 + \ldots + b_{k-1} \theta^{k-1} + b_k \theta^k}{d_k}.
\]

In particular, if \( \alpha \) is a minimal integer of degree \( k \) in \( \theta \) then there exists \( a_0, a_1, \ldots, a_{k-1} \in \mathbb{Z} \) such that

\[
\alpha = \frac{a_0 + a_1 \theta + a_2 \theta^2 + \ldots + a_{k-1} \theta^{k-1} + \theta^k}{d_k}.
\]

We have now reached the climax of this theory to obtain a method of finding an integral basis for an algebraic number field \( K \) of degree \( n \).

**Theorem 6.1.5** Let \( K \) be an algebraic number field of degree \( n \). Let \( \theta \in O_K \) such that \( K = \mathbb{Q}(\theta) \). For \( k = 0, 1, 2, \ldots, n-1 \), let \( \alpha_k \) be a minimal integer in \( \theta \) of degree \( k \). Then

\[
\{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\}
\]
is an integral basis for $K$.

**Remark 6.1.6** In order to find an integral basis for an algebraic number field of degree $n$, we need only find a minimal integer of each degree up to $n - 1$.

This leads us to one last theorem which will also be helpful in finding these integral bases.

**Theorem 6.1.7** Let $K$ be an algebraic number field of degree $n$. Let $\theta \in O_K$ such that $K = \mathbb{Q}(\theta)$. For $k = 0, 1, 2, \ldots, n - 1$, let $\alpha_k$ be a minimal integer in $\theta$ of degree $k$ of the form

$$\alpha_k = \frac{a_{k0} + a_{k1}\theta + a_{k2}\theta^2 + \ldots + a_{k_{k-1}}\theta^{k-1} + \theta^{k}}{d_k}$$

where $a_{k0}, a_{k1}, \ldots, a_{k_{k-1}} \in \mathbb{Z}$ and $\alpha_0 = d_0 = 1$. Then

$$d_0d_1\cdots d_{n-1} = \text{ind}(\theta),$$

$$d_i \mid d_{i+1}$$

and

$$d_i^{2(n-i)} \mid D(\theta)$$

for $i = 0, 1, \ldots, n - 1$ and where $D(\theta)$ is the discriminant of the algebraic integer $\theta$ (equal to the polynomial discriminant of the minimal polynomial of $\theta$).

**Remark 6.1.8** There may be many values of $d_i$ that yield an algebraic integer. However, since we are finding a minimal integer $\alpha_k$, we choose the biggest $d_i$. That is, the minimal integer $\alpha_k$ is one whose denominator is largest yet still satisfies the above theorem. Moreover, when choosing to examine the possible choices for each $d_i$, we ignore the trivial case $d_i = 1$ and examine the others first, in particular, the prime possibilities of $d_i$. Lastly, we need only consider the values of $a_{k0}, a_{k1}, \ldots, a_{k_{k-1}}$ mod $d_k$. Since $O_K$ is a ring, we can subtract off integers or integer multiples of $\theta$ and still
remain in \(O_K\). Choosing these appropriately has the effect of reducing the coefficients modulo the denominator.

We will also make use of the following property of fields given in [6] (see Proposition 4.4.8, p.168).

**Proposition 6.1.9** Let \(K\) and \(L\) be number fields with \(K \subset L\). Then

\[
d(K)^{[L:K]} | d(L).
\]

We end off the preliminaries with an important theorem by T. Nagel ([25]) used to determine the squarefree values of polynomials.

**Theorem 6.1.10** Assume \(f(x) \in \mathbb{Z}[x]\) is an irreducible quadratic and define

\[
N_f = \gcd(f(m), m \in \mathbb{Z}).
\]

If \(N_f\) is squarefree then \(f(m)\) is squarefree for infinitely many integers \(m\).

Note that P. Erdös proves a similar theorem for irreducible cubics in [12].

### 6.2 Important Lemmas

**Lemma 6.2.1** Let \(g(x) = x^3 + ax^2 + bx + 1 \in \mathbb{Z}[x]\). Let \(\alpha\) be a root of \(g(x)\). Suppose that \(g(x)\) defines a monogenic cubic field \(C\) and that \(\{1, \alpha, \alpha^2\}\) is a power basis of \(C\). Let \(f(x) = x^6 + ax^4 + bx^2 + 1\) and suppose that \(\theta\) is a root of \(f(x)\). Let \(K = \mathbb{Q}(\theta)\) and suppose that \([K : \mathbb{Q}] = 6\). Then \(K\) is monogenic with power basis \(\{1, \theta, \theta^2, \theta^3, \theta^4, \theta^5\}\) if and only if

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

**Proof.** The discriminant of \(g(x) = x^3 + ax^2 + bx + 1\) is equal to

\[
D(g(x)) = -27 + 18ab + a^2b^2 - 4a^3 - 4b^3.
\]
Furthermore, the discriminant of \( f(x) = x^6 + ax^4 + bx^2 + 1 \) is equal to

\[
D(f(x)) = -2^6(-27 + 18ab + a^2b^2 - 4a^3 - 4b^3)^2.
\]

We now wish to calculate the field discriminant \( d(K) \) of the field \( K \). Since

\[
D(f(x)) = -2^6 \cdot D(g(x))^2,
\]

the roots of \( g(x) \) are just the squares of the roots of \( f(x) \). Hence, \( \mathbb{Q} \subset C \subset K \). We also have \([K : \mathbb{Q}] = 6\) and \([C : \mathbb{Q}] = 3\) and so

\[
[K : C] = 2.
\]

By Proposition 6.1.9, we conclude

\[
d(C)^2 \mid d(K).
\]

Since \( C \) is monogenic with power basis \( \{1, \alpha, \alpha^2\} \),

\[
D(g(x)) = d(C) \cdot (\text{ind}(\alpha))^2
\]

implies

\[
D(g(x)) = d(C) \Leftrightarrow D(g(x))^2 = d(C)^2.
\]

Similarly, we also have

\[
D(f(x)) = d(K) \cdot (\text{ind}(\theta))^2,
\]
or equivalently,

\[
d(K) = \frac{D(f(x))}{\text{ind}(\theta)^2} = -2^6 \cdot D(g(x))^2 \frac{D(g(x))}{\text{ind}(\theta)^2} = -2^6 \cdot d(C)^2 \frac{d(C)}{\text{ind}(\theta)^2}.
\]

By equation (23), this implies

\[
\frac{-2^6}{\text{ind}(\theta)^2} \in \mathbb{Z},
\]

or equivalently,

\[
(\text{ind}(\theta))^2 = 2^s
\]

for \(s \in \{0, 2, 4, 6\}\). Thus,

\[
d(K) = \frac{-2^6(-27 + 18ab + a^2b^2 - 4a^3 - 4b^3)}{2^s}
\]

where \(s \in \{0, 2, 4, 6\}\). Equivalently,

\[
d(K) = -2^t(-27 + 18ab + a^2b^2 - 4a^3 - 4b^3)^2
\]

where \(t \in \{0, 2, 4, 6\}\). So \((\text{ind}(\theta))^2 = 1\) if \(s = 0\), or \(t = 6\). This implies \(K\) is monogenic with power basis \(\{1, \theta, \theta^2, \theta^3, \theta^4, \theta^5\}\) if and only if \(t = 6\). We wish to find conditions on \(a\) and \(b\) such that \(t < 6\) and so \(K\) is monogenic as long as these conditions are not satisfied. Assume \(t < 6\) and so \(K\) is not monogenic. Then

\[
(\text{ind}(\theta))^2 \neq 1,
\]

or equivalently,

\[
(\text{ind}(\theta))^2 = 2^s
\]
for \( s \in \{2, 4, 6\} \). Hence,

\[ 2 \mid \text{ind}(\theta). \]

By Theorem 6.1.7, one of the denominators present in an integral basis for the algebraic number field \( K \) is equal to two. Using Theorem 6.1.7, we deduce

\[ \lambda = \frac{a_0 + a_1 \theta + a_2 \theta^2 + a_3 \theta^3 + a_4 \theta^4 + \theta^5}{2} \]

is in an integral basis for \( K \), and hence an algebraic integer, for some integers \( a_i \in \mathbb{Z} \). Moreover, by Remark 6.1.8, we conclude \( t < 6 \) if and only if

\[ \lambda = \frac{a_0 + a_1 \theta + a_2 \theta^2 + a_3 \theta^3 + a_4 \theta^4 + \theta^5}{2} \]

is an algebraic integer for some integers \( a_i \in \{0, 1\} \). Since there are only two possible values for each \( a_i \) \( (i = 0, 1, 2, 3, 4) \), this implies we have \( 2^5 = 32 \) possible values for \( \lambda \).

We will show that we can exclude the following twenty-three cases as \( \lambda \) is never an algebraic integer:

\[ \begin{align*}
(a_0, a_1, a_2, a_3, a_4) &= (0, 0, 0, 0, 0), (0, 0, 0, 0, 1), (0, 0, 0, 1, 1), (0, 0, 1, 0, 0), (0, 0, 1, 0, 1), \\
& \quad (0, 0, 1, 1, 0), (0, 1, 0, 0, 1), (0, 1, 0, 1, 1), (0, 1, 0, 1, 0), (0, 1, 1, 0, 0), \\
& \quad (0, 1, 1, 1, 0), (0, 1, 1, 1, 1), (1, 0, 0, 0, 0), (1, 0, 0, 0, 1), (1, 0, 0, 1, 0), \\
& \quad (1, 0, 1, 0, 0), (1, 0, 1, 0, 1), (1, 0, 1, 1, 1), (1, 1, 0, 0, 0), (1, 1, 0, 1, 0), \\
& \quad (1, 1, 0, 1, 1), (1, 1, 1, 0, 1), (1, 1, 1, 1, 0).
\end{align*} \]

**Case** \((0, 0, 0, 0, 0)\) : \( \lambda = \frac{\theta^5}{2} \)

We begin first by using MAPLE\textsuperscript{TM} to determine the sextic polynomial

\[ x^6 + cx^5 + dx^4 + ex^3 + fx^2 + gx + h \]

satisfied by \( \lambda \) where \( c, d, e, f, g, h \in \mathbb{Z} \). Note that both this sextic polynomial as well
as
\[ f(x) = x^6 + ax^4 + bx^2 + 1 \]

have \( \theta \) as a root. Using MAPLE\textsuperscript{TM}, we compute the remainder of this division and set each of its coefficients equal to zero. We find
\[ h = \frac{1}{64} \notin \mathbb{Z} \]

and so \( \lambda \) is not algebraic integer.

**Case** \((0,0,0,0,1) : \ \lambda = \frac{\theta^4 + \theta^5}{2} \)

Using a similar method to the one used in the above case, we find
\[ f = \frac{f_1}{16} \]

where \( f_1 \) is a polynomial in terms of \( a \) and \( b \) with integral coefficients such that
\[ f_1 \equiv 1 + a + ba + b^2 + ba^2 + b^3 + b^3a + b^4 + b^4a + b^5 \pmod{2} \]
\[ \equiv 1 + a \pmod{2}. \]

Thus, we see that \( a \equiv 1 \pmod{2} \) and so we set \( a = 2k + 1 \ (k \in \mathbb{Z}) \) and find that
\[ g = \frac{g_1}{16} \]

where \( g_1 \) is a polynomial in terms of \( b \) and \( k \) with integral coefficients such that
\[ g_1 \equiv 1 + b^3 \pmod{2}. \]

Thus, we see that \( b \equiv 1 \pmod{2} \) and so we set \( b = 2m + 1 \ (m \in \mathbb{Z}) \) and find that
\[ d = 4m - \frac{3}{2}k + 11m^2 + 18k^3 + 24k^4 + 2k^2 - 20k^3m - 38k^2m - 13km + 10km^2 + 8k^5. \]
Since $d \in \mathbb{Z}$, we see that $k \equiv 0 \pmod{2}$ and so we set $k = 2w$ ($w \in \mathbb{Z}$). We then find

$$e = \frac{-5}{2}m + 10m^3 + 3w + 24wm^3 - 64w^3m^2 - 64w^2m^2 + 32w^2 + 128w^4 + 144w^3 + 10m^2 - 64w^3m - 112w^2m - 34wm + 16wm^2$$

and so $m \equiv 0 \pmod{2}$ and so we set $m = 2j$ ($j \in \mathbb{Z}$). We find

$$f = \frac{f_2}{8}$$

where $f_2$ is a polynomial in terms of $j$ and $w$ with integral coefficients such that

$$f_2 \equiv 1 \pmod{2}.$$

Since $f \in \mathbb{Z}$, we require $f_2 \equiv 0 \pmod{2}$. Thus, $\lambda$ is not algebraic integer.

**Case (0, 0, 0, 1, 1):** $\lambda = \frac{\theta^3 + \theta^4 + \theta^5}{2}$

Using a similar method to the one used in the above case, we find

$$e = \frac{e_1}{4}$$

where $e_1$ is a polynomial in terms of $a$ and $b$ with integral coefficients such that

$$e_1 \equiv b^2a^3 + b^2a^2 + b^3a + b^2a + a + b^2 + b + 1 \pmod{2}$$

$$\equiv a + 1 \pmod{2}.$$ 

Thus, we see that $a \equiv 1 \pmod{2}$ and so we set $a = 2k + 1$ ($k \in \mathbb{Z}$) and find that

$$g = \frac{g_1}{16}$$
where \( g_1 \) is a polynomial in terms of \( b \) and \( k \) with integral coefficients such that

\[
g_1 \equiv 1 + b + b^3 \pmod{2} \\
\equiv 1 \pmod{2}.
\]

Since \( g \in \mathbb{Z} \), we require \( g_1 \equiv 0 \pmod{2} \). Thus, \( \lambda \) is not algebraic integer.

**Case** \( (0, 0, 1, 0, 0) \): \( \lambda = \varphi^{\alpha + \beta^5} \)

Using a similar method to the one used in the above case, we find

\[
e = \frac{e_1}{4}
\]

where \( e_1 \) is a polynomial in terms of \( a \) and \( b \) with integral coefficients such that

\[
e_1 \equiv ba^4 + a^3 \pmod{2}.
\]

This implies either \( a \equiv 0 \pmod{2} \) or \( a \equiv b \equiv 1 \pmod{2} \).

First assume \( a \equiv 0 \pmod{2} \) and so we set \( a = 2k \ (k \in \mathbb{Z}) \) and find that

\[
g = \frac{g_1}{16}
\]

where \( g_1 \) is a polynomial in terms of \( b \) and \( k \) with integral coefficients such that

\[
g_1 \equiv b^4 \pmod{2}.
\]

This implies \( b \equiv 0 \pmod{2} \) and so we set \( b = 2m \ (m \in \mathbb{Z}) \) and find that

\[
d = \frac{d_1}{2}
\]
where \( d_1 \) is a polynomial in terms of \( k \) and \( m \) with integral coefficients such that
\[
d_1 \equiv m \pmod{2}.
\]
This implies \( m \equiv 0 \pmod{2} \) and so we set \( m = 2n \ (n \in \mathbb{Z}) \) and find that
\[
e = \frac{e_2}{2}
\]
where \( e_2 \) is a polynomial in terms of \( k \) and \( n \) with integral coefficients such that
\[
e_2 \equiv 1 \pmod{2}.
\]
Since \( e \in \mathbb{Z} \), we require \( e_2 \equiv 0 \pmod{2} \). Thus, \( \lambda \) is not algebraic integer.
Now assume \( a \equiv b \equiv 1 \pmod{2} \). So we set \( a = 2l + 1, b = 2j + 1 \ (l, j \in \mathbb{Z}) \) and find that
\[
d = \frac{d_2}{2}
\]
where \( d_2 \) is a polynomial in terms of \( l \) and \( j \) with integral coefficients such that
\[
d_2 \equiv l \pmod{2}.
\]
This implies \( l \equiv 0 \pmod{2} \) and so we set \( l = 2p \ (p \in \mathbb{Z}) \) and find that
\[
e = \frac{e_3}{2}
\]
where \( e_3 \) is a polynomial in terms of \( j \) and \( p \) with integral coefficients such that
\[
e_3 \equiv j \pmod{2}.
\]
This implies \( j \equiv 0 \pmod{2} \) and so we set \( j = 2q \) \((q \in \mathbb{Z})\) and find that

\[
f = \frac{f_1}{8}
\]

where \( f_1 \) is a polynomial in terms of \( p \) and \( q \) with integral coefficients such that

\[
f_1 \equiv 1 \pmod{2}.
\]

Since \( f \in \mathbb{Z} \), we require \( f_1 \equiv 0 \pmod{2} \). Thus, \( \lambda \) is not algebraic integer.

**Case \((0, 0, 1, 0, 1)\) : \( \lambda = \frac{\theta^2 + \theta^4 + \theta^5}{2} \)**

Using a similar method to the one used in the above case, we find

\[
g = \frac{g_1}{16}
\]

where \( g_1 \) is a polynomial in terms of \( a \) and \( b \) with integral coefficients such that

\[
g_1 \equiv b + a^2 + ba^3 + 1 + b^3a + b^4 \pmod{2}
\]

\[
\equiv a^2 + 1 \pmod{2}.
\]

This implies \( a \equiv 1 \pmod{2} \) and so we set \( a = 2k + 1 \) \((k \in \mathbb{Z})\) and find that

\[
d = \frac{d_1}{4}
\]

where \( d_1 \) is a polynomial in terms of \( b \) and \( k \) with integral coefficients such that

\[
d_1 \equiv b^2 \pmod{2}.
\]

This implies \( b \equiv 0 \pmod{2} \) and so we set \( b = 2j \) \((j \in \mathbb{Z})\) and find that

\[
e = \frac{e_1}{2}
\]
where $e_1$ is a polynomial in terms of $j$ and $k$ with integral coefficients such that

$$e_1 \equiv j \pmod{2}.$$

This implies $j \equiv 0 \pmod{2}$ and so we set $j = 2m \ (m \in \mathbb{Z})$ and find that

$$f = \frac{f_1}{4}$$

where $f_1$ is a polynomial in terms of $m$ and $k$ with integral coefficients such that

$$f_1 \equiv 1 \pmod{2}.$$ 

Since $f \in \mathbb{Z}$, we require $f_1 \equiv 0 \pmod{2}$. Thus, $\lambda$ is not algebraic integer.

**Case** $(0, 0, 1, 1, 0) : \quad \lambda = \frac{\theta^2 + \theta^3 + \theta^5}{2}$

Using a similar method to the one used in the above case, we find

$$d = \frac{d_1}{4}$$

where $d_1$ is a polynomial in terms of $a$ and $b$ with integral coefficients such that

$$d_1 \equiv a^5 + ba^3 + a^3 + ba + b^2a + b + 1 \pmod{2}$$

$$\equiv b^2a + b + 1 \pmod{2}.$$ 

This implies $b \equiv 1 \pmod{2}$ and so we set $b = 2k + 1 \ (k \in \mathbb{Z})$ and find that

$$d = \frac{d_2}{4}$$

where $d_2$ is a polynomial in terms of $a$ and $k$ with integral coefficients such that

$$d_2 \equiv a^5 \pmod{2}.$$
This implies \( a \equiv 0 \pmod{2} \) and so we set \( a = 2j \) \((j \in \mathbb{Z})\) and find that

\[
e = \frac{e_1}{2}
\]

where \( e_1 \) is a polynomial in terms of \( j \) and \( k \) with integral coefficients such that

\[
e_1 \equiv j \pmod{2}.
\]

This implies \( j \equiv 0 \pmod{2} \) and so we set \( j = 2m \) \((m \in \mathbb{Z})\) and find that

\[
f = \frac{f_1}{4}
\]

where \( f_1 \) is a polynomial in terms of \( m \) and \( k \) with integral coefficients such that

\[
f_1 \equiv 1 \pmod{2}.
\]

Since \( f \in \mathbb{Z} \), we require \( f_1 \equiv 0 \pmod{2} \). Thus, \( \lambda \) is not algebraic integer.

**Case** \((0, 1, 0, 0, 1) : \quad \lambda = \frac{\theta + \theta^4 + \theta^5}{2} \)

Using a similar method to the one used in the above case, we find

\[
g = \frac{g_1}{16}
\]

where \( g_1 \) is a polynomial in terms of \( a \) and \( b \) with integral coefficients such that

\[
g_1 \equiv 1 + a^2 + ba + ba^2 + b^2 + ba^3 + b^3 \pmod{2}
\]

\[
\equiv 1 + a^2 + ba \pmod{2}.
\]

This implies \( a \equiv 1 \pmod{2} \) and so we set \( a = 2k + 1 \) \((k \in \mathbb{Z})\) and find that

\[
d = \frac{d_1}{4}
\]
where \( d_1 \) is a polynomial in terms of \( b \) and \( k \) with integral coefficients such that

\[
d_1 \equiv b^2 \pmod 2.
\]

This implies \( b \equiv 0 \pmod 2 \) and so we set \( b = 2j \ (j \in \mathbb{Z}) \) and find that

\[
e = \frac{e_1}{4}
\]

where \( e_1 \) is a polynomial in terms of \( j \) and \( k \) with integral coefficients such that

\[
e_1 \equiv 1 \pmod 2.
\]

Since \( e \in \mathbb{Z} \), we require \( e_1 \equiv 0 \pmod 2 \). Thus, \( \lambda \) is not algebraic integer.

**Case** \((0, 1, 0, 1, 0)\):

\[
\lambda = \frac{\theta + \theta^3 + \theta^5}{2}
\]

Using a similar method to the one used in the above case, we find

\[
d = \frac{d_1}{4}
\]

where \( d_1 \) is a polynomial in terms of \( a \) and \( b \) with integral coefficients such that

\[
d_1 \equiv a^5 + ba^3 + a^3 + a^2 + b^2a + a + ba + 1 + b \pmod 2
\]

\[
\equiv ba^3 + 1 + b \pmod 2.
\]

This implies \( b \equiv 1 \pmod 2 \) and so we set \( b = 2k + 1 \ (k \in \mathbb{Z}) \) and find that

\[
d = \frac{d_2}{4}
\]
where $d_2$ is a polynomial in terms of $a$ and $k$ with integral coefficients such that

$$
d_2 \equiv a^5 + a^2 + a \pmod{2}
\equiv a \pmod{2}.
$$

This implies $a \equiv 0 \pmod{2}$ and so we set $a = 2j \ (j \in \mathbb{Z})$ and find that

$$f = \frac{f_1}{16},$$

where $f_1$ is a polynomial in terms of $j$ and $k$ with integral coefficients such that

$$f_1 \equiv 1 \pmod{2}.$$ 

Since $f \in \mathbb{Z}$, we require $f_1 \equiv 0 \pmod{2}$. Thus, $\lambda$ is not algebraic integer.

**Case (0, 1, 0, 1, 1) :** $\lambda = \frac{\theta + \theta^3 + \theta^4 + \theta^5}{2}$

Using a similar method to the one used in the above case, we find

$$g = \frac{g_1}{16},$$

where $g_1$ is a polynomial in terms of $a$ and $b$ with integral coefficients such that

$$g_1 \equiv a + b + a^2 + ba + b^2 + ba^3 + b^3 + 1 \pmod{2}
\equiv b + 1 \pmod{2}.$$ 

This implies $b \equiv 1 \pmod{2}$ and so we set $b = 2k + 1 \ (k \in \mathbb{Z})$ and find that

$$e = \frac{e_1}{4}.$$
where \( e_1 \) is a polynomial in terms of \( a \) and \( k \) with integral coefficients such that

\[
e_1 \equiv a^2 + a^3 \pmod{2}.
\]

Thus we either have \( a \equiv 0 \pmod{2} \) or \( a \equiv 1 \pmod{2} \).

First assume \( a \equiv 0 \pmod{2} \) and so we set \( a = 2j \ (j \in \mathbb{Z}) \) and find that

\[
e = \frac{e_2}{2}
\]

where \( e_2 \) is a polynomial in terms of \( j \) and \( k \) with integral coefficients such that

\[
e_2 \equiv k + 1 \pmod{2}.
\]

This implies \( k \equiv 1 \pmod{2} \) and so we set \( k = 2l + 1 \ (l \in \mathbb{Z}) \) and find that

\[
f = \frac{f_1}{4}
\]

where \( f_1 \) is a polynomial in terms of \( j \) and \( l \) with integral coefficients such that

\[
f_1 \equiv 1 \pmod{2}.
\]

Since \( f \in \mathbb{Z} \), we require \( f_1 \equiv 0 \pmod{2} \). Thus, \( \lambda \) is not algebraic integer.

Now assume \( a \equiv 1 \pmod{2} \) and so we set \( a = 2m + 1 \ (m \in \mathbb{Z}) \) and find that

\[
d = \frac{d_1}{2}
\]

where \( d_1 \) is a polynomial in terms of \( m \) and \( k \) with integral coefficients such that

\[
d_1 \equiv k \pmod{2}.
\]
This implies \( k \equiv 0 \pmod{2} \) and so we set \( k = 2n \ (n \in \mathbb{Z}) \) and find that

\[
e = \frac{e_3}{2}
\]

where \( e_3 \) is a polynomial in terms of \( m \) and \( n \) with integral coefficients such that

\[
e_3 \equiv m \pmod{2}.
\]

This implies \( m \equiv 0 \pmod{2} \) and so we set \( m = 2p \ (p \in \mathbb{Z}) \) and find that

\[
f = \frac{f_2}{8}
\]

where \( f_2 \) is a polynomial in terms of \( n \) and \( p \) with integral coefficients such that

\[
f_2 \equiv 1 \pmod{2}.
\]

Since \( f \in \mathbb{Z} \), we require \( f_2 \equiv 0 \pmod{2} \). Thus, \( \lambda \) is not algebraic integer.

**Case** \((0, 1, 1, 0, 0)\): \( \lambda = \frac{\theta_1 + \theta_2 + \theta_3}{2} \)

Using a similar method to the one used in the above case, we find

\[
h = \frac{h_1}{64}
\]

where \( h_1 \) is a polynomial in terms of \( a \) and \( b \) with integral coefficients such that

\[
h_1 \equiv a + 1 + a^2 + a^3 + a^4 + ba^3 + b^2a + b^3 + b^4 \pmod{2}
\]

\[
\equiv 1 + ba^3 + b^2a \pmod{2}.
\]

This implies \( b \equiv 1 \pmod{2} \) and so we set \( b = 2k + 1 \ (k \in \mathbb{Z}) \) and find that

\[
g = \frac{g_1}{16}
\]
where $g_1$ is a polynomial in terms of $a$ and $k$ with integral coefficients such that

$$
g_1 \equiv a + a^2 + a^3 \pmod{2}
\equiv a \pmod{2}.
$$

This implies $a \equiv 0 \pmod{2}$ and so we set $a = 2j$ ($j \in \mathbb{Z}$) and find that

$$
d = \frac{d_1}{4}
$$

where $d_1$ is a polynomial in terms of $j$ and $k$ with integral coefficients such that

$$
d_1 \equiv 1 \pmod{2}.
$$

Since $d \in \mathbb{Z}$, we require $d_1 \equiv 0 \pmod{2}$. Thus, $\lambda$ is not algebraic integer.

**Case** $(0, 1, 1, 1, 0)$: $\lambda = \frac{\theta + \theta^2 + \theta^3 + \theta^5}{2}$

Using a similar method to the one used in the above case, we find

$$
g = \frac{g_1}{16}
$$

where $g_1$ is a polynomial in terms of $a$ and $b$ with integral coefficients such that

$$
g_1 \equiv 1 + a^2 + ba + b^2 + b^2a + b^2a^2 + b^4 \pmod{2}
\equiv 1 + a^2 \pmod{2}.
$$

This implies $a \equiv 1 \pmod{2}$ and so we set $a = 2k + 1$ ($k \in \mathbb{Z}$) and find that

$$
e = \frac{e_1}{2}$$
where \( e_1 \) is a polynomial in terms of \( b \) and \( k \) with integral coefficients such that

\[
e_1 \equiv 1 + b^3 \pmod{2}.
\]

This implies \( b \equiv 1 \pmod{2} \) and so we set \( b = 2j + 1 \) \((j \in \mathbb{Z})\) and find that

\[
d = \frac{d_1}{2}
\]

where \( d_1 \) is a polynomial in terms of \( j \) and \( k \) with integral coefficients such that

\[
d_1 \equiv j \pmod{2}.
\]

This implies \( j \equiv 0 \pmod{2} \) and so we set \( j = 2m \) \((m \in \mathbb{Z})\) and find that

\[
g = \frac{g_2}{8}
\]

where \( g_2 \) is a polynomial in terms of \( k \) and \( m \) with integral coefficients such that

\[
g_2 \equiv k + 1 \pmod{2}.
\]

This implies \( k \equiv 1 \pmod{2} \) and so we set \( k = 2p + 1 \) \((p \in \mathbb{Z})\) and find that

\[
f = \frac{f_1}{8}
\]

where \( f_1 \) is a polynomial in terms of \( m \) and \( p \) with integral coefficients such that

\[
f_1 \equiv 1 \pmod{2}.
\]

Since \( f \in \mathbb{Z} \), we require \( f_1 \equiv 0 \pmod{2} \). Thus, \( \lambda \) is not algebraic integer.

**Case** \((0, 1, 1, 1, 1)\) : \( \lambda = \frac{\theta + \theta^2 + \theta^3 + \theta^4 + \theta^5}{2} \)
Using a similar method to the one used in the above case, we find

\[ f = \frac{f_1}{16} \]

where \( f_1 \) is a polynomial in terms of \( a \) and \( b \) with integral coefficients such that

\[
f_1 \equiv ba^4 + a^3 + b^2a^3 + b^2a^2 + ba^2 + b^3a^2 + b^4a + b^3a + b^4 + 1 + b^5 \pmod{2} \]

\[
\equiv a^3 + b^4a + 1 \pmod{2}.
\]

This implies \( a \equiv 1 \pmod{2} \) and so we set \( a = 2k + 1 \) \((k \in \mathbb{Z})\) and find that

\[ g = \frac{g_1}{16} \]

where \( g_1 \) is a polynomial in terms of \( b \) and \( k \) with integral coefficients such that

\[
g_1 \equiv b + 1 + b^3 + b^4 \pmod{2}
\]

\[
\equiv b + 1 \pmod{2}.
\]

This implies \( b \equiv 1 \pmod{2} \) and so we set \( b = 2j + 1 \) \((j \in \mathbb{Z})\) and find that

\[ h = \frac{h_1}{64} \]

where \( h_1 \) is a polynomial in terms of \( j \) and \( k \) with integral coefficients such that

\[ h_1 \equiv 1 \pmod{2}. \]

Since \( h \in \mathbb{Z} \), we require \( h_1 \equiv 0 \pmod{2} \). Thus, \( \lambda \) is not algebraic integer.

**Case** \((1, 0, 0, 0, 0)\) : \( \lambda = \frac{1 + \phi^5}{2} \)
Using a similar method to the one used in the above case, we find

\[ d = \frac{d_1}{4} \]

where \( d_1 \) is a polynomial in terms of \( a \) and \( b \) with integral coefficients such that

\[
\begin{align*}
d_1 &\equiv a^5 + ba^3 + a^2 + b^2a + 1 + b \pmod{2} \\
&\equiv ba^3 + b^2a + 1 + b \pmod{2}.
\end{align*}
\]

This implies \( b \equiv 1 \pmod{2} \) and so we set \( b = 2k + 1 \) \((k \in \mathbb{Z})\) and find that

\[
f = \frac{f_1}{16}
\]

where \( f_1 \) is a polynomial in terms of \( a \) and \( k \) with integral coefficients such that

\[
f_1 \equiv a^2 + 1 \pmod{2}.
\]

This implies \( a \equiv 1 \pmod{2} \) and so we set \( a = 2j + 1 \) \((j \in \mathbb{Z})\) and find that

\[
d = \frac{d_2}{2}
\]

where \( d_2 \) is a polynomial in terms of \( j \) and \( k \) with integral coefficients such that

\[
d_2 \equiv j \pmod{2}.
\]

This implies \( j \equiv 0 \pmod{2} \) and so we set \( j = 2m \) \((m \in \mathbb{Z})\) and find that

\[
g = \frac{g_1}{8}
\]
where \( g_1 \) is a polynomial in terms of \( k \) and \( m \) with integral coefficients such that

\[
g_1 \equiv k + 1 \pmod{2}.
\]

This implies \( k \equiv 1 \pmod{2} \) and so we set \( k = 2n + 1 \ (n \in \mathbb{Z}) \) and find that

\[
f = \frac{f_2}{4}
\]

where \( f_2 \) is a polynomial in terms of \( m \) and \( n \) with integral coefficients such that

\[
f_2 \equiv n \pmod{2}.
\]

This implies \( n \equiv 0 \pmod{2} \) and so we set \( n = 2p \ (p \in \mathbb{Z}) \) and find that

\[
h = \frac{h_1}{32}
\]

where \( h_1 \) is a polynomial in terms of \( m \) and \( p \) with integral coefficients such that

\[
h_1 \equiv 1 \pmod{2}.
\]

Since \( h \in \mathbb{Z} \), we require \( h_1 \equiv 0 \pmod{2} \). Thus, \( \lambda \) is not algebraic integer.

**Case** \((1, 0, 0, 0, 1) : \lambda = \frac{1 + \theta^4 + \theta^5}{2} \)

Using a similar method to the one used in the above case, we find

\[
f = \frac{f_1}{16}
\]

where \( f_1 \) is a polynomial in terms of \( a \) and \( b \) with integral coefficients such that

\[
f_1 \equiv a + ba + b^2 + ba^2 + b^3 + b^2a + b^4 + b^3a + b^5 \pmod{2}
\equiv a \pmod{2}.
\]
This implies $a \equiv 0 (\text{mod } 2)$ and so we set $a = 2k \ (k \in \mathbb{Z})$ and find that

$$d = \frac{d_1}{4}$$

where $d_1$ is a polynomial in terms of $b$ and $k$ with integral coefficients such that

$$d_1 \equiv b + 1 \ (\text{mod } 2).$$

This implies $b \equiv 1 (\text{mod } 2)$ and so we set $b = 2j + 1 \ (j \in \mathbb{Z})$ and find that

$$e = \frac{e_1}{2}$$

where $e_1$ is a polynomial in terms of $j$ and $k$ with integral coefficients such that

$$e_1 \equiv 1 \ (\text{mod } 2).$$

Since $e \in \mathbb{Z}$, we require $e_1 \equiv 0 (\text{mod } 2)$. Thus, $\lambda$ is not algebraic integer.

**Case** $(1, 0, 0, 1, 0)$: $\lambda = \frac{1 + \theta^3 + \theta^5}{2}$

Using a similar method to the one used in the above case, we find

$$f = \frac{f_1}{16}$$

where $f_1$ is a polynomial in terms of $a$ and $b$ with integral coefficients such that

$$f_1 \equiv ba^3 + ba^2 + a^2 + b^3a^2 + ba + a + b^3a + b^3 + b + b^2 + b^5 \ (\text{mod } 2) \equiv ba \ (\text{mod } 2).$$

This implies $a \equiv 0 (\text{mod } 2)$ or $b \equiv 0 (\text{mod } 2)$. 

75
First assume \( a \equiv 0 \pmod{2} \) and so we set \( a = 2k \ (k \in \mathbb{Z}) \) and find that

\[ d = \frac{d_1}{4} \]

where \( d_1 \) is a polynomial in terms of \( b \) and \( k \) with integral coefficients such that

\[ d_1 \equiv b \pmod{2}. \]

This implies \( b \equiv 0 \pmod{2} \) and so we set \( b = 2j \ (j \in \mathbb{Z}) \) and find that

\[ d = \frac{d_2}{2} \]

where \( d_2 \) is a polynomial in terms of \( j \) and \( k \) with integral coefficients such that

\[ d_2 \equiv 1 + j \pmod{2}. \]

This implies \( j \equiv 1\pmod{2} \) and so we set \( j = 2m + 1 \ (m \in \mathbb{Z}) \) and find that

\[ h = \frac{h_1}{64} \]

where \( h_1 \) is a polynomial in terms of \( k \) and \( m \) with integral coefficients such that

\[ h_1 \equiv 1 \pmod{2}. \]

Since \( h \in \mathbb{Z} \), we require \( h_1 \equiv 0 \pmod{2} \). Thus, \( \lambda \) is not algebraic integer.

Now we assume \( b \equiv 0 \pmod{2} \) and so we set \( b = 2l \ (l \in \mathbb{Z}) \) and find that

\[ d = \frac{d_3}{4} \]
where \( d_3 \) is a polynomial in terms of \( a \) and \( l \) with integral coefficients such that

\[
d_3 \equiv a^5 + a^3 + a^2 \pmod{2}
\]

\[
\equiv a^2 \pmod{2}.
\]

This implies \( a \equiv 0 \pmod{2} \) and so we set \( a = 2p \ (p \in \mathbb{Z}) \) and find that

\[
h = \frac{h_2}{64}
\]

where \( h_2 \) is a polynomial in terms of \( l \) and \( p \) with integral coefficients such that

\[
h_2 \equiv 1 \pmod{2}.
\]

Since \( h \in \mathbb{Z} \), we require \( h_2 \equiv 0 \pmod{2} \). Thus, \( \lambda \) is not algebraic integer.

**Case** \((1, 0, 1, 0, 0)\): \( \lambda = \frac{1+\theta^2+\theta^6}{2} \)

Using a similar method to the one used in the above case, we find

\[
f = \frac{f_1}{16}
\]

where \( f_1 \) is a polynomial in terms of \( a \) and \( b \) with integral coefficients such that

\[
f_1 \equiv ba^2 + b^2 + b^2a^3 + b^5 + 1 \pmod{2}
\]

\[
\equiv ba^2 + b^2a^3 + 1 \pmod{2}.
\]

This implies \( b \equiv 1 \pmod{2} \) and so we set \( b = 2k + 1 \ (k \in \mathbb{Z}) \) and find that

\[
d = \frac{d_1}{4}
\]
where \( d_1 \) is a polynomial in terms of \( a \) and \( k \) with integral coefficients such that

\[
d_1 \equiv a^5 + a^3 + a \pmod{2}
\]
\[
\equiv a \pmod{2}.
\]

This implies \( a \equiv 0 \pmod{2} \) and so we set \( a = 2j \ (j \in \mathbb{Z}) \) and find that

\[
f = \frac{f_2}{16}
\]

where \( f_2 \) is a polynomial in terms of \( j \) and \( k \) with integral coefficients such that

\[
f_2 \equiv 1 \pmod{2}.
\]

Since \( f \in \mathbb{Z} \), we require \( f_2 \equiv 0 \pmod{2} \). Thus, \( \lambda \) is not algebraic integer.

**Case** \((1, 0, 1, 0, 1)\) : \( \lambda = \frac{1 + \theta^2 + \theta^4 + \theta^5}{2} \)

Using a similar method to the one used in the above case, we find

\[
d = \frac{d_1}{4}
\]

where \( d_1 \) is a polynomial in terms of \( a \) and \( b \) with integral coefficients such that

\[
d_1 \equiv a^5 + a^4 + ba^3 + b^2a + 1 + b \pmod{2}
\]
\[
\equiv 1 + b \pmod{2}.
\]

This implies \( b \equiv 1 \pmod{2} \) and so we set \( b = 2k + 1 \ (k \in \mathbb{Z}) \) and find that

\[
e = \frac{e_1}{4}
\]
where \( e_1 \) is a polynomial in terms of \( a \) and \( k \) with integral coefficients such that

\[
e_1 \equiv a + a^3 + a^4 + 1 \pmod{2}
\]

\[
e_1 \equiv a + 1 \pmod{2}.
\]

This implies \( a \equiv 1 \pmod{2} \) and so we set \( a = 2j + 1 \ (j \in \mathbb{Z}) \) and find that

\[
d = \frac{d_2}{2}
\]

where \( d_2 \) is a polynomial in terms of \( j \) and \( k \) with integral coefficients such that

\[
d_2 \equiv j \pmod{2}.
\]

This implies \( j \equiv 0 \pmod{2} \) and so we set \( j = 2m \ (m \in \mathbb{Z}) \) and find that

\[
g = \frac{g_1}{8}
\]

where \( g_1 \) is a polynomial in terms of \( k \) and \( m \) with integral coefficients such that

\[
g_1 \equiv 1 + k \pmod{2}.
\]

This implies \( k \equiv 1 \pmod{2} \) and so we set \( k = 2p + 1 \ (p \in \mathbb{Z}) \) and find that

\[
f = \frac{f_1}{8}
\]

where \( f_1 \) is a polynomial in terms of \( m \) and \( p \) with integral coefficients such that

\[
f_1 \equiv 1 \pmod{2}.
\]

Since \( f \in \mathbb{Z} \), we require \( f_1 \equiv 0 \pmod{2} \). Thus, \( \lambda \) is not algebraic integer.
**Case** (1, 0, 1, 1, 1) : \( \lambda = \frac{1+\theta^2+\theta^3+\theta^4+\theta^5}{2} \)

Using a similar method to the one used in the above case, we find

\[
e = \frac{e_1}{4}
\]

where \( e_1 \) is a polynomial in terms of \( a \) and \( b \) with integral coefficients such that

\[
e_1 \equiv ba^4 + a^3 + b^2a^3 + ba^3 + b^2a^2 + a^2 + ba^2 + b^3a + 1 + b^2 \pmod{2}
\]

\[
\equiv 1 + b^2 \pmod{2}.
\]

This implies \( b \equiv 1 \pmod{2} \) and so we set \( b = 2k + 1 \ (k \in \mathbb{Z}) \) and find that

\[
f = \frac{f_1}{16}
\]

where \( f_1 \) is a polynomial in terms of \( a \) and \( k \) with integral coefficients such that

\[
f_1 \equiv a^2 \pmod{2}.
\]

This implies \( a \equiv 0 \pmod{2} \) and so we set \( a = 2j \ (j \in \mathbb{Z}) \) and find that

\[
d = \frac{d_1}{4}
\]

where \( d_1 \) is a polynomial in terms of \( j \) and \( k \) with integral coefficients such that

\[
d_1 \equiv 1 \pmod{2}.
\]

Since \( d \in \mathbb{Z} \), we require \( d_1 \equiv 0 \pmod{2} \). Thus, \( \lambda \) is not algebraic integer.

**Case** (1, 1, 0, 0, 0) : \( \lambda = \frac{1+\theta+\theta^5}{2} \)
Using a similar method to the one used in the above case, we find

\[ f = \frac{f_1}{16} \]

where \( f_1 \) is a polynomial in terms of \( a \) and \( b \) with integral coefficients such that

\[
f_1 \equiv ba^4 + a^3 + ba^2 + b^3a + ab + a + b + b^2 + b^5 \pmod{2}
\equiv b \pmod{2}.
\]

This implies \( b \equiv 0 \pmod{2} \) and so we set \( b = 2k \ (k \in \mathbb{Z}) \) and find that

\[ d = \frac{d_1}{4} \]

where \( d_1 \) is a polynomial in terms of \( a \) and \( k \) with integral coefficients such that

\[
d_1 \equiv a^5 + a^2 + a + 1 \pmod{2}
\equiv a + 1 \pmod{2}.
\]

This implies \( a \equiv 1 \pmod{2} \) and so we set \( a = 2j + 1 \ (j \in \mathbb{Z}) \) and find that

\[ d = \frac{d_2}{2} \]

where \( d_2 \) is a polynomial in terms of \( j \) and \( k \) with integral coefficients such that

\[ d_2 \equiv 1 \pmod{2}. \]

Since \( d \in \mathbb{Z} \), we require \( d_2 \equiv 0 \pmod{2} \). Thus, \( \lambda \) is not algebraic integer.

**Case** \((1, 1, 0, 1, 0)\): \( \lambda = \frac{1 + \theta + \theta^3 + \theta^5}{2} \)
Using a similar method to the one used in the above case, we find

\[ f = \frac{f_1}{16} \]

where \( f_1 \) is a polynomial in terms of \( a \) and \( b \) with integral coefficients such that

\[
\begin{align*}
f_1 & \equiv ba^4 + ba^3 + a^3 + a^2 + b^3a^2 + b^3a + b^3 + 1 + b^2 + b^5 \pmod{2} \\
& \equiv b^2 + 1 \pmod{2}.
\end{align*}
\]

This implies \( b \equiv 1 \pmod{2} \) and so we set \( b = 2k + 1 \ (k \in \mathbb{Z}) \) and find that

\[ d = \frac{d_1}{4} \]

where \( d_1 \) is a polynomial in terms of \( a \) and \( k \) with integral coefficients such that

\[
\begin{align*}
d_1 & \equiv a^5 + a^2 + a + 1 \pmod{2} \\
& \equiv a + 1 \pmod{2}.
\end{align*}
\]

This implies \( a \equiv 1 \pmod{2} \) and so we set \( a = 2j + 1 \ (j \in \mathbb{Z}) \) and find that

\[ d = \frac{d_2}{2} \]

where \( d_2 \) is a polynomial in terms of \( j \) and \( k \) with integral coefficients such that

\[ d_2 \equiv k \pmod{2}. \]

This implies \( k \equiv 0 \pmod{2} \) and so we set \( k = 2m \ (m \in \mathbb{Z}) \) and find that

\[ g = \frac{g_1}{8} \]
where \( g_1 \) is a polynomial in terms of \( j \) and \( m \) with integral coefficients such that

\[
g_1 \equiv 1 + j \pmod{2}.
\]

This implies \( j \equiv 1 \pmod{2} \) and so we set \( j = 2p + 1 \) \((p \in \mathbb{Z})\) and find that

\[
h = \frac{h_1}{32}
\]

where \( h_1 \) is a polynomial in terms of \( m \) and \( p \) with integral coefficients such that

\[
h_1 \equiv 1 \pmod{2}.
\]

Since \( h \in \mathbb{Z} \), we require \( h_1 \equiv 0 \pmod{2} \). Thus, \( \lambda \) is not algebraic integer.

**Case** \((1, 1, 0, 1, 1)\):

\[
\lambda = \frac{1 + \theta + \theta^2 + \theta^3 + \theta^5}{2}
\]

Using a similar method to the one used in the above case, we find

\[
g = \frac{g_1}{16}
\]

where \( g_1 \) is a polynomial in terms of \( a \) and \( b \) with integral coefficients such that

\[
g_1 \equiv a + b + ba + a^3 + ba^2 + ba^3 + b^3 + b^2a^2 + ba^4 + b^3a + b^2a^3 + b^4 + b^3a^2 + b^4a + b^5 + 1 \pmod{2}
\]

\[
\equiv ba + 1 \pmod{2}
\]

This implies \( a \equiv 1 \pmod{2} \) and so we set \( a = 2k + 1 \) \((k \in \mathbb{Z})\) and find that

\[
e = \frac{e_1}{4}
\]
where \( e_1 \) is a polynomial in terms of \( b \) and \( k \) with integral coefficients such that

\[
e_1 \equiv b^3 + 1 \pmod{2}.
\]

This implies \( b \equiv 1 \pmod{2} \) and so we set \( b = 2j + 1 \) \((j \in \mathbb{Z})\) and find that

\[
d = \frac{d_1}{4}
\]

where \( d_1 \) is a polynomial in terms of \( j \) and \( k \) with integral coefficients such that

\[
d_1 \equiv 1 \pmod{2}.
\]

Since \( d \in \mathbb{Z} \), we require \( d_1 \equiv 0 \pmod{2} \). Thus, \( \lambda \) is not algebraic integer.

**Case** \((1,1,1,0,1)\) : \( \lambda = \frac{1 + \theta + \theta^2 + \theta^4 + \theta^5}{2} \)

Using a similar method to the one used in the above case, we find

\[
d = \frac{d_1}{4}
\]

where \( d_1 \) is a polynomial in terms of \( a \) and \( b \) with integral coefficients such that

\[
d_1 \equiv a^5 + a^4 + ba^3 + b^2a + a + b + 1 \pmod{2}
\]

\[
\equiv a + b + 1 \pmod{2}.
\]

This implies either \( a \equiv 0 \pmod{2}, b \equiv 1 \pmod{2} \) or \( a \equiv 1 \pmod{2}, b \equiv 0 \pmod{2} \).

First assume \( a \equiv 0 \pmod{2}, b \equiv 1 \pmod{2} \) and so we set \( a = 2k \) \((k \in \mathbb{Z})\) and \( b = 2j + 1 \) \((j \in \mathbb{Z})\) and find that

\[
f = \frac{f_1}{16}
\]

where \( f_1 \) is a polynomial in terms of \( j \) and \( k \) with integral coefficients such that

\[
f_1 \equiv 1 \pmod{2}.
\]
Since $f \in \mathbb{Z}$, we require $f_1 \equiv 0 \pmod{2}$. Thus, $\lambda$ is not algebraic integer.

Now assume $a \equiv 1 \pmod{2}, b \equiv 0 \pmod{2}$ and so we set $a = 2m + 1 \ (m \in \mathbb{Z})$ and $b = 2n \ (n \in \mathbb{Z})$ and find that

$$f = \frac{f_2}{16}$$

where $f_2$ is a polynomial in terms of $m$ and $n$ with integral coefficients such that

$$f_2 \equiv 1 \pmod{2}.$$

Since $f \in \mathbb{Z}$, we require $f_2 \equiv 0 \pmod{2}$. Thus, $\lambda$ is not algebraic integer.

Case $(1, 1, 1, 1, 0)$: $\lambda = \frac{1 + \theta + \theta^2 + \theta^3 + \theta^5}{2}$

Using a similar method to the one used in the above case, we find

$$g = \frac{g_1}{16}$$

where $g_1$ is a polynomial in terms of $a$ and $b$ with integral coefficients such that

$$g_1 \equiv a + b + ba^2 + b^2a^2 + b^3 + 1 + b^2a^3 + b^4 + b^3a^2 + b^5 \pmod{2}$$

$$\equiv a + 1 \pmod{2}.$$

This implies $a \equiv 1 \pmod{2}$ and so we set $a = 2k + 1 \ (k \in \mathbb{Z})$ and find that

$$e = \frac{e_1}{2}$$

where $e_1$ is a polynomial in terms of $b$ and $k$ with integral coefficients such that

$$e_1 \equiv b + b^2 + b^3 + 1 \pmod{2}$$

$$\equiv b + 1 \pmod{2}.$$
This implies \( b \equiv 1 \pmod{2} \) and so we set \( b = 2j + 1 \ (j \in \mathbb{Z}) \) and find that

\[
d = \frac{d_1}{4}
\]

where \( d_1 \) is a polynomial in terms of \( j \) and \( k \) with integral coefficients such that

\[d_1 \equiv 1 \pmod{2}.
\]

Since \( d \in \mathbb{Z} \), we require \( d_1 \equiv 0 \pmod{2} \). Thus, \( \lambda \) is not algebraic integer.

Thus, in the twenty-three cases given above, we have shown \( \lambda \) is never an algebraic integer. In the remaining nine cases, TABLE 6.2.2 gives necessary and sufficient conditions on \( a \) and \( b \) for \( \lambda \) to be an algebraic integer. Thus, \( t < 6 \) if and only if we have the following:

**Table 6.2.2: Lifting Monogenic Cubic Fields - Lemma 6.2.1**

<table>
<thead>
<tr>
<th>((a_0, a_1, a_2, a_3, a_4))</th>
<th>Conditions on ((a, b)) for ( \lambda ) to be an Algebraic Integer</th>
</tr>
</thead>
<tbody>
<tr>
<td>((0, 0, 0, 1, 0))</td>
<td>((a, b) \equiv (3, 3) ) or ((7, 7) \pmod{8})</td>
</tr>
<tr>
<td>((0, 0, 1, 1, 1))</td>
<td>((a, b) \equiv (3, 3) \pmod{4})</td>
</tr>
<tr>
<td>((0, 1, 0, 0, 0))</td>
<td>((a, b) \equiv (1, 1) ) or ((3, 3) \pmod{4})</td>
</tr>
<tr>
<td>((0, 1, 1, 0, 1))</td>
<td>((a, b) \equiv (2, 2) \pmod{4}) or ((a, b) \equiv (3, 3) ) or ((7, 7) \pmod{8})</td>
</tr>
<tr>
<td>((1, 0, 0, 1, 1))</td>
<td>((a, b) \equiv (3, 3) ) or ((7, 7) \pmod{8})</td>
</tr>
<tr>
<td>((1, 0, 1, 1, 0))</td>
<td>((a, b) \equiv (2, 2) ) or ((3, 3) \pmod{4})</td>
</tr>
<tr>
<td>((1, 1, 0, 0, 1))</td>
<td>((a, b) \equiv (1, 1) ) or ((3, 3) \pmod{4})</td>
</tr>
<tr>
<td>((1, 1, 1, 0, 0))</td>
<td>((a, b) \equiv (3, 3) ) or ((7, 7) \pmod{8})</td>
</tr>
<tr>
<td>((1, 1, 1, 1, 1))</td>
<td>((a, b) \equiv (0, 2) ) or ((2, 0) \pmod{4})</td>
</tr>
</tbody>
</table>

We will consider each case separately and show how we obtained these results.

**Case** \((0, 0, 0, 1, 0)\): \( \lambda = \frac{\theta^3 + \theta^5}{2} \)

First assume \((a, b) \equiv (3, 3) \pmod{8}\). We set \( a = 8s + 3 \) and \( b = 8r + 3 \ (r, s \in \mathbb{Z}) \).
Then, by MAPLE\textsuperscript{TM}, $\lambda$ satisfies the polynomial

\[
x^6 + (-22r + 26s - 960rs + 1040s^2 - 4736rs^2 + 6656s^3 + 13312s^4 \\
+ 8192s^5 + 176r^2 + 640r^2s - 5120rs^3)x^4 + (-188rs + 104s^2 + 1888rs^2 \\
- 416s^3 + 1056r^3 + 2816r^4 + 88r^2 - 2528r^2s + 2048r^3s^2 - 6400r^3s \\
+ 4352r^2s^2 - 4096r^4s - 768rs^3)x^2 + r^2 + s^2 - 2rs
\]

which belongs to $\mathbb{Z}[x]$ and so $\lambda$ is an algebraic integer. Now assume $(a, b) \equiv (7, 7)$ (mod 8) and so we set $a = 8q + 7$ and $b = 8p + 7$ ($p, q \in \mathbb{Z}$). Then, by MAPLE\textsuperscript{TM}, $\lambda$ satisfies the polynomial

\[
x^6 + (1154 + 10666q - 1830p + 51200q^3 + 33792q^4 + 8192q^5 - 8896pq + 35024q^2 \\
- 12416pq^2 + 496p^2 + 640p^2q - 5120pq^3)x^4 + (1 + 10q - 6p - 800q^3 + 5024p^3 \\
+ 5888p^4 + 2048p^5 + 2048p^3q^2 - 12544p^3q + 7424p^2q^2 - 4096p^4q - 2364pq \\
+ 1192q^2 + 6624pq^2 + 1176p^2 - 10848p^2q - 768pq^3)x^2 + p^2 - 2pq + q^2
\]

which belongs to $\mathbb{Z}[x]$ and so $\lambda$ is an algebraic integer.

Now we prove the converse. Assume $\lambda$ is an algebraic integer. We begin first by using MAPLE\textsuperscript{TM} to determine the sextic polynomial

\[
x^6 + cx^5 + dx^4 + ex^3 + fx^2 + gx + h
\]

satisfied by $\lambda$ where $c, d, e, f, g, h \in \mathbb{Z}$. Note that both this sextic polynomial as well as

\[f(x) = x^6 + ax^4 + bx^2 + 1\]

have $\theta$ as a root. Using MAPLE\textsuperscript{TM}, we compute the remainder of this division and
set each of its coefficients equal to zero. We find
\[ f = \frac{f_1}{16} \]
where \( f_1 \) is a polynomial in terms of \( a \) and \( b \) with integral coefficients such that
\[
\begin{align*}
    f_1 & \equiv ba^3 + b^3a^2 + ba^2 + a^2 + ba + b^3a + a + b^3 + b^5 + b + b^2 + 1 \pmod{2} \\
    & \equiv ba^3 + 1 \pmod{2}.
\end{align*}
\]
This implies \( a \equiv 1 \pmod{2} \) and \( b \equiv 1 \pmod{2} \) and so we set \( a = 2k + 1 \) (\( k \in \mathbb{Z} \)) and \( b = 2j + 1 \) (\( j \in \mathbb{Z} \)) and find that
\[ d = \frac{d_1}{2} \]
where \( d_1 \) is a polynomial in terms of \( j \) and \( k \) with integral coefficients such that
\[ d_1 \equiv j + k \pmod{2}. \]
This implies either \( j \equiv 0 \pmod{2}, k \equiv 0 \pmod{2} \) or \( j \equiv 1 \pmod{2}, k \equiv 1 \pmod{2} \).
First assume \( j \equiv 0 \pmod{2}, k \equiv 0 \pmod{2} \) and so we set \( j = 2m \) (\( m \in \mathbb{Z} \)) and \( k = 2n \) (\( n \in \mathbb{Z} \)) and find that
\[ f = \frac{f_2}{4} \]
where \( f_2 \) is a polynomial in terms of \( m \) and \( n \) with integral coefficients such that
\[ f_2 \equiv 1 \pmod{2}. \]
Since \( f \in \mathbb{Z} \), we require \( f_2 \equiv 0 \pmod{2} \). Thus, \( \lambda \) is not algebraic integer, a contradiction.
So we must have \( j \equiv 1 \pmod{2}, k \equiv 1 \pmod{2} \). Hence, we set \( j = 2u + 1 \) (\( u \in \mathbb{Z} \)) and
\[ k = 2v + 1 \ (v \in \mathbb{Z}) \] and find that
\[ h = \frac{h_1}{4} \]

where \( h_1 \) is a polynomial in terms of \( u \) and \( v \) with integral coefficients such that
\[ h_1 \equiv u^2 + v^2 \pmod{2}. \]

This implies either \( u \equiv 0 \pmod{2} \), \( v \equiv 0 \pmod{2} \) or \( u \equiv 1 \pmod{2} \), \( v \equiv 1 \pmod{2} \).

First assume \( u \equiv 0 \pmod{2} \), \( v \equiv 0 \pmod{2} \) and so we set \( u = 2r \ (r \in \mathbb{Z}) \) and \( v = 2s \ (s \in \mathbb{Z}) \) and find that every coefficient of \( x^6 + cx^5 + dx^4 + ex^3 + fx^2 + gx + h \) is an integer. Hence,
\[
\begin{aligned}
\begin{cases}
a = 8s + 3 \\
b = 8r + 3
\end{cases}
\end{aligned}
\]
and so \((a, b) \equiv (3, 3) \pmod{8} \).

Now assume \( u \equiv 1 \pmod{2} \), \( v \equiv 1 \pmod{2} \) and so we set \( u = 2p + 1 \ (p \in \mathbb{Z}) \) and \( v = 2q + 1 \ (q \in \mathbb{Z}) \) and find that every coefficient of \( x^6 + cx^5 + dx^4 + ex^3 + fx^2 + gx + h \) is an integer. Hence,
\[
\begin{aligned}
\begin{cases}
a = 8q + 7 \\
b = 8p + 7
\end{cases}
\end{aligned}
\]
and so \((a, b) \equiv (7, 7) \pmod{8} \), which completes the proof for this case.

**Case** \((0, 0, 1, 1, 1) : \) \( \lambda = \frac{\theta^2 + \theta^3 + \theta^4 + \theta^5}{2} \)

Assume \((a, b) \equiv (3, 3) \pmod{4} \). We set \( a = 4n + 3 \) and \( b = 4l + 3 \ (l, n \in \mathbb{Z}) \). Then,
by \textsc{maple™}, \( \lambda \) satisfies the polynomial

\[ x^6 + (-16n^2 - 20n + 8l)x^5 + (3n - 3l + 360n^2 + 256n^5 + 992n^3 + 896n^4 \\
+ 68l^2 + 80l^2n - 328ln - 656ln^2 - 320ln^3)x^4 + (2n - 2l + 344n^2 + 144l^3 \\
+ 720n^3 + 320n^4 + 144l^2 - 224l^2n - 456ln - 544ln^2 + 320ln^3 + 256ln^4 \\
- 256l^2n^3 - 768l^2n^2 + 192l^3n)x^3 + (147n^2 - 64l^3n^2 - 64l^4n + 256l^3 + 240l^4 \\
+ 64l^5 + 120n^3 + 32n^4 + 101l^2 - 500l^2n - 244ln + 128ln^2 + 80ln^3 + 64l^2n^3 \\
+ 48l^2n^2 - 400l^3n)x^2 + (26n^2 + 44l^3 + 16l^4 + 12n^3 + 22l^2 - 80l^2n - 48ln \\
+ 24ln^2 + 16ln^3 - 16l^2n^2 - 16l^3n)x - 4ln - ln^2 + 2l^2 + 2n^2 + n^3 - l^2n + l^3 \]

which belongs to \( \mathbb{Z}[x] \) and so \( \lambda \) is an algebraic integer.

Now we prove the converse. Assume \( \lambda \) is an algebraic integer. We begin first by using \textsc{maple™} to determine the sextic polynomial

\[ x^6 + cx^5 + dx^4 + ex^3 + fx^2 + gx + h \]

satisfied by \( \lambda \) where \( c, d, e, f, g, h \in \mathbb{Z} \). Note that both this sextic polynomial as well as

\[ f(x) = x^6 + ax^4 + bx^2 + 1 \]

have \( \theta \) as a root. Using \textsc{maple™}, we compute the remainder of this division and set each of its coefficients equal to zero. We find

\[ e = \frac{e_1}{4} \]

where \( e_1 \) is a polynomial in terms of \( a \) and \( b \) with integral coefficients such that

\[ e_1 \equiv ba^4 + ba^3 + b^2a^3 + a^3 + ba^2 + a^2 + b^2a^2 + b^3a + 1 + b^2 \pmod{2} \]

\[ \equiv 1 + b^2 \pmod{2}. \]
This implies \( b \equiv 1 \pmod{2} \) and so we set \( b = 2k + 1 \ (k \in \mathbb{Z}) \) and find that

\[
g = \frac{g_1}{16}
\]

where \( g_1 \) is a polynomial in terms of \( a \) and \( k \) with integral coefficients such that

\[
g_1 \equiv a + a^2 + a^3 + 1 \pmod{2}
\]

\[
\equiv 1 + a \pmod{2}.
\]

This implies \( a \equiv 1 \pmod{2} \) and so we set \( a = 2m + 1 \ (m \in \mathbb{Z}) \) and find that

\[
d = \frac{d_1}{2}
\]

where \( d_1 \) is a polynomial in terms of \( k \) and \( m \) with integral coefficients such that

\[
d_1 \equiv m + k \pmod{2}.
\]

This implies either \( m \equiv 0 \pmod{2}, k \equiv 0 \pmod{2} \) or \( m \equiv 1 \pmod{2}, k \equiv 1 \pmod{2} \).

First assume \( m \equiv 0 \pmod{2}, k \equiv 0 \pmod{2} \) and so we set \( m = 2i \ (i \in \mathbb{Z}) \) and \( k = 2j \ (j \in \mathbb{Z}) \) and find that

\[
f = \frac{f_1}{2}
\]

where \( f_1 \) is a polynomial in terms of \( i \) and \( j \) with integral coefficients such that

\[
f_1 \equiv 1 \pmod{2}.
\]

Since \( f \in \mathbb{Z} \), we require \( f_1 \equiv 0 \pmod{2} \). Thus, \( \lambda \) is not algebraic integer, a contradiction.

So we must have \( m \equiv 1 \pmod{2}, k \equiv 1 \pmod{2} \). Hence, we set \( m = 2n + 1 \ (n \in \mathbb{Z}) \) and \( k = 2l + 1 \ (l \in \mathbb{Z}) \) and find that every coefficient of \( x^6 + cx^5 + dx^4 + ex^3 + fx^2 + gx + h \)
is an integer. Hence,

\[
\begin{aligned}
    a &= 4n + 3 \\
    b &= 4l + 3
\end{aligned}
\]

and so \((a, b) \equiv (3, 3) \pmod{4}\), which completes the proof for this case.

**Case** \((0, 1, 0, 0, 0)\): \(\lambda = \frac{\theta + \phi}{2}\)

First assume \((a, b) \equiv (1, 1) \pmod{4}\). We set \(a = 4u + 1\) and \(b = 4v + 1\) \((u, v \in \mathbb{Z})\). Then, by MAPLE\textsuperscript{TM}, \(\lambda\) satisfies the polynomial

\[
x^6 + (1 - 6v + 6u + 80v^2u + 20v^2 - 240vu^2 - 320vu^3 - 44vu + 24u^2 \\
+ 112u^3 + 256u^5 + 320u^4)x^4 + (128v^3u^2 - 16v^3u + 32v^2u^2 + 16v^4 \\
+ 64v^5 + 64vu^4 + 4v^2u + 4v^2 - 28vu^2 - 32vu^3 - 4u^2 - 12u^3 - 12v^3 + 16u^4)x^2 \\
+ 4v^4 + 8v^2u^2 + 4u^4
\]

which belongs to \(\mathbb{Z}[x]\) and so \(\lambda\) is an algebraic integer. Now assume \((a, b) \equiv (3, 3) \pmod{4}\) and so we set \(a = 4p + 3\) and \(b = 4q + 3\) \((p, q \in \mathbb{Z})\). Then, by MAPLE\textsuperscript{TM}, \(\lambda\) satisfies the polynomial

\[
x^6 + (3 + 112p - 68q + 60q^2 + 80q^2p - 444qp + 632p^2 - 720qp^2 - 320qp^3 \\
+ 960p^4 + 256p^5 + 1232p^3)x^4 + (3 + 8p + 44q + 64qp^4 + 64q^5 + 136q^2 + 204q^2p \\
+ 100qp + 36p^2 + 148qp^2 + 96qp^3 + 176q^4 + 48p^4 + 204q^3 + 128q^3p^2 + 112q^3p \\
+ 224q^3p^2 + 68p^3)x^2 + 1 + 4q + 8qp + 8p^3 + 4p + 4q^4 + 4p^4 + 8p^2 + 8qp^2 + 8q^2p^2 \\
+ 8q^2p + 8q^3 + 8q^2
\]

which belongs to \(\mathbb{Z}[x]\) and so \(\lambda\) is an algebraic integer.

Now we prove the converse. Assume \(\lambda\) is an algebraic integer. We begin first by using MAPLE\textsuperscript{TM} to determine the sextic polynomial

\[
x^6 + cx^5 + dx^4 + ex^3 + fx^2 + gx + h
\]
satisfied by $\lambda$ where $c, d, e, f, g, h \in \mathbb{Z}$. Note that both this sextic polynomial as well as

$$f(x) = x^6 + ax^4 + bx^2 + 1$$

have $\theta$ as a root. Using MAPLE\textsuperscript{TM}, we compute the remainder of this division and set each of its coefficients equal to zero. We find

$$h = \frac{h_1}{64}$$

where $h_1$ is a polynomial in terms of $a$ and $b$ with integral coefficients such that

$$h_1 \equiv a^4 + b^4 \pmod{2}.$$ 

This implies either $a \equiv 0 \pmod{2}, b \equiv 0 \pmod{2}$ or $a \equiv 1 \pmod{2}, b \equiv 1 \pmod{2}$.

First assume $a \equiv 0 \pmod{2}, b \equiv 0 \pmod{2}$ and so we set $a = 2k$ ($k \in \mathbb{Z}$) and $b = 2j$ ($j \in \mathbb{Z}$) and find that

$$f = \frac{f_1}{16}$$

where $f_1$ is a polynomial in terms of $j$ and $k$ with integral coefficients such that

$$f_1 \equiv 1 \pmod{2}.$$ 

Since $f \in \mathbb{Z}$, we require $f_1 \equiv 0 \pmod{2}$. Thus, $\lambda$ is not algebraic integer, a contradiction.

So we must have $a \equiv 1 \pmod{2}, b \equiv 1 \pmod{2}$. Hence, we set $a = 2m + 1$ ($m \in \mathbb{Z}$) and $b = 2n + 1$ ($n \in \mathbb{Z}$) and find that

$$h = \frac{h_2}{4}$$
where \( h_2 \) is a polynomial in terms of \( m \) and \( n \) with integral coefficients such that

\[
h_2 \equiv n^4 + m^4 \pmod{2}.
\]

This implies either \( m \equiv 0 \pmod{2}, n \equiv 0 \pmod{2} \) or \( m \equiv 1 \pmod{2}, n \equiv 1 \pmod{2} \).

First assume \( m \equiv 0 \pmod{2}, n \equiv 0 \pmod{2} \) and so we set \( m = 2u \) \((u \in \mathbb{Z})\) and \( n = 2v \) \((v \in \mathbb{Z})\) and find that every coefficient of \( x^6 + cx^5 + dx^4 + ex^3 + fx^2 + gx + h \) is an integer. Hence,

\[
\begin{aligned}
a &= 4u + 1 \\
b &= 4v + 1
\end{aligned}
\]

and so \((a, b) \equiv (1, 1) \pmod{4}\).

Now assume \( m \equiv 1 \pmod{2}, n \equiv 1 \pmod{2} \) and so we set \( m = 2p + 1 \) \((p \in \mathbb{Z})\) and \( n = 2q + 1 \) \((q \in \mathbb{Z})\) and find that every coefficient of \( x^6 + cx^5 + dx^4 + ex^3 + fx^2 + gx + h \) is an integer. Hence,

\[
\begin{aligned}
a &= 4p + 3 \\
b &= 4q + 3
\end{aligned}
\]

and so \((a, b) \equiv (3, 3) \pmod{4}\), which completes the proof for this case.

**Case** \((0, 1, 1, 0, 1)\) : \( \lambda = \frac{\theta + \theta^2 + \theta^4 + \theta^5}{2} \)

First assume \((a, b) \equiv (2, 2) \pmod{4}\). We set \( a = 4m + 2 \) and \( b = 4l + 2 \) \((l, m \in \mathbb{Z})\).
Then, by MAPLE\textsuperscript{\textregistered}, $\lambda$ satisfies the polynomial

$$x^6 + (-16m^2 - 12m + 2 + 8l)x^5 + (2 - 7m - 3l - 320lm^3 - 544lm^2$$
$$-240lm + 64l^2 + 80l^2m + 168m^2 + 608m^3 + 704m^4 + 256m^5)x^4$$
$$+ (2 + 9m - 19l + 320lm^3 - 320lm^2 - 324lm + 84l^2 - 272l^2m + 228m^2$$
$$+ 496m^3 + 256lm^4 - 256l^2m^3 - 704l^2m^2 + 192l^3m + 160l^3)x^3$$
$$+ (1 + m - 11l + 144lm^3 - 28lm^2 - 153lm + 65l^2 - 140l^2m + 89m^2$$
$$+ 148m^3 + 64m^4 + 64lm^4 + 64l^2m^3 - 16l^2m^2 + 64l^4m + 188l^3 + 208l^4 + 64l^5)x^2$$
$$+ (-3m - 3l - 44lm^2 - 52lm + 28l^2 + 4l^2m + 28m^2 + 64m^3 + 32m^4 + 16l^3m$$
$$+ 40l^3 + 16l^4)x + 9l^2 + 9m^2 + 4l^3m + 4lm^3 - 9lm + 12m^3 + 4l^4 + 4m^4 + 12l^3$$

which belongs to $\mathbb{Z}[x]$ and so $\lambda$ is an algebraic integer. Now assume $(a, b) \equiv (3, 3)$ (mod 8) and so we set $a = 8u + 3$ and $b = 8v + 3$ ($u, v \in \mathbb{Z}$). Then, by MAPLE\textsuperscript{\textregistered}, $\lambda$ satisfies the polynomial

$$x^6 + (-64u^2 - 40u + 16v)x^5 + (3 - 120v - 5120vu^3 - 6272vu^2 - 2128vu$$
$$+ 640v^2u + 204u + 16384u^4 + 8192u^5 + 2928u^2 + 336v^2 + 11136u^3)x^4$$
$$+ (-182v + 7168vu^3 - 3456vu^2 - 2832vu - 4224v^2u + 182u + 5120u^4$$
$$+ 2576u^2 + 8192vu^4 - 8192v^2u^3 - 14336v^2u^2 + 3072v^3u + 496v^2$$
$$+ 1664v^3 + 7040u^3)x^3 + (3 + 34v + 3840vu^3 + 960vu^2 - 800vu - 896v^2u$$
$$+ 70u + 1280u^4 + 1008u^2 + 2048vu^4 + 2048v^2u^3 + 512v^2u^2 + 1024v^3u$$
$$+ 2048v^4u + 1060v^2 + 3616v^3 + 4864v^4 + 2144u^3 + 2048v^5)x^2$$
$$+ (10v - 352vu^2 - 276vu + 128v^2u + 14u + 512u^4 + 308u^2 + 256v^3u + 272v^2$$
$$+ 480v^3 + 256v^4 + 768u^3)x + 1 + 64u^4 + 81v^2 + 10u + 10v + 136u^3 + 64vu^3$$
$$+ 24vu^2 + 64v^4 + 24v^2u + 81u^2 - 30vu + 136v^3 + 64v^3u$$

which belongs to $\mathbb{Z}[x]$ and so $\lambda$ is an algebraic integer. Now assume $(a, b) \equiv (7, 7)$
(mod 8) and so we set \( a = 8z + 7 \) and \( b = 8w + 7 \) (\( w, z \in \mathbb{Z} \)). Then, by MAPLE\textsuperscript{TM}, \( \lambda \) satisfies the polynomial

\[
x^6 + (-64z^2 - 104z - 28 + 16w)x^5 + (1977 - 2736w + 656w^2 + 16276z
\]
\[
+ 61824z^3 + 640w^2z - 5120wz^3 - 13952wz^2 - 11600wz + 47472z^2 + 36864z^4
\]
\[
+ 8192z^5)x^4 + (252 - 4878w - 1424w^2 + 3200w^3 + 6398z + 27008z^3
\]
\[
+ 3072w^3z - 20096w^2z + 15360wz^3 - 7040wz^2 - 19216wz + 23952z^2
\]
\[
+ 9216z^4 - 26624w^2z^2 - 8192w^2z^3 + 8192wz^4)x^3 + (2076 + 8158w
\]
\[
+ 18580w^2 + 21024w^3 + 11008w^4 + 2048w^5 + 5902z + 9184z^3
\]
\[
+ 2048w^4z + 5120w^3z + 5760w^2z + 9984wz^3 + 13376wz^2 + 7008wz
\]
\[
+ 11936z^2 + 2304z^4 + 3584w^2z^2 + 2048w^2z^3 + 2048wz^4)x^2
\]
\[
+(280 + 704w + 1632w^2 + 1120w^3 + 256w^4 + 904z + 1792z^3 + 256w^3z
\]
\[
+ 512w^2z - 352wz^2 - 308wz + 2052z^2 + 512z^4)x + 100 + 120w^2z
\]
\[
+ 296w^3 + 64w^4 + 441w^2 + 296z^3 + 260w + 64z^4 + 441z^2 + 114wz + 260z
\]
\[
+ 120w^2 + 64w^3z + 64wz^3
\]

which belongs to \( \mathbb{Z}[x] \) and so \( \lambda \) is an algebraic integer.

Now we prove the converse. Assume \( \lambda \) is an algebraic integer. We begin first by using MAPLE\textsuperscript{TM} to determine the sextic polynomial

\[
x^6 + cx^5 + dx^4 + ex^3 + fx^2 + gx + h
\]

satisfied by \( \lambda \) where \( c, d, e, f, g, h \in \mathbb{Z} \). Note that both this sextic polynomial as well as

\[
f(x) = x^6 + ax^4 + bx^2 + 1
\]

have \( \theta \) as a root. Using MAPLE\textsuperscript{TM}, we compute the remainder of this division and
set each of its coefficients equal to zero. We find

$$e = \frac{e_1}{4}$$

where \( e_1 \) is a polynomial in terms of \( a \) and \( b \) with integral coefficients such that

$$e_1 \equiv b a^4 + ba^3 + b^2 a^3 + a^3 + b^2 a^2 + a^2 + ba + b^2 a + a + b^3 a + b^2 + b \pmod{2}$$

This implies either \( a \equiv 0 \pmod{2} \) or \( b \equiv 1 \pmod{2} \).

First assume \( a \equiv 0 \pmod{2} \) and so we set \( a = 2k \ (k \in \mathbb{Z}) \) and find that

$$d = \frac{d_1}{4}$$

where \( d_1 \) is a polynomial in terms of \( b \) and \( k \) with integral coefficients such that

$$d_1 \equiv b \pmod{2}.$$ 

This implies \( b \equiv 0 \pmod{2} \) and so we set \( b = 2j \ (j \in \mathbb{Z}) \) and find that

$$f = \frac{f_1}{4}$$

where \( f_1 \) is a polynomial in terms of \( j \) and \( k \) with integral coefficients such that

$$f_1 \equiv k^2 + k + jk + 1 + j + j^2 \pmod{2}$$

$$\equiv jk + 1 \pmod{2}.$$ 

This implies \( j \equiv 1 \pmod{2}, k \equiv 1 \pmod{2} \) and so we set \( j = 2l + 1 \ (l \in \mathbb{Z}) \) and \( k = 2m + 1 \ (m \in \mathbb{Z}) \) and find that every coefficient of \( x^6 + cx^5 + dx^4 + ex^3 + fx^2 + gx + h \)
is an integer. Hence,

\[
\begin{align*}
  a &= 4m + 2 \\
  b &= 4l + 2
\end{align*}
\]

and so \((a, b) \equiv (2, 2) \pmod{4}\).

Now we assume \(b \equiv 1 \pmod{2}\) and so we set \(b = 2p + 1 \ (p \in \mathbb{Z})\) and find that

\[
g = \frac{g_1}{16}
\]

where \(g_1\) is a polynomial in terms of \(a\) and \(p\) with integral coefficients such that

\[
g_1 \equiv 1 + a^2 \pmod{2}.
\]

This implies \(a \equiv 1 \pmod{2}\) and so we set \(a = 2q + 1 \ (q \in \mathbb{Z})\) and find that

\[
f = \frac{f_2}{4}
\]

where \(f_2\) is a polynomial in terms of \(p\) and \(q\) with integral coefficients such that

\[
f_2 \equiv 1 + p^2 \pmod{2}.
\]

This implies \(p \equiv 1 \pmod{2}\) and so we set \(p = 2r + 1 \ (r \in \mathbb{Z})\) and find that

\[
e = \frac{e_2}{2}
\]

where \(e_2\) is a polynomial in terms of \(q\) and \(r\) with integral coefficients such that

\[
e_2 \equiv 1 + q \pmod{2}.
\]
This implies \( q \equiv 1 \pmod{2} \) and so we set \( q = 2s + 1 \ (s \in \mathbb{Z}) \) and find that
\[
h = \frac{h_1}{4}
\]
where \( h_1 \) is a polynomial in terms of \( r \) and \( s \) with integral coefficients such that
\[
h_1 \equiv r^2 + s^2 \pmod{2}.
\]
This implies either \( r \equiv 0 \pmod{2}, s \equiv 0 \pmod{2} \) or \( r \equiv 1 \pmod{2}, s \equiv 1 \pmod{2} \).

First assume \( r \equiv 0 \pmod{2}, s \equiv 0 \pmod{2} \) and so we set \( r = 2v \) (\( v \in \mathbb{Z} \)) and \( s = 2u \) (\( u \in \mathbb{Z} \)) and find that every coefficient of \( x^6 + cx^5 + dx^4 + ex^3 + fx^2 + gx + h \) is an integer. Hence,
\[
\begin{aligned}
a &= 8u + 3 \\
b &= 8v + 3
\end{aligned}
\]
and so \((a, b) \equiv (3, 3) \pmod{8} \).

Now assume \( r \equiv 1 \pmod{2}, s \equiv 1 \pmod{2} \) and so we set \( r = 2w + 1 \) (\( w \in \mathbb{Z} \)) and \( s = 2z + 1 \) (\( z \in \mathbb{Z} \)) and find that every coefficient of \( x^6 + cx^5 + dx^4 + ex^3 + fx^2 + gx + h \) is an integer. Hence,
\[
\begin{aligned}
a &= 8z + 7 \\
b &= 8w + 7
\end{aligned}
\]
and so \((a, b) \equiv (7, 7) \pmod{8} \), which completes the proof for this case.

**Case** \((1, 0, 0, 1, 1)\):
\[
\lambda = \frac{1+\varphi^2+\varphi^3+\varphi^5}{2}
\]
First assume \((a, b) \equiv (3, 3) \pmod{8} \). We set \( a = 8s + 3 \) and \( b = 8r + 3 \) (\( r, s \in \mathbb{Z} \)).
Then, by MAPLE\textsuperscript{TM}, $\lambda$ satisfies the polynomial

\[
x^6 + (-64s^2 - 48s - 6 + 16r)x^5 + (15 - 62r + 210s + 640sr^2 - 5120s^3r + 8192s^3
-1344sr - 5248s^2r + 14336s^4 + 8192s^5 + 1872s^2 + 272r^2)x^4
+(15 - 64r + 312s - 896sr^2 + 2816r^4 + 2048r^5 + 15616s^2r^2 - 7680sr^3 + 12288s^3r^2
+2048s^2r^3 - 2048sr^4 + 768s^3r + 9568s^3 - 52sr + 3520s^2r + 18432s^4 + 12288s^5
-224r^3 + 2700s^2 - 372r^2)x^2 + (-6 + 20r - 132s + 1088sr^2 - 2816r^4 - 2048r^5
-9472s^2r^2 + 5376sr^3 - 6144s^3r^2 - 2048s^2r^3 + 2048sr^4 - 1280s^3r - 2624s^5
-280sr - 3616s^2r - 5632s^4 - 4096s^5 - 480r^3 - 972s^2 + 156r^2)x - 2r + 256s^3r
+66sr + 808s^2r + 1856s^2r^2 - 1152sr^3 + 1024s^3r^2 - 280sr^2 + 512s^2r^3 - 512sr^4
+22s + 1 + 141s^2 + 248s^3 + 640s^4 + 512s^5 - 11r^2 + 184r^3 + 704r^4 + 512r^5
\]

which belongs to $\mathbb{Z}[x]$ and so $\lambda$ is an algebraic integer. Now assume $(a, b) \equiv (7, 7) \pmod{8}$ and so we set $a = 8v + 7$ and $b = 8u + 7 \ (u, v \in \mathbb{Z})$. Then, by MAPLE\textsuperscript{TM},
\( \lambda \) satisfies the polynomial

\[
x^6 + (-64v^2 - 112v - 38 + 16u)x^5 + (1569 - 2094u + 12898v + 54784v^3 + 39440v^2
+ 8192v^5 + 592u^2 + 640vu^2 - 9792vu - 5120v^3u - 12928v^2u + 34816v^4)x^4
+ (-4540 + 692u - 32740v - 20480v^2u^2 + 3072vu^3 - 8192v^3u^2 - 108928v^3u
- 16384v^5 + 2432u^3 + 336u^2 - 10368vu^2 - 4656vu - 4096v^3u - 10752v^2u
- 67584v^4)x^3
+ (4908 + 4378u + 30418v + 37120v^2u^2 - 9728vu^3 + 12288v^3u^2 + 2048v^2u^3 - 2048vu^4
+ 80608v^3 + 71164v^2 + 12288v^5 + 5152u^3 + 6912u^4 + 2048u^5 + 4540u^2 + 12416vu^2
+ 22732vu + 13056v^3u + 40256v^2u + 49152v^4)x^2 + (-2288 - 3884u - 12300v
- 21760v^2u^2 + 7424vu^3 - 6144v^3u^2 - 2048v^2u^3 + 2048vu^4 - 26304v^3 - 26172v^2
- 4096v^5 - 7008u^3 - 6912u^4 - 2048u^5 - 5140u^2 - 4928vu^2 - 14328vu - 7424v^3u
- 25760v^2u - 15872v^4)x + 892u + 1836v + 388 - 1664vu^3 + 1024v^3u^2 + 512v^2u^3
+ 4160v^2u^2 + 1728u^4 + 512u^5 + 1357u^2 + 616vu^2 + 2674vu + 1280v^3u + 4968v^2u
+ 1920v^4 + 512vu^4 + 3192v^3 + 3621v^2 + 512v^5 + 1912u^3
\]

which belongs to \( \mathbb{Z}[x] \) and so \( \lambda \) is an algebraic integer.

Now we prove the converse. Assume \( \lambda \) is an algebraic integer. We begin first by using MAPLE\textsuperscript{TM} to determine the sextic polynomial

\[
x^6 + cx^5 + dx^4 + ex^3 + fx^2 + gx + h
\]

satisfied by \( \lambda \) where \( c, d, e, f, g, h \in \mathbb{Z} \). Note that both this sextic polynomial as well as

\[
f(x) = x^6 + ax^4 + bx^2 + 1
\]

have \( \theta \) as a root. Using MAPLE\textsuperscript{TM}, we compute the remainder of this division and
set each of its coefficients equal to zero. We find

\[ e = \frac{e_1}{4} \]

where \( e_1 \) is a polynomial in terms of \( a \) and \( b \) with integral coefficients such that

\[ e_1 \equiv b^2a^3 + b^2a^2 + b^3a + b^2a + a + b^2 + b + 1 \quad (\text{mod } 2) \]
\[ \equiv a + 1 \quad (\text{mod } 2). \]

This implies \( a \equiv 1 \pmod{2} \) and so we set \( a = 2k + 1 \ (k \in \mathbb{Z}) \) and find that

\[ d = \frac{d_1}{4} \]

where \( d_1 \) is a polynomial in terms of \( b \) and \( k \) with integral coefficients such that

\[ d_1 \equiv b + b^2 \quad (\text{mod } 2). \]

This implies \( b \equiv 0 \pmod{2} \) or \( b \equiv 1 \pmod{2} \).

First assume \( b \equiv 0 \pmod{2} \) and so we set \( b = 2j \ (j \in \mathbb{Z}) \) and find that

\[ d = \frac{d_2}{2} \]

where \( d_2 \) is a polynomial in terms of \( j \) and \( k \) with integral coefficients such that

\[ d_2 \equiv 1 + j \quad (\text{mod } 2). \]

This implies \( j \equiv 1 \pmod{2} \) and so we set \( j = 2m + 1 \ (m \in \mathbb{Z}) \) and find that

\[ g = \frac{g_1}{4} \]
where $g_1$ is a polynomial in terms of $k$ and $m$ with integral coefficients such that

\[ g_1 \equiv 1 \pmod{2}. \]

Since $g \in \mathbb{Z}$, we require $g_1 \equiv 0 \pmod{2}$. Thus, $\lambda$ is not algebraic integer, a contradiction.

So we must have $b \equiv 1 \pmod{2}$ and so we set $b = 2l + 1 \ (l \in \mathbb{Z})$ and find that

\[ f = \frac{f_1}{4} \]

where $f_1$ is a polynomial in terms of $l$ and $k$ with integral coefficients such that

\[
\begin{align*}
    f_1 & \equiv l + k + 1 + kl + l^2 + k^2 \pmod{2} \\
    & \equiv 1 + kl \pmod{2}.
\end{align*}
\]

This implies $k \equiv 1 \pmod{2}, l \equiv 1 \pmod{2}$ and so we set $k = 2p + 1 \ (p \in \mathbb{Z})$ and $l = 2q + 1 \ (q \in \mathbb{Z})$ and find that

\[ h = \frac{h_1}{4} \]

where $h_1$ is a polynomial in terms of $p$ and $q$ with integral coefficients such that

\[ h_1 \equiv p^2 + q^2 \pmod{2}. \]

This implies either $p \equiv 0 \pmod{2}, q \equiv 0 \pmod{2}$ or $p \equiv 1 \pmod{2}, q \equiv 1 \pmod{2}$.

First assume $p \equiv 0 \pmod{2}, q \equiv 0 \pmod{2}$ and so we set $p = 2s \ (s \in \mathbb{Z})$ and $q = 2r \ (r \in \mathbb{Z})$ and find that every coefficient of $x^6 + cx^5 + dx^4 + ex^3 + fx^2 + gx + h$ is an integer. Hence,

\[
\begin{cases}
    a = 8s + 3 \\
    b = 8r + 3
\end{cases}
\]

and so $(a, b) \equiv (3, 3) \pmod{8}$. 103
Now assume $p \equiv 1 \pmod{2}, q \equiv 1 \pmod{2}$ and so we set $p = 2v + 1$ ($v \in \mathbb{Z}$) and $q = 2u + 1$ ($u \in \mathbb{Z}$) and find that every coefficient of $x^6 + cx^5 + dx^4 + ex^3 + fx^2 + gx + h$ is an integer. Hence,

$$\begin{align*}
& a = 8v + 7 \\
& b = 8u + 7
\end{align*}$$

and so $(a, b) \equiv (7, 7) \pmod{8}$, which completes the proof for this case.

**Case** $(1, 0, 1, 1, 0)$: $\lambda = \frac{1 + \theta^2 + \theta^3 + \theta^5}{2}$

First assume $(a, b) \equiv (2, 2) \pmod{4}$. We set $a = 4l + 2$ and $b = 4m + 2$ ($l, m \in \mathbb{Z}$). Then, by MAPLE\textsuperscript{TM}, $\lambda$ satisfies the polynomial

\[
x^6 + (-1 + 4l)x^5 + (1 + 7m - 8l + 240l^3 + 512l^4 - 320ml^3 - 352ml^2 - 44ml \\
+ 80m^2l + 24m^2 + 256l^5)x^4 + (-4m + l + 32m^3 - 304l^3 - 896l^4 + 24l^2 + 1024ml^3 \\
+ 656ml^2 + 8ml - 320m^2l + 256ml^4 - 256m^2l^2 - 24m^2 - 512l^5)x^3 \\
+ (-128m^4l + 12m^3 + 128m^4 + 64m^2l^3 + 64m^3l^2 + 64m^5 + 120l^3 + 608l^4 - 352m^3l \\
- l^2 - 1040ml^3 - 284ml^2 - 7ml + 132m^2l - 384ml^4 + 672m^2l^2 + 11m^2 + 384l^5)x^2 \\
+ (128m^4l - 12m^3 - 112m^4 - 64m^2l^3 - 64m^3l^2 - 64m^5 - 12l^3 - 192l^4 + 320m^3l \\
+ 448ml^3 + 24ml^2 + 192ml^4 - 464m^2l^2 - 128l^5)x - 72ml^3 - 32ml^4 + 16m^5 \\
- 32m^4l + 24m^4 + 16l^5 + 16m^2l^3 + 16m^3l^2 + 24l^4 - 72m^3l + 96m^2l^2
\]

which belongs to $\mathbb{Z}[x]$ and so $\lambda$ is an algebraic integer. Now assume $(a, b) \equiv (3, 3) \pmod{4}$ and so we set $a = 4u + 3$ and $b = 4v + 3$ ($u, v \in \mathbb{Z}$). Then, by MAPLE\textsuperscript{TM},
\[ x^6 + 4ux^5 + (\text{polynomial of degree 6}) = 0 \]

which belongs to \( \mathbb{Z}[x] \) and so \( \lambda \) is an algebraic integer.

Now we prove the converse. Assume \( \lambda \) is an algebraic integer. We begin first by using MAPLE\textsuperscript{TM} to determine the sextic polynomial

\[ x^6 + cx^5 + dx^4 + ex^3 + fx^2 + gx + h \]

satisfied by \( \lambda \) where \( c, d, e, f, g, h \in \mathbb{Z} \). Note that both this sextic polynomial as well as

\[ f(x) = x^6 + ax^4 + bx^2 + 1 \]

have \( \theta \) as a root. Using MAPLE\textsuperscript{TM}, we compute the remainder of this division and set each of its coefficients equal to zero. We find

\[ d = \frac{d_1}{4} \]
where \(d_1\) is a polynomial in terms of \(a\) and \(b\) with integral coefficients such that

\[
d_1 \equiv a^5 + a^3 + ba^3 + b^2a + ba + b \pmod{2}
\]

\[
\equiv ba + b \pmod{2}.
\]

This implies either \(b \equiv 0 \pmod{2}\) or \(a \equiv 1 \pmod{2}\).

First we assume \(b \equiv 0 \pmod{2}\) and so we set \(b = 2k \ (k \in \mathbb{Z})\) and find that

\[
f = \frac{f_1}{16}
\]

where \(f_1\) is a polynomial in terms of \(a\) and \(k\) with integral coefficients such that

\[
f_1 \equiv a^2 \pmod{2}.
\]

This implies \(a \equiv 0 \pmod{2}\) and so we set \(a = 2j \ (j \in \mathbb{Z})\) and find that

\[
d = \frac{d_2}{2}
\]

where \(d_2\) is a polynomial in terms of \(j\) and \(k\) with integral coefficients such that

\[
d_2 \equiv k + 1 \pmod{2}.
\]

This implies \(k \equiv 1 \pmod{2}\) and so we set \(k = 2m + 1 \ (m \in \mathbb{Z})\) and find that

\[
f = \frac{f_2}{4}
\]

where \(f_2\) is a polynomial in terms of \(j\) and \(m\) with integral coefficients such that

\[
f_2 \equiv j^2 + 1 \pmod{2}.
\]
This implies $j \equiv 1 \pmod{2}$ and so we set $j = 2l + 1 \ (l \in \mathbb{Z})$ and find that every coefficient of $x^6 + cx^5 + dx^4 + ex^3 + fx^2 + gx + h$ is an integer. Hence,

$$\begin{cases} 
    a = 4l + 2 \\
    b = 4m + 2
\end{cases}$$

and so $(a, b) \equiv (2, 2) \pmod{4}$.

Now we assume $a \equiv 1 \pmod{2}$ and so we set $a = 2p + 1 \ (p \in \mathbb{Z})$ and find that

$$f = \frac{f_3}{16}$$

where $f_3$ is a polynomial in terms of $b$ and $p$ with integral coefficients such that

$$f_3 \equiv b + 1 + b^2 + b^5 \pmod{2}$$

$$\equiv b + 1 \pmod{2}.$$ 

This implies $b \equiv 1 \pmod{2}$ and so we set $b = 2q + 1 \ (q \in \mathbb{Z})$ and find that

$$d = \frac{d_3}{2}$$

where $d_3$ is a polynomial in terms of $p$ and $q$ with integral coefficients such that

$$d_3 \equiv p + q \pmod{2}.$$ 

This implies either $p \equiv 0 \pmod{2}, q \equiv 0 \pmod{2}$ or $p \equiv 1 \pmod{2}, q \equiv 1 \pmod{2}$.

First assume $p \equiv 0 \pmod{2}, q \equiv 0 \pmod{2}$ and so we set $p = 2r \ (r \in \mathbb{Z})$ and $q = 2s \ (s \in \mathbb{Z})$ and find that

$$f = \frac{f_4}{2}$$
where \( f_4 \) is a polynomial in terms of \( r \) and \( s \) with integral coefficients such that

\[ f_4 \equiv 1 \pmod{2}. \]

Since \( f \in \mathbb{Z} \), we require \( f_4 \equiv 0 \pmod{2} \). Thus, \( \lambda \) is not algebraic integer, a contradiction.

Hence, we must have \( p \equiv 1 \pmod{2} \), \( q \equiv 1 \pmod{2} \) and so we set \( p = 2u + 1 \) \((u \in \mathbb{Z})\) and \( q = 2v + 1 \) \((v \in \mathbb{Z})\) and find that every coefficient of \( x^6 + cx^5 + dx^4 + ex^3 + fx^2 + gx + h \) is an integer. Hence,

\[
\begin{align*}
a &= 4u + 3 \\
b &= 4v + 3
\end{align*}
\]

and so \((a, b) \equiv (3, 3) \pmod{4}\), which completes the proof for this case.

**Case** \((1, 1, 0, 0, 1)\) : \( \lambda = \frac{1 + \theta + \theta^3 + \theta^5}{2} \)

First assume \((a, b) \equiv (1, 1) \pmod{4}\). We set \( a = 4n + 1 \) and \( b = 4m + 1 \) \((l, m \in \mathbb{Z})\).

Then, by MAPLE\textsuperscript{TM}, \( \lambda \) satisfies the polynomial

\[
x^6 + (-16n^2 - 8n - 2 + 8m)x^5 + (2 - 18m + 18n + 72n^2 - 304mn^2 - 76mn + 176n^3 + 384n^4 + 256n^5 - 320mn^3 + 80m^2n + 44m^2)x^4 + (8m - 8n - 56n^2 + 384mn^2 + 64mn - 208n^3 - 640n^4 - 512n^5 + 512mn^3 - 256m^2n^2 - 128m^2n - 256m^2n^3 + 192m^3n + 80m^3 - 56m^2)x^3 + (8n^2 - 192mn^2 - 16mn + 64n^3 + 400n^4 + 384n^5 - 304mn^3 + 352m^2n^2 + 64m^2n + 384m^2n^3 - 208m^3n + 128m^3n^2 + 64mn^4 + 64m^4n - 96m^3 + 48m^4 + 64m^5 + 24m^2)x^2 + (32mn^2 - 112n^4 - 128n^5 + 64mn^3 - 160m^2n^2 - 192m^2n^3 + 64m^3n - 128m^3n^2 - 64mn^4 - 64m^4n + 32m^3 - 48m^4 - 64m^5)x + 16m^4n + 32m^2n^3 + 16n^4 + 16n^5 + 32m^2n^2 + 16m^4 + 16m^5 + 32m^3n^2 + 16mn^4
\]

which belongs to \( \mathbb{Z}[x] \) and so \( \lambda \) is an algebraic integer. Now assume \((a, b) \equiv (3, 3) \pmod{4}\) and so we set \( a = 4p + 3 \) and \( b = 4l + 3 \) \((l, p \in \mathbb{Z})\). Then, by MAPLE\textsuperscript{TM}, \( \lambda \)

108
satisfies the polynomial

\[ x^6 + (-16p^2 - 24p - 6 + 8l)x^5 + (18 + 204p - 88l + 1024p^4 + 1424p^3 \\
+ 84l^2 + 256p^5 - 320lp^2 - 784lp^2 - 540lp + 80l^2p + 840p^2)x^4 \\
+ (-32 - 404p + 116l - 1920p^4 - 2576p^3 + 48l^2 - 512p^5 + 176l^3 \\
+ 192l^3p + 256lp^3 + 512lp^2 + 400lp - 640l^2p^2 - 288lp^2 - 256lp^3 - 1552p^2)x^3 \\
+ (36 + 344p + 36l + 1392p^4 + 1832p^3 + 140l^2 + 384p^5 + 64l^4p + 240l^4 + 152l^3 \\
+ 64l^5 + 128l^3p^2 + 48l^3p + 64l^4p^2 + 208lp^3 + 272lp^2 + 1120l^2p^2 + 680l^2p \\
+ 384l^2lp^3 + 1156lp^2)p^2 + (-24 - 160p - 88l - 464p^4 - 624p^3 - 216l^2 - 128p^5 \\
- 64l^4p - 240l^4 - 288l^3 - 64l^5 - 128l^3p^2 - 192l^3p - 64l^4p - 256lp^3 - 512lp^2 \\
- 336lp - 640l^2p^2 - 496l^2p - 192l^2p^3 - 440p^2)x + 36p + 36l + 8 + 64p^4 + 96p^3 + 80l^2 \\
+ 16p^5 + 16l^4p + 64l^4 + 96l^3 + 16l^5 + 32l^3p^2 + 64l^3p + 16lp^4 \\
+ 64lp^3 + 128lp^2 + 96lp + 128l^2p^2 + 128l^2p + 32l^2p^3 + 80p^2 \]

which belongs to \( \mathbb{Z}[x] \) and so \( \lambda \) is an algebraic integer.

Now we prove the converse. Assume \( \lambda \) is an algebraic integer. We begin first by using MAPLE\textsuperscript{TM} to determine the sextic polynomial

\[ x^6 + cx^5 + dx^4 + ex^3 + fx^2 + gx + h \]

satisfied by \( \lambda \) where \( c, d, e, f, g, h \in \mathbb{Z} \). Note that both this sextic polynomial as well as

\[ f(x) = x^6 + ax^4 + bx^2 + 1 \]

have \( \theta \) as a root. Using MAPLE\textsuperscript{TM}, we compute the remainder of this division and set each of its coefficients equal to zero. We find

\[ d = \frac{d_1}{4} \]
where  is a polynomial in terms of and  with integral coefficients such that

\[
d_1 \equiv a^5 + a^4 + ba^3 + a^2 + b^2a + a + b + 1 \pmod{2} \\
\equiv b + 1 \pmod{2}.
\]

This implies  and so we set  and find that

\[
e = \frac{e_1}{4}
\]

where  is a polynomial in terms of  and  with integral coefficients such that

\[
e_1 \equiv a + 1 + a^2 + a^3 \pmod{2} \\
\equiv a + 1 \pmod{2}.
\]

This implies  and so we set  and find that

\[
h = \frac{h_1}{2}
\]

where  is a polynomial in terms of  and  with integral coefficients such that

\[
h_1 \equiv j^5 + k^5 + k^4j + kj^4 \pmod{2} \\
\equiv j^5 + k^5 \pmod{2}.
\]

This implies either  or  or  and  and so we set  and  and find that every coefficient of  is an integer. Hence,

\[
\begin{aligned}
a &= 4n + 1 \\
b &= 4m + 1
\end{aligned}
\]
and so \((a, b) \equiv (1, 1) \pmod{4}\).

Now we assume \(j \equiv 1 \pmod{2}, k \equiv 1 \pmod{2}\) and so we set \(j = 2p + 1 \ (p \in \mathbb{Z})\) and \(k = 2l + 1 \ (l \in \mathbb{Z})\) and find that every coefficient of \(x^6 + cx^5 + dx^4 + ex^3 + fx^2 + gx + h\) is an integer. Hence,

\[
\begin{aligned}
a &= 4p + 3 \\
b &= 4l + 3
\end{aligned}
\]

and so \((a, b) \equiv (3, 3) \pmod{4}\), which completes the proof for this case.

**Case** \((1, 1, 1, 0, 0)\) : \(\lambda = \frac{1+\theta+\theta^2+\theta^5}{2}\)

First assume \((a, b) \equiv (3, 3) \pmod{8}\). We set \(a = 8s + 3\) and \(b = 8t + 3 \ (s, t \in \mathbb{Z})\).

Then, by MAPLE\textsuperscript{TM}, \(\lambda\) satisfies the polynomial

\[
x^6 + 8sx^5 + (3 + 216s - 132t + 2544s^2 - 5760s^2t - 5120s^3t + 9856s^3 + 640st^2 - 1776st + 240t^2 + 8192s^5 + 15360s^4)x^4 + (-174s + 142t - 4096s^2t^2 + 8192s^4t + 22528s^3t + 3296st + 15616s^2t^2 - 3120s^2 - 15232s^3 - 16384s^5 - 27648s^4 - 832t^2 - 4352st^2 + 256t^3)x^3 + (3 + 70s + 34t + 12032s^2t^2 + 1024st^3 - 10240s^4t + 2048s^3t^2 + 4096s^2t^3 - 23040s^3t - 1744st - 12192s^2t + 1660s^2 + 9664s^3 + 12288s^5 + 19712s^4 + 1288t^2 + 7264st^2 + 960t^3 + 2816t^4 + 2048t^5)x^2 + (26s - 66t - 8448s^2t^2 - 1024st^3 + 4096s^4t - 2048s^3t^2 - 4096s^2t^3 + 8960s^3t + 236st + 3776s^2t - 200s^2 - 2432s^3 - 4096s^5 - 6144s^4 - 692t^2 - 4160st^2 - 896t^3 - 2560t^4 - 2048t^5)x + 22t + 808st^2 + 184s^3 - 2s - 11s^2 + 141t^2 - 1152s^3t + 1 + 1856s^2t^2 - 512s^4t + 512s^5 + 704s^4 + 248t^3 + 640t^4 + 512t^5 + 256st^3 + 512s^3t^2 + 1024s^2t^3 - 280s^2t + 66st
\]

which belongs to \(\mathbb{Z}[x]\) and so \(\lambda\) is an algebraic integer. Now assume \((a, b) \equiv (7, 7) \pmod{8}\) and so we set \(a = 8u + 7\) and \(b = 8v + 7 \ (u, v \in \mathbb{Z})\). Then, by MAPLE\textsuperscript{TM},
\[ \lambda \text{ satisfies the polynomial} \]
\[
x^6 + (8u + 4)x^5 + (1785 - 2540v + 14864u + 58496u^3 + 8192u^5 + 43888u^2 - 13440u^2v + 560v^2 + 640uv^2 - 10736uw - 5120u^3v + 35840u^4)x^4
\]
\[ +(-1476 + 5182v - 15822u - 92032u^3 - 4096u^2v^2 - 16384u^5 + 256v^3 - 58096u^2v^2 + 3648v^2 - 8448uv^2 + 8192u^4v + 38912u^3v - 64512u^4)x^3
\]
\[ + (2172 + 4698v + 10354u + 58560u^3 + 21248u^2v^2 + 12288u^5 + 13248v^3 + 34316u^2v^2 + 18712v^2 - 11664uw + 5120u^2v^3 - 10240u^4v - 41472u^3v + 2048u^3v^2 + 7936u^4 + 4096u^2v^3 + 45312u^4)x^2
\]
\[ + (-1480 - 6512v - 4136u - 16896u^3 - 17664u^2v^2 - 4096u^5 - 12672v^3 - 9896u^2 - 8768u^2v - 15188v^2 - 21824uv^2 - 5204uv - 5120uv^3 + 4096u^4v + 15104u^3v - 2048u^3v^2 - 7680v^4 - 2048v^5 - 4096u^2v^3 - 14336u^4)x + 1836v + 892u + 388 + 1912u^3 + 4160u^2v^2 + 512u^5 + 3192v^3 + 1357u^2 + 616u^2v + 3621v^2 + 4968uv^2 + 2674uv + 1280uv^3 - 512u^4v - 1664u^3v + 512u^3v^2 + 1920v^4 + 512v^5 + 1024u^2v^3 + 1728u^4
\]

which belongs to \( \mathbb{Z}[x] \) and so \( \lambda \) is an algebraic integer.

Now we prove the converse. Assume \( \lambda \) is an algebraic integer. We begin first by using MAPLE\textsuperscript{TM} to determine the sextic polynomial
\[
x^6 + cx^5 + dx^4 + ex^3 + fx^2 + gx + h
\]
satisfied by \( \lambda \) where \( c, d, e, f, g, h \in \mathbb{Z} \). Note that both this sextic polynomial as well as
\[
f(x) = x^6 + ax^4 + bx^2 + 1
\]
have \( \theta \) as a root. Using MAPLE\textsuperscript{TM}, we compute the remainder of this division and
set each of its coefficients equal to zero. We find

\[ d = \frac{d_1}{4} \]

where \( d_1 \) is a polynomial in terms of \( a \) and \( b \) with integral coefficients such that

\[ d_1 \equiv a^5 + ba^3 + b^2a + a + b + 1 \pmod{2} \]
\[ \equiv b + 1 \pmod{2}. \]

This implies \( b \equiv 1 \pmod{2} \) and so we set \( b = 2k + 1 \ (k \in \mathbb{Z}) \) and find that

\[ e = \frac{e_1}{4} \]

where \( e_1 \) is a polynomial in terms of \( a \) and \( k \) with integral coefficients such that

\[ e_1 \equiv a^3 + a^4 \pmod{2}. \]

This implies either \( a \equiv 0 \pmod{2} \) or \( a \equiv 1 \pmod{2} \).

First assume \( a \equiv 0 \pmod{2} \) and so we set \( a = 2j \ (j \in \mathbb{Z}) \) and find that

\[ d = \frac{d_2}{2} \]

where \( d_2 \) is a polynomial in terms of \( j \) and \( k \) with integral coefficients such that

\[ d_2 \equiv 1 + k \pmod{2}. \]

This implies \( k \equiv 1 \pmod{2} \) and so we set \( k = 2m + 1 \ (m \in \mathbb{Z}) \) and find that

\[ g = \frac{g_1}{4} \]
where $g_1$ is a polynomial in terms of $j$ and $m$ with integral coefficients such that

$$g_1 \equiv 1 + j \pmod{2}.$$ 

This implies $j \equiv 1 \pmod{2}$ and so we set $j = 2n + 1 \ (n \in \mathbb{Z})$ and find that

$$e = \frac{e_2}{2}$$

where $e_2$ is a polynomial in terms of $m$ and $n$ with integral coefficients such that

$$e_2 \equiv 1 \pmod{2}.$$ 

Since $e \in \mathbb{Z}$, we require $e_2 \equiv 0 \pmod{2}$. Thus, $\lambda$ is not algebraic integer, a contradiction.

Hence, we must have $a \equiv 1 \pmod{2}$ and so we set $a = 2p + 1 \ (p \in \mathbb{Z})$ and find that

$$f = \frac{f_1}{4}$$

where $f_1$ is a polynomial in terms of $k$ and $p$ with integral coefficients such that

$$f_1 \equiv 1 + p^2 \pmod{2}.$$ 

This implies $p \equiv 1 \pmod{2}$ and so we set $p = 2q + 1 \ (q \in \mathbb{Z})$ and find that

$$e = \frac{e_3}{2}$$

where $e_3$ is a polynomial in terms of $k$ and $q$ with integral coefficients such that

$$e_3 \equiv 1 + k \pmod{2}.$$
This implies $k \equiv 1 \pmod{2}$ and so we set $k = 2r + 1 \ (r \in \mathbb{Z})$ and find that
\[ h = \frac{h_1}{4} \]
where $h_1$ is a polynomial in terms of $q$ and $r$ with integral coefficients such that
\[ h_1 \equiv r^2 + q^2 \pmod{2}. \]

This implies either $r \equiv 0 \pmod{2}, q \equiv 0 \pmod{2}$ or $r \equiv 1 \pmod{2}, q \equiv 1 \pmod{2}$.

First assume $r \equiv 0 \pmod{2}, q \equiv 0 \pmod{2}$ and so we set $r = 2t \ (t \in \mathbb{Z})$ and $q = 2s \ (s \in \mathbb{Z})$ and find that every coefficient of $x^6 + cx^5 + dx^4 + ex^3 + fx^2 + gx + h$ is an integer. Hence,
\[
\begin{align*}
    a &= 8s + 3 \\
    b &= 8t + 3
\end{align*}
\]
and so $(a, b) \equiv (3, 3) \pmod{8}$.

Now we assume $r \equiv 1 \pmod{2}, q \equiv 1 \pmod{2}$ and so we set $r = 2u + 1 \ (u \in \mathbb{Z})$ and $q = 2v + 1 \ (v \in \mathbb{Z})$ and find that every coefficient of $x^6 + cx^5 + dx^4 + ex^3 + fx^2 + gx + h$ is an integer. Hence,
\[
\begin{align*}
    a &= 8u + 7 \\
    b &= 8v + 7
\end{align*}
\]
and so $(a, b) \equiv (7, 7) \pmod{8}$, which completes the proof for this case.

**Case** $(1, 1, 1, 1)$: $\lambda = \frac{1+\theta+\theta^2+\theta^3+\theta^4}{2}$

First assume $(a, b) \equiv (0, 2) \pmod{4}$. We set $a = 4v$ and $b = 4u + 2 \ (u, v \in \mathbb{Z})$. Then,
by MAPLE\textsuperscript{TM}, \(\lambda\) satisfies the polynomial

\[
x^6 + (-16v^2 + 4v + 1 + 8u)x^5 + (256v^5 - 64v^4 - 320v^3 u - 144v^3 + 88v^2 + 64v^2 u - 15v
+ 52vu + 80vu^2 - 11u + 8u^2)x^4 + (-7 - 8u + 68v + 384v^4 - 512v^5 - 212v^2 + 144v^3
+ 320v^3 u - 400v^2 u - 256v^3 u^2 - 28u^2 + 108vu + 256v^4 u + 160vu^2 - 192v^2 u^2 + 192vu^3)x^3
+ (10 + 35u - 81v - 352v^4 + 384v^5 + 212v^2 - 100v^3 - 192v^3 u + 532v^2 u + 320v^3 u^2
+ 100u^2 - 248vu - 320v^4 u - 464vu^2 + 136u^3 + 400v^2 u^2 - 64vu^4 - 464vu^3 + 64v^2 u^3
+ 144u^4 + 64u^5)x^2 + (-5 - 22u + 38v + 128v^4 - 128v^5 - 92v^2 + 40v^3 + 80v^3 u - 264v^2 u
- 128v^3 u^2 - 68u^2 + 140vu + 128v^4 u + 288vu^2 - 112u^3 - 240v^2 u^2 + 64vu^4 + 304vu^3
- 64v^2 u^3 - 128v^4 - 64u^5)x + 1 + 5u - 7v - 16v^4 + 16v^5 + 16v^2 - 8v^3 - 16v^3 u + 48v^2 u
+ 16v^3 u^2 + 16u^2 - 28vu - 16v^4 u - 60vu^2 + 28u^3 + 48v^2 u^2 - 16vu^4 - 64vu^3 + 16v^2 u^3
+ 32u^4 + 16u^5
\]

which belongs to \(\mathbb{Z}[x]\) and so \(\lambda\) is an algebraic integer. Now assume \((a, b) \equiv (2, 0)\)
(mod 4) and so we set \(a = 4n + 2\) and \(b = 4m\) \((n, m \in \mathbb{Z})\). Then, by MAPLE\textsuperscript{TM}, \(\lambda\)
satisfies the polynomial

\[ x^6 + (-16n^2 - 12n - 5 + 8m)x^5 + (17 - 57m + 95n + 304n^2 + 48m^2 + 528n^3) \\
+ 576n^4 - 320mn^3 - 416mn^2 - 204mn + 80m^2n + 256n^5 \]
\[ +( -20 + 102m - 122n - 436n^2 - 172m^2 + 96m^3 - 848n^3 - 1024n^4 + 1088mn^3 \]
\[ + 1040mn^2 + 444mn - 512m^2n + 256mn^4 - 256m^2n^3 - 576m^2n^2 + 192m^3n - 512n^5 \]x^3
\[ +(17 - 104m + 100n + 344n^2 + 64m^5 + 216m^2 - 48m^4 - 144m^3 + 652n^3 + 768n^4 \]
\[ -1152mn^3 - 1068mn^2 - 464mn + 680m^2n - 320mn^4 + 320m^2n^3 + 784m^2n^2 \]
\[ - 272m^3n + 64m^3n^2 - 64m^4n + 384n^5 \]x^2 \[ + (-7 + 46m - 38n - 124n^2 - 64m^5 \]
\[ -100m^2 + 64m^4 + 56m^3 - 224n^3 - 256n^4 + 464mn^3 + 432mn^2 + 196mn - 312m^2n \]
\[ + 128mn^4 - 128m^2n^3 - 336m^2n^2 + 112m^3n - 64m^3n^2 + 64m^4n - 128n^5 \]x + 1
\[ + 5n + 16n^2 + 16m^5 - 7m + 16m^2 - 16m^4 - 8m^3 + 28n^3 + 32n^4 - 64mn^3 - 60mn^2 \]
\[ - 28mn + 48m^2n - 16m^4n + 16m^2n^3 + 48m^2n^2 - 16m^3n + 16m^3n^2 - 16m^4n + 16n^5 \]

which belongs to \( \mathbb{Z}[x] \) and so \( \lambda \) is an algebraic integer.

Now we prove the converse. Assume \( \lambda \) is an algebraic integer. We begin first by using MAPLE\textsuperscript{TM} to determine the sextic polynomial

\[ x^6 + cx^5 + dx^4 + ex^3 + fx^2 + gx + h \]

satisfied by \( \lambda \) where \( c, d, e, f, g, h \in \mathbb{Z} \). Note that both this sextic polynomial as well as

\[ f(x) = x^6 + ax^4 + bx^2 + 1 \]

have \( \theta \) as a root. Using MAPLE\textsuperscript{TM}, we compute the remainder of this division and set each of its coefficients equal to zero. We find

\[ d = \frac{d_1}{4} \]
where \( d_1 \) is a polynomial in terms of \( a \) and \( b \) with integral coefficients such that

\[
d_1 \equiv a^5 + a^4 + ba^3 + a^3 + ba + a + b^2 a + b \pmod{2}
\equiv ba^3 + b \pmod{2}.
\]

This implies either \( a \equiv 1 \pmod{2} \) or \( b \equiv 0 \pmod{2} \).

First assume \( a \equiv 1 \pmod{2} \) and so we set \( a = 2p + 1 \) (\( p \in \mathbb{Z} \)) and find that

\[
f = \frac{f_1}{16}
\]

where \( f_1 \) is a polynomial in terms of \( b \) and \( p \) with integral coefficients such that

\[
f_1 \equiv 1 + b^5 \pmod{2}.
\]

This implies \( b \equiv 1 \pmod{2} \) and so we set \( b = 2q + 1 \) (\( q \in \mathbb{Z} \)) and find that

\[
f = \frac{f_2}{8}
\]

where \( f_2 \) is a polynomial in terms of \( p \) and \( q \) with integral coefficients such that

\[
f_2 \equiv 1 + q \pmod{2}.
\]

This implies \( q \equiv 1 \pmod{2} \) and so we set \( q = 2r + 1 \) (\( r \in \mathbb{Z} \)) and find that

\[
d = \frac{d_2}{2}
\]

where \( d_2 \) is a polynomial in terms of \( p \) and \( r \) with integral coefficients such that

\[
d_2 \equiv 1 \pmod{2}.
\]
Since \( d \in \mathbb{Z} \), we require \( d_2 \equiv 0 \pmod{2} \). Thus, \( \lambda \) is not algebraic integer, a contradiction.

Hence, we must have \( b \equiv 0 \pmod{2} \) and so we set \( b = 2k \ (k \in \mathbb{Z}) \) and find that

\[
f = \frac{f_3}{16}
\]

where \( f_3 \) is a polynomial in terms of \( a \) and \( k \) with integral coefficients such that

\[
f_3 \equiv a^3 \pmod{2}.
\]

This implies \( a \equiv 0 \pmod{2} \) and so we set \( a = 2l \ (l \in \mathbb{Z}) \) and find that

\[
d = \frac{d_3}{2}
\]

where \( d_3 \) is a polynomial in terms of \( k \) and \( l \) with integral coefficients such that

\[
d_3 \equiv l + 1 + k \pmod{2}.
\]

This implies either \( l \equiv 0 \pmod{2}, k \equiv 1 \pmod{2} \) or \( l \equiv 1 \pmod{2}, k \equiv 0 \pmod{2} \).

First assume \( l \equiv 1 \pmod{2}, k \equiv 0 \pmod{2} \) and so we set \( l = 2n + 1 \ (n \in \mathbb{Z}) \) and \( k = 2m \ (m \in \mathbb{Z}) \) and find that every coefficient of \( x^6 + cx^5 + dx^4 + ex^3 + fx^2 + gx + h \) is an integer. Hence,

\[
\begin{align*}
a &= 4n + 2 \\
b &= 4m
\end{align*}
\]

and so \( (a, b) \equiv (2, 0) \pmod{4} \).

Now we assume \( l \equiv 0 \pmod{2}, k \equiv 1 \pmod{2} \) and so we set \( l = 2v \ (v \in \mathbb{Z}) \) and \( k = 2u + 1 \ (u \in \mathbb{Z}) \) and find that every coefficient of \( x^6 + cx^5 + dx^4 + ex^3 + fx^2 + gx + h \) is an integer. Hence,

\[
\begin{align*}
a &= 4v \\
b &= 4u + 2
\end{align*}
\]
and so \((a, b) \equiv (0, 2) \pmod{4}\), which completes the proof for this case.

In conclusion, \(K\) is monogenic with power basis \(\{1, \theta, \theta^2, \theta^3, \theta^4, \theta^5\}\) if and only if

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

Our second lemma is proved in a similar manner.

**Lemma 6.2.2** Let \(g(x) = x^3 + ax^2 + bx - 1 \in \mathbb{Z}[x]\). Let \(\alpha\) be a root of \(g(x)\). Suppose that \(g(x)\) defines a monogenic cubic field \(C\) and that \(\{1, \alpha, \alpha^2\}\) is a power basis of \(C\). Let \(f(x) = x^6 + ax^4 + bx^2 - 1\) and suppose that \(\theta\) is a root of \(f(x)\). Let \(K = \mathbb{Q}(\theta)\) and suppose that \([K : \mathbb{Q}] = 6\). Then \(K\) is monogenic with power basis \(\{1, \theta, \theta^2, \theta^3, \theta^4, \theta^5\}\) if and only if

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

**Proof.** In a similar proof to that of Lemma 6.2.1, it can be shown (see Appendix) that \(\lambda = \frac{a_0 + a_1 \theta + a_2 \theta^2 + a_3 \theta^3 + a_4 \theta^4 + \theta^5}{2}\) is never an algebraic integer when

\[
(a_0, a_1, a_2, a_3, a_4) = (0, 0, 0, 0, 0), (0, 0, 0, 1, 0), (0, 0, 0, 1, 1), (0, 1, 0, 0, 1), (0, 1, 0, 1, 0),
(0, 1, 1, 0, 0), (0, 1, 1, 1, 1), (1, 0, 0, 1, 0), (1, 0, 1, 0, 0), (1, 0, 1, 1, 1),
(1, 1, 0, 1, 1), (1, 1, 1, 0, 1), (1, 1, 1, 1, 0).
\]

In the remaining cases, TABLE 6.2.3 gives necessary and sufficient conditions on \(a\) and \(b\) for \(\lambda\) to be an algebraic integer.
Table 6.2.3: Lifting Monogenic Cubic Fields - Lemma 6.2.2

<table>
<thead>
<tr>
<th>((a_0, a_1, a_2, a_3, a_4))</th>
<th>Conditions on ((a, b)) for (\lambda) to be an Algebraic Integer</th>
</tr>
</thead>
<tbody>
<tr>
<td>((0, 0, 0, 0, 1))</td>
<td>((a, b) \equiv (13, 3)) (mod 16) and (a \equiv -b) (mod 64)</td>
</tr>
<tr>
<td>((0, 0, 1, 0, 0))</td>
<td>((a, b) \equiv (0, 0)) (mod 4)</td>
</tr>
<tr>
<td>((0, 0, 1, 0, 1))</td>
<td>((a, b) \equiv (3, 2)) (mod 4)</td>
</tr>
<tr>
<td>((0, 0, 1, 1, 0))</td>
<td>((a, b) \equiv (2, 1)) (mod 4)</td>
</tr>
<tr>
<td>((0, 0, 1, 1, 1))</td>
<td>((a, b) \equiv (1, 3)) (mod 4)</td>
</tr>
<tr>
<td>((0, 1, 0, 0, 0))</td>
<td>((a, b) \equiv (1, 3), (3, 1)) (mod 4)</td>
</tr>
<tr>
<td>((0, 1, 0, 1, 1))</td>
<td>((a, b) \equiv (2, 1)) (mod 4) or ((a, b) \equiv (13, 3)) (mod 16) and (a \equiv -b) (mod 64)</td>
</tr>
<tr>
<td>((0, 1, 1, 0, 1))</td>
<td>((a, b) \equiv (0, 0)) (mod 4) or ((a, b) \equiv (1, 7), (5, 3)) (mod 8)</td>
</tr>
<tr>
<td>((0, 1, 1, 1, 0))</td>
<td>((a, b) \equiv (3, 2)) (mod 4) or ((a, b) \equiv (13, 3)) (mod 16) and (a \equiv -b) (mod 64)</td>
</tr>
<tr>
<td>((1, 0, 0, 0, 0))</td>
<td>((a, b) \equiv (13, 3)) (mod 16) and (a \equiv -b) (mod 64)</td>
</tr>
<tr>
<td>((1, 0, 0, 0, 1))</td>
<td>((a, b) \equiv (2, 1)) (mod 4)</td>
</tr>
<tr>
<td>((1, 0, 0, 1, 1))</td>
<td>((a, b) \equiv (3, 2)) (mod 4) or ((a, b) \equiv (1, 7), (5, 3)) (mod 8)</td>
</tr>
<tr>
<td>((1, 0, 1, 0, 1))</td>
<td>((a, b) \equiv (13, 3)) (mod 16) and (a \equiv -b) (mod 64)</td>
</tr>
<tr>
<td>((1, 0, 1, 1, 0))</td>
<td>((a, b) \equiv (0, 0), (1, 3)) (mod 4)</td>
</tr>
<tr>
<td>((1, 1, 0, 0, 0))</td>
<td>((a, b) \equiv (3, 2)) (mod 4)</td>
</tr>
<tr>
<td>((1, 1, 0, 0, 1))</td>
<td>((a, b) \equiv (1, 3), (3, 1)) (mod 4)</td>
</tr>
<tr>
<td>((1, 1, 0, 1, 0))</td>
<td>((a, b) \equiv (13, 3)) (mod 16) and (a \equiv -b) (mod 64)</td>
</tr>
<tr>
<td>((1, 1, 1, 0, 0))</td>
<td>((a, b) \equiv (2, 1)) (mod 4) or ((a, b) \equiv (1, 7), (5, 3)) (mod 8)</td>
</tr>
<tr>
<td>((1, 1, 1, 1, 1))</td>
<td>((a, b) \equiv (0, 0), (2, 2)) (mod 4) or ((a, b) \equiv (13, 3)) (mod 16) and (a \equiv -b) (mod 64)</td>
</tr>
</tbody>
</table>

Before we prove our next two lemmas, we make the following observation.

**Remark 6.2.3** We wish to determine when \(4x^3 - 27\) \((x \in \mathbb{Z})\) is a square. Setting
4x^3 - 27 = y^2 for x, y ∈ ℤ we have

\[
4x^3 - 27 = y^2 \iff 64x^3 - 432 = 16y^2 \\
\iff (4x)^3 - 432 = (4y)^2 \\
\iff X^3 - 432 = Y^2.
\]

Using the computational software program MAGMA\textsuperscript{TM}, we see that the elliptic curve \( Y^2 = X^3 - 432 \) has conductor 27, rank 0 and \((12, \pm 36)\) as its only integral points. Since \( X = 12 \iff x = 3 \), we deduce \( 4x^3 - 27 = y^2 \) \((x, y ∈ ℤ)\) if and only if \( x = 3 \). In conclusion, we observe that \( 4x^3 - 27 \) \((x ∈ ℤ)\) is a square if and only if \( x = 3 \).

**Lemma 6.2.4** For the values of \( d \) specified in column 1 of TABLE 6.2.4 define \( f_d(x) \) as in column 2. Then \( f_d(x) \) is irreducible and the Galois group of \( f_d(x) \) is given in column 3.

<table>
<thead>
<tr>
<th>( d )</th>
<th>( f_d(x) )</th>
<th>Galois Group of ( f_d )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( d ∈ ℤ )</td>
<td>( x^6 + (2d + 2)x^4 + (2d - 1)x^2 - 1 )</td>
<td>( A_4 )</td>
</tr>
<tr>
<td>( d ∈ ℤ )</td>
<td>( x^6 - (2d + 2)x^4 + (2d - 1)x^2 + 1 )</td>
<td>( A_4 \times C_2 )</td>
</tr>
<tr>
<td>( d ∈ ℤ, d \equiv 1 \text{ (mod 2)}, d &gt; 3 )</td>
<td>( x^6 - dx^2 - 1 )</td>
<td>((S_4, +))</td>
</tr>
<tr>
<td>( d ∈ ℤ, d \equiv 1 \text{ (mod 2)}, d &gt; 3 )</td>
<td>( x^6 - dx^2 + 1 )</td>
<td>( S_4 \times C_2 )</td>
</tr>
<tr>
<td>( d ∈ ℤ, d \neq 0, 2, 3 )</td>
<td>( x^6 + 2dx^4 + d^2x^2 + 1 )</td>
<td>( D_6 )</td>
</tr>
</tbody>
</table>

**Proof.** The assertion of the first row of TABLE 6.2.4 is proved in [8] and so we need only give the proofs of the assertions of the second, third, fourth and fifth rows of TABLE 6.2.4. We begin first with the second row.

Let

\[
f_d(x) = x^6 - (2d + 2)x^4 + (2d - 1)x^2 + 1
\]
where $d \in \mathbb{Z}$ and also assume

\[
\theta_d \text{ is a root of } f_d(x), \\
K_d = \mathbb{Q}(\theta_d), \\
L_d = \text{normal closure of } K_d, \\
g_d(x) = x^3 - (2d + 2)x^2 + (2d - 1)x + 1.
\]

First we show that $K_d$ contains a unique real cyclic cubic subfield $C_d$. For $d \in \mathbb{Z}$, we have

\[
g_d(1) = -1 \neq 0
\]

and

\[
g_d(-1) = -1 - 4d \neq 0.
\]

Thus, by the Rational Root theorem, we deduce $g_d(x) = x^3 - (2d + 2)x^2 + (2d - 1)x + 1$ is irreducible over $\mathbb{Q}$ for $d \in \mathbb{Z}$. Now $\theta_d$ is a root of $f_d(x)$ which implies $\theta_d^2$ is a root of $g_d(x)$ and so $C_d = \mathbb{Q}(\theta_d^2)$ is a cubic subfield of $K_d$. Moreover, the discriminant of $g_d(x)$ is equal to $(4d^2 + 2d + 7)^2$ and so this cubic subfield $C_d$ is cyclic and hence real.

Now we prove $C_d$ is unique. Assume there exists another (distinct) cubic subfield $F$ of $K_d$. Then the compositum field $C_d \cap F$ is a subfield of $K_d$ of degree 9 over $\mathbb{Q}$. Hence $9 \mid [K_d : \mathbb{Q}]$. However, $[K_d : \mathbb{Q}] \leq 6$, a contradiction. Thus, $K_d$ contains a unique real cyclic cubic subfield $C_d$.

Now we prove $f_d(x)$ is irreducible over $\mathbb{Q}$. By way of contradiction, assume $f_d(x)$ is reducible over $\mathbb{Q}$. Then $[K_d : \mathbb{Q}] < 6$. We have shown that $K_d$ contains a subfield of degree 3 over $\mathbb{Q}$ and so we must have $[K_d : \mathbb{Q}] = 3$. Therefore, $\theta_d$ is a root of an irreducible cubic polynomial over $\mathbb{Q}$, say

\[
h(x) = x^3 + ax^2 + bx + c
\]

for $a, b, c \in \mathbb{Z}$. Clearly $-\theta_d$ is a root of $-h(-x)$. Moreover, it is easy to see that
\( h(x) \neq -h(-x) \). Since \( \theta_d \) and \(-\theta_d\) are both roots of \( f_d(x) \), we deduce that

\[
f_d(x) = h(x) \cdot (-h(-x)) = x^6 + (2b - a^2)x^4 + (b^2 - 2ac)x^2 - c^2.
\]

But \( f_d(x) = x^6 - (2d + 2)x^4 + (2d - 1)x^2 + 1 \) implying \(-c^2 = 1\), a contradiction. Hence \( f_d(x) \) is irreducible over \( \mathbb{Q} \).

Next we show that \( f_d(x) \) has four real roots and two complex (nonreal) roots. First we note that since the square of each root of \( f_d \) belongs to the real cubic subfield \( C_d \), each root of \( f_d \) must be of the form \( r \) or \( ri \), where \( r \in \mathbb{R} \). We also note that for each root of \( f_d \), its negative is also a root of \( f_d \). Now the discriminant of \( f_d(x) \) is equal to

\[
-2^6(4d^2 + 2d + 7)^4 < 0
\]

which implies \( f_d(x) \) has some nonreal roots. The discriminant of \( f_d \) would be positive if \( f_d \) had four complex roots. Hence, \( f_d \) has either two or six complex roots. Therefore, the number of real roots of \( f_d \) is either four or zero. First assume \( f_d \) has no real roots. Then the roots of \( f_d \) would be

\[
\pm r_1i, \pm r_2i, \pm r_3i
\]

where \( r_1, r_2, r_3 \in \mathbb{R} \setminus \{0\} \). It then follows that

\[
f_d(x) = (x^2 + r_1^2)(x^2 + r_2^2)(x^2 + r_3^2) = x^6 + (r_1^2 + r_2^2 + r_3^2)x^4 + (r_1^2r_2^2 + r_2^2r_3^2 + r_1^2r_3^2)x^2 + r_1^2r_2^2r_3^2
\]

so that the coefficients of the \( x_4 \) and \( x^2 \) terms are always positive. However, this is a contradiction since \( f_d(x) = x^6 - (2d + 2)x^4 + (2d - 1)x^2 + 1 \) for \( d \in \mathbb{Z} \). Hence, \( f_d \)
has four real roots and two nonreal roots, namely,

$$\pm \phi_1 = \pm r_1, \quad \pm \phi_2 = \pm r_2, \quad \pm \phi_3 = \pm r_3i,$$

where $r_1, r_2, r_3 \in \mathbb{R}$ with $\phi_1 = \theta_d$.

Next we show 

$$[L_d : \mathbb{Q}] = 24.$$ 

Since $f_d$ is irreducible over $\mathbb{Q}$, we have 

$$[K_d : \mathbb{Q}] = 6.$$ 

We will show $\phi_2 \notin K_d$. By way of contradiction, suppose that $\phi_2 \in K_d = \mathbb{Q}(\phi_1)$. Then 

$$\phi_2 = \alpha + \beta \phi_1$$

for $\alpha, \beta \in C_d \subset K_d$. Squaring both sides of this equation and rearranging, we obtain 

$$\phi_2^2 - \alpha^2 - \beta^2 \phi_1^2 = 2\alpha \beta \phi_1.$$ 

Using the fact that $\phi_1^2, \phi_2^2 \in C_d$ and $C_d$ is closed under addition and multiplication, we deduce 

$$2\alpha \beta \phi_1 \in C_d.$$ 

Since $\phi_1$ generates $K_d$, a degree six extension of $\mathbb{Q}$, we have $\phi_1 \notin C_d$. Thus, either $\alpha = 0$ or $\beta = 0$. Since $\phi_2 \notin C_d$, we must have $\beta \neq 0$. Therefore, $\alpha = 0$ so that 

$$\phi_2 = \beta \phi_1.$$
Squaring both sides of this equation yields

\[ \phi_2^2 = \beta^2 \phi_1^2. \]

Since each \( \phi_i^2 \) generates a cyclic (and normal) cubic field, namely \( C_d \), and are conjugate elements, there exists an isomorphism \( \sigma \) of \( C_d \) which we will write in cycle notation as

\( (\phi_1^2, \phi_2^2, \phi_3^2). \)

Applying this isomorphism to our previous equation, we obtain

\[
\sigma(\phi_2^2) = \sigma(\beta^2 \phi_1^2) \iff \phi_2^2 = \sigma(\beta^2) \sigma(\phi_1^2) \\
\iff \phi_2^2 = \sigma(\beta^2) \phi_2^2.
\]

However,

\[ \sigma(\beta^2) \phi_2^2 = \sigma(\beta^2 \phi_2^2) > 0 \]

and

\[ \phi_3^2 = -r_3^2 < 0, \]

a contradiction. Hence, \( \phi_2 \notin K_d \). Therefore,

\[ [K_d(\phi_2) : \mathbb{Q}] = [K_d(\phi_2) : K_d] \cdot [K_d : \mathbb{Q}] = 2 \cdot 6 = 12. \]

Since \( \phi_3 \) is complex, we have \( \phi_3 \notin K_d(\phi_2) \) and so

\[ [L_d : \mathbb{Q}] = [K_d(\phi_2, \phi_3) : \mathbb{Q}] = [K_d(\phi_2, \phi_3) : K_d(\phi_2)] \cdot [K_d(\phi_2) : \mathbb{Q}] = 2 \cdot 12 = 24. \]

Lastly, we now show the Galois group of \( f_d \) is \( A_4 \times C_2 \). Since

\[ [L_d : \mathbb{Q}] = 24 \]
and the discriminant of \( f_d \) is negative, we see that the Galois group is either \((S_4, -)\) or \(A_4 \times C_2\) (see p. 330, [6]). Now \( L_d \) contains a cyclic cubic and hence normal subfield, namely \( C_d \), so that the Galois group of \( f_d \) contains a normal subgroup of index 3, that is a normal subgroup of order 8. However, \( S_4 \) does not have a normal subgroup of order 8 and so we deduce that the Galois group of \( f_d \) must be \( A_4 \times C_2 \).

We now prove the assertion of the third row of TABLE 6.2.4. Let

\[
 f_d(x) = x^6 - dx^2 - 1
\]

where \( d \equiv 1 \pmod{2}, d > 3, d \in \mathbb{Z} \) and also assume

\[
 \theta_d \text{ is a root of } f_d(x), \\
 K_d = \mathbb{Q}(\theta_d), \\
 L_d = \text{normal closure of } K_d, \\
 g_d(x) = x^3 - dx - 1.
\]

First we show that \( K_d \) contains a unique totally real non-abelian cubic subfield \( C_d \).

For \( d \equiv 1 \pmod{2}, d > 3, d \in \mathbb{Z} \), we have

\[
 g_d(1) = -d \neq 0
\]

and

\[
 g_d(-1) = -2 + d \neq 0.
\]

Thus, by the Rational Root theorem, we deduce \( g_d(x) = x^3 - dx - 1 \) is irreducible over \( \mathbb{Q} \) for the specified \( d \) given above. Now \( \theta_d \) is a root of \( f_d(x) \) which implies \( \theta_d^2 \) is a root of \( g_d(x) \) and so \( C_d = \mathbb{Q}(\theta_d^2) \) is a cubic subfield of \( K_d \). Moreover, the discriminant of \( g_d(x) \) is equal to \( 4d^3 - 27 \) (not a square) and so this cubic subfield \( C_d \) is non-abelian. Since the discriminant of \( g_d(x) \) is positive for the specified \( d \) values above, it follows that \( C_d \) is totally real. Now we prove \( C_d \) is unique. Assume there exists another
(distinct) cubic subfield $F$ of $K_d$. Then the compositum field $C_d \vee F$ is a subfield of $K_d$ of degree 9 over $\mathbb{Q}$. Hence $9 \mid [K_d : \mathbb{Q}]$. However, $[K_d : \mathbb{Q}] \leq 6$, a contradiction. Thus, $K_d$ contains a unique real non-abelian cubic subfield $C_d$.

Now we prove $f_d(x)$ is irreducible over $\mathbb{Q}$. By way of contradiction, assume $f_d(x)$ is reducible over $\mathbb{Q}$. Then $[K_d : \mathbb{Q}] < 6$. We have shown that $K_d$ contains a subfield of degree 3 over $\mathbb{Q}$ and so we must have $[K_d : \mathbb{Q}] = 3$. Therefore, $\theta_d$ is a root of an irreducible cubic polynomial over $\mathbb{Q}$, say

$$h(x) = x^3 + ax^2 + bx + c$$

for $a, b, c \in \mathbb{Z}$. Clearly $-\theta_d$ is a root of $-h(-x)$. Moreover, it is easy to see that $h(x) \neq -h(-x)$. Since $\theta_d$ and $-\theta_d$ are both roots of $f_d(x)$, we deduce that

$$f_d(x) = h(x) \cdot (-h(-x))$$

$$= x^6 + (2b - a^2)x^4 + (b^2 - 2ac)x^2 - c^2.$$

So $f_d(x) = x^6 - dx^2 - 1$ implies

$$\begin{cases} 
2b - a^2 = 0 \\
b^2 - 2ac = -d \\
c^2 = 1 
\end{cases}$$

or equivalently,

$$d = \begin{cases} 
-\frac{a}{3}(a^3 - 8) & \text{if } c = 1 \\
-\frac{a}{3}(a^3 + 8) & \text{if } c = -1 
\end{cases}.$$

Since $d \in \mathbb{Z}$, this implies $a \equiv 0 \pmod{2}$. This then implies $d \equiv 0 \pmod{2}$, a contradiction. Hence $f_d(x)$ is irreducible over $\mathbb{Q}$.

Next we show that $f_d$ has two real roots and four nonreal roots. We begin with showing $f_d$ has some nonreal roots. By way of contradiction, assume that all the
roots of $f_d(x)$ are real. For $d \equiv 1 \pmod{2}$, $d > 3$, $d \in \mathbb{Z}$, we have

$$\begin{cases} g(-d) = -(d^3 - d^2 + 1) < 0 \\ g(-1) = -2 + d > 0 \end{cases}.$$ 

This implies, by the Intermediate Value Theorem, $g_d(x)$ has a root, say $\alpha_1$, in the interval $(-d, -1)$. Since $g_d(x^2) = f_d(x)$, this implies a root of $f_d(x)$ is then $\sqrt{\alpha_1}$. Since all the roots of $f_d(x)$ are real, $\alpha_1$ must be a real positive number. But $\alpha_1 \in (-d, -1)$, a contradiction. Thus, the roots of $f_d(x)$ are not all real. Since the discriminant of $f_d$ is equal to $2^6(4d^3 - 27)^2 > 0$, $f_d$ must have exactly four nonreal roots. We note that since the square of each root of $f_d$ belongs to the real cubic subfield $C_d$ or a conjugate field of $C_d$, each root of $f_d$ must be of the form $r$ or $ri$, where $r \in \mathbb{R}$. We also note that for each root of $f_d$, its negative is also a root of $f_d$. Therefore, we may take the six roots of $f_d$ to be

$$\pm \phi_1 = \pm r_1, \; \pm \phi_2 = \pm r_2i, \; \pm \phi_3 = \pm r_3i$$

where $r_1, r_2, r_3 \in \mathbb{R}$ with $\phi_1 = \theta_d$.

Next we show that

$$[L_d : \mathbb{Q}] = 24$$

and we need to determine the Galois group of $f_d$. Since $f_d$ is irreducible over $\mathbb{Q}$, we have

$$[K_d : \mathbb{Q}] = 6.$$ 

Moreover, $K_d$ is real implies we must have $\phi_2 \notin K_d$. Therefore,

$$[K_d(\phi_2) : \mathbb{Q}] = [K_d(\phi_2) : K_d] \cdot [K_d : \mathbb{Q}] = 2 \cdot 6 = 12.$$ 

This implies that

$$12 \mid [L_d : \mathbb{Q}].$$
Now we either have $\phi_3 \in K_d(\phi_2)$ or $\phi_3 \notin K_d(\phi_2)$ and so this implies

$$[L_d : \mathbb{Q}] = [K_d(\phi_2, \phi_3) : \mathbb{Q}] \leq 24.$$ 

Hence, we either have $[L_d : \mathbb{Q}] = 12$ or $[L_d : \mathbb{Q}] = 24$. By way of contradiction, assume

$$[L_d : \mathbb{Q}] = 12.$$ 

Since the discriminant of $f_d$ is a square in $\mathbb{Q}$, the Galois group of $f_d$ would be $A_4$ (see p. 330, [6]). Since $A_4$ contains a normal subgroup of order four (the Klein four-group), this implies $L_d$ contains a normal subfield of degree three. However, $C_d$ is the unique totally real non-abelian cubic subfield of $K_d$ (and hence $L_d$), a contradiction. Thus

$$[L_d : \mathbb{Q}] = 24$$

and since the discriminant of $f_d$ is a square in $\mathbb{Q}$, the Galois group of $f_d$ is $(S_4, +)$ (see p. 330, [6]).

We now prove the assertion of the fourth row of TABLE 6.2.4. Let

$$f_d(x) = x^6 - dx^2 + 1$$

where $d \equiv 1 \pmod{2}$, $d > 3$, $d \in \mathbb{Z}$ and also assume

- $\theta_d$ is a root of $f_d(x)$,
- $K_d = \mathbb{Q}(\theta_d)$,
- $L_d = \text{normal closure of } K_d$,
- $g_d(x) = x^3 - dx + 1$.

First we show that $K_d$ contains a unique totally real non-abelian cubic subfield $C_d$. 

130
For $d \equiv 1 \pmod{2}$, $d > 3$, $d \in \mathbb{Z}$, we have

$$g_d(1) = 2 - d \neq 0$$

and

$$g_d(-1) = d \neq 0.$$

Thus, by the Rational Root theorem, we deduce $g_d(x) = x^3 - dx + 1$ is irreducible over $\mathbb{Q}$ for the specified $d$ given above. Now $\theta_d$ is a root of $f_d(x)$ which implies $\theta_d^2$ is a root of $g_d(x)$ and so $C_d = \mathbb{Q}(\theta_d^2)$ is a cubic subfield of $K_d$. Moreover, the discriminant of $g_d(x)$ is equal to $4d^3 - 27$ (not a square) and so this cubic subfield $C_d$ is non-abelian.

Since the discriminant of $g_d(x)$ is positive for the specified $d$ values above, it follows that $C_d$ is totally real. Now we prove $C_d$ is unique. Assume there exists another (distinct) cubic subfield $F$ of $K_d$. Then the compositum field $C_d \vee F$ is a subfield of $K_d$ of degree 9 over $\mathbb{Q}$. Hence $9 \mid [K_d : \mathbb{Q}]$. However, $[K_d : \mathbb{Q}] \leq 6$, a contradiction. Thus, $K_d$ contains a unique real non-abelian cubic subfield $C_d$.

Now we prove $f_d(x)$ is irreducible over $\mathbb{Q}$. By way of contradiction, assume $f_d(x)$ is reducible over $\mathbb{Q}$. Then $[K_d : \mathbb{Q}] < 6$. We have shown that $K_d$ contains a subfield of degree 3 over $\mathbb{Q}$ and so we must have $[K_d : \mathbb{Q}] = 3$. Therefore, $\theta_d$ is a root of an irreducible cubic polynomial over $\mathbb{Q}$, say

$$h(x) = x^3 + ax^2 + bx + c$$

for $a, b, c \in \mathbb{Z}$. Clearly $-\theta_d$ is a root of $-h(-x)$. Moreover, it is easy to see that $h(x) \neq -h(-x)$. Since $\theta_d$ and $-\theta_d$ are both roots of $f_d(x)$, we deduce that

$$f_d(x) = h(x) \cdot (-h(-x)) = x^6 + (2b - a^2)x^4 + (b^2 - 2ac)x^2 - c^2.$$

But $f_d(x) = x^6 - dx^2 + 1$ implying $-c^2 = 1$, a contradiction. Hence $f_d(x)$ is irreducible.
Next we show that $f_d$ has four real roots and two nonreal roots. Again we note that since the square of each root of $f_d$ belongs to the real cubic subfield $C_d$ or a conjugate field of $C_d$, each root of $f_d$ must be of the form $r$ or $ri$, where $r \in \mathbb{R}$. We also note that for each root of $f_d$, its negative is also a root of $f_d$. Now the discriminant of $f_d(x)$ is equal to

$$-2^6(4d^3 - 27)^2 < 0$$

which implies $f_d(x)$ has some nonreal roots. The discriminant of $f_d$ would be positive if $f_d$ had four complex roots. Hence, $f_d$ has either two or six complex roots.

Therefore, the number of real roots of $f_d$ is either four or zero. First assume $f_d$ has no real roots. Then the roots of $f_d$ would be

$$\pm r_1i, \pm r_2i, \pm r_3i$$

where $r_1, r_2, r_3 \in \mathbb{R}$. It then follows that

$$f_d(x) = (x^2 + r_1^2)(x^2 + r_2^2)(x^2 + r_3^2)$$

$$= x^6 + (r_1^2 + r_2^2 + r_3^2)x^4 + (r_1^2r_2^2 + r_1^2r_3^2 + r_2^2r_3^2)x^2 + r_1^2r_2^2r_3^2$$

so that the coefficients of the $x^4$ and $x^2$ terms are always positive. However, this is a contradiction since $f_d(x) = x^6 - dx^2 + 1$ for $d > 3$. Hence, $f_d$ has four real roots and two nonreal roots, namely,

$$\pm \phi_1 = \pm r_1, \pm \phi_2 = \pm r_2, \pm \phi_3 = \pm r_3i,$$

where $r_1, r_2, r_3 \in \mathbb{R}$ with $\phi_1 = \theta_d$.

Next we show

$$[L_d : \mathbb{Q}] = 48$$
and determine the Galois group of $f_d$. Since $f_d$ is irreducible over $\mathbb{Q}$, we have

$$[K_d : \mathbb{Q}] = 6.$$ 

Let $E_d$ denote the normal closure of $C_d = \mathbb{Q}(\theta_d^2)$ where $C_d$ is a non-abelian cubic field. Then

$$E_d = \mathbb{Q}(\phi_1^2, \phi_2^2, \phi_3^2)$$

and so $E_d$ is a normal real field extension of $\mathbb{Q}$ of degree six. First we show that $\phi_1 \notin E_d$. By way of contradiction, assume $\phi_1 \in E_d$. Since $K_d = \mathbb{Q}(\phi_1)$, this then implies $K_d \subseteq E_d$. Since $\phi_3 \in K_d$ this then implies $\phi_3 \in E_d$. But $E_d$ is a real field extension of $\mathbb{Q}$ as $\phi_1, \phi_2, \phi_3 \in \mathbb{R}$ and $\phi_3$ is nonreal, a contradiction. Hence $\phi_1 \notin E_d$. Now $\phi_1^2 \in E_d$ and so

$$[E_d(\phi_1) : \mathbb{Q}] = [E_d(\phi_1) : E_d] \cdot [E_d : \mathbb{Q}] = 2 \cdot 6 = 12.$$ 

Now assume, by way of contradiction, that $\phi_2 \in E_d(\phi_1)$ and so

$$\phi_2 = \alpha + \beta \phi_1$$

for $\alpha, \beta \in E_d$. Squaring both sides of this equation and using closure properties, we deduce that

$$2\alpha \beta \phi_1 = \phi_2^2 - \alpha^2 - \beta^2 \phi_1^2 \iff 2\alpha \beta \phi_1 \in E_d.$$ 

Since $\phi_1 \notin E_d$ we must have either $\alpha = 0$ or $\beta = 0$. But $\beta = 0$ is impossible as $\phi_2 \notin E_d$. Therefore, $\alpha = 0$ and so

$$\phi_2 = \beta \phi_1$$

so that

$$\phi_2^2 = \beta^2 \phi_1^2.$$
Since each \( \phi_j^2 \) generates a cubic field and are conjugate elements, there exists an isomorphism \( \sigma \) of \( E_d \) which we will write in cycle notation as

\[
(\phi_1^2, \phi_2^2, \phi_3^2).
\]

Applying this isomorphism to our previous equation, we obtain

\[
\sigma(\phi_2^2) = \sigma(\beta^2 \phi_1^2) \iff \phi_3^2 = \sigma(\beta^2) \sigma(\phi_1^2)
\]

\[
\iff \phi_3^2 = \sigma(\beta^2) \phi_2^2.
\]

However,

\[\sigma(\beta^2) \phi_2^2 = \sigma(\beta)^2 r_2^2 > 0\]

and

\[\phi_3^2 = -r_3^2 < 0,\]

a contradiction. Hence, \( \phi_2 \notin E_d(\phi_1). \) Therefore,

\[\left[ E_d(\phi_1, \phi_2) : \mathbb{Q} \right] = \left[ E_d(\phi_1, \phi_2) : E_d(\phi_1) \right] \cdot \left[ E_d(\phi_1) : \mathbb{Q} \right] = 2 \cdot 12 = 24.\]

Finally, as \( \phi_3 \) is nonreal, we have \( \phi_3 \notin E_d(\phi_1, \phi_2). \) Thus

\[\left[ E_d(\phi_1, \phi_2, \phi_3) : \mathbb{Q} \right] = \left[ E_d(\phi_1, \phi_2, \phi_3) : E_d(\phi_1, \phi_2) \right] \cdot \left[ E_d(\phi_1, \phi_2) : \mathbb{Q} \right] = 2 \cdot 24 = 48\]

and so

\[\left[ L_d : \mathbb{Q} \right] = 48.\]

Then we deduce that the Galois group of \( f_d \) is \( S_4 \times C_2 \) (see p. 330, [6]).

Finally we prove the assertion of the fifth row of TABLE 6.2.4. Let

\[ f_d(x) = x^6 + 2dx^4 + d^2x^2 + 1 \]
where \(d \in \mathbb{Z}, d \neq 0, 2, 3\) and also assume

\[
\theta_d \text{ is a root of } f_d(x), \\
K_d = \mathbb{Q}(\theta_d), \\
L_d = \text{normal closure of } K_d, \\
g_d(x) = x^3 + 2dx^2 + d^2x + 1.
\]

First we show that \(K_d\) contains a unique non-abelian cubic subfield \(C_d\). For \(d \in \mathbb{Z}, d \neq 0, 2, 3\), we have

\[
g_d(1) = 2 + 2d + d^2 \neq 0
\]

and

\[
g_d(-1) = -d(-2 + d) \neq 0.
\]

Thus, by the Rational Root theorem, we deduce \(g_d(x) = x^3 + 2dx^2 + d^2x + 1\) is irreducible over \(\mathbb{Q}\) for the specified \(d\) given above. Now \(\theta_d\) is a root of \(f_d(x)\) which implies \(\theta_d^2\) is a root of \(g_d(x)\) and so \(C_d = \mathbb{Q}(\theta_d^2)\) is a cubic subfield of \(K_d\). Moreover, the discriminant of \(g_d(x)\) is equal to \(4d^3 - 27\) (not a square) and so this cubic subfield \(C_d\) is non-abelian. Now we prove \(C_d\) is unique. Assume there exists another (distinct) cubic subfield \(F\) of \(K_d\). Then the compositum field \(C_d \cap F\) is a subfield of \(K_d\) of degree 9 over \(\mathbb{Q}\). Hence \(9 \mid [K_d : \mathbb{Q}]\). However, \([K_d : \mathbb{Q}] \leq 6\), a contradiction. Thus, \(K_d\) contains a unique non-abelian cubic subfield \(C_d\).

Now we prove \(f_d(x)\) is irreducible over \(\mathbb{Q}\). By way of contradiction, assume \(f_d(x)\) is reducible over \(\mathbb{Q}\). Then \([K_d : \mathbb{Q}] < 6\). We have shown that \(K_d\) contains a subfield of degree 3 over \(\mathbb{Q}\) and so we must have \([K_d : \mathbb{Q}] = 3\). Therefore, \(\theta_d\) is a root of an irreducible cubic polynomial over \(\mathbb{Q}\), say

\[
h(x) = x^3 + ax^2 + bx + c
\]

for \(a, b, c \in \mathbb{Z}\). Clearly \(-\theta_d\) is a root of \(-h(-x)\). Moreover, it is easy to see that
$h(x) \neq -h(-x)$. Since $\theta_d$ and $-\theta_d$ are both roots of $f_d(x)$, we deduce that

$$f_d(x) = h(x) \cdot (-h(-x))$$

$$= x^6 + (2b - a^2)x^4 + (b^2 - 2ac)x^2 - c^2.$$ 

But $f_d(x) = x^6 + 2dx^4 + d^2x^2 + 1$ implying $-c^2 = 1$, a contradiction. Hence $f_d(x)$ is irreducible over $\mathbb{Q}$. Since $f_d$ is irreducible over $\mathbb{Q}$, we then have

$$[K_d : \mathbb{Q}] = 6.$$ 

Next we note that over the field $K_d$ we have the factorization

$$f_d(x) = (x - \theta_d)(x + \theta_d)(x^2 - \theta_d x + \theta_d^2 + d)(x^2 + \theta_d x + \theta_d^2 + d).$$

Moreover, the discriminant of $f_d$ is equal to $-2^6(4d^3 - 27)^2$ and so the splitting field of $f_d(x)$ contains the quadratic subfields $\mathbb{Q}(\sqrt{4d^3 - 27})$ and $\mathbb{Q}(\sqrt{-1})$. Since

$$4d^3 - 27 = -z^2$$

is impossible modulo 4, $4d^3 - 27$ is not a generator of $\mathbb{Q}(\sqrt{-1})$ and so these two quadratic subfields are distinct. Therefore, at least one of the quadratics in the above factorization must be irreducible over $K_d$ and so

$$[L_d : \mathbb{Q}] \geq 12.$$ 

However both quadratics in the above factorization have the same discriminant, namely $-3\theta_d^2 - 4d$. Thus, when we adjoin a root of one of them to $K_d$, we have constructed the entire splitting field. Hence,

$$[L_d : \mathbb{Q}] = 12.$$ 

136
Since the discriminant of $f_d$ is not a square in $\mathbb{Q}$, the Galois group of $f_d$ must be $D_6$ (see p.330, [6]). ■

**Lemma 6.2.5** There exist at most finitely many polynomials

$$f(x) = x^6 + ax^4 + bx^2 \pm 1$$

irreducible over $\mathbb{Q}$ with the Galois group of $f$ equal to either $C_6, S_3$ or $(S_4, -)$ and such that a root of $f(x)$ is a monogenic generator of a sextic field and a root of $x^3 + ax^2 + bx \pm 1$ is a monogenic generator of a cubic field.

**Proof.** First we treat the case when the Galois group is $C_6$. Assume $f(x) = x^6 + ax^4 + bx^2 \pm 1$ is irreducible over $\mathbb{Q}$ with Galois group $C_6$ and such that a root of $f(x)$ is a monogenic generator of a sextic field and a root of $x^3 + ax^2 + bx \pm 1$ is a monogenic generator of a cubic field. By way of contradiction, assume there are infinitely many such polynomials. According to [6] (see p. 330), the discriminant of the polynomial $f(x)$ cannot be a square in $\mathbb{Q}$. As the discriminant of $x^6 + ax^4 + bx^2 - 1$ is

$$2^6(-27 - 18ab + a^2b^2 + 4a^3 - 4b^3)^2 = [2^3(-27 - 18ab + a^2b^2 + 4a^3 - 4b^3)]^2,$$

this forces $f(x) = x^6 + ax^4 + bx^2 + 1$. Moreover, the discriminant of $f(x)$ is equal to

$$-2^6(27 - 18ab - a^2b^2 + 4a^3 + 4b^3)^2 = -z^2$$

for some integer $z$ and so the splitting field of $f(x)$ contains $i$. By assumption, the splitting field must be equal to the compositum of a cubic field defined by

$$g(x) = x^3 + ax^2 + bx + 1$$

and the quadratic subfield $\mathbb{Q}(i)$. Moreover, since the Galois group of $f(x)$ is $C_6$, this cubic subfield is cyclic and is unique.
We note that if \( \theta \) is a root of \( f(x) \) then it follows that \( \theta^2 \) is a root of \( g(x) \). Since the roots of \( g(x) \) must be real (as they are elements of a cyclic cubic field), the roots of \( f(x) \) are either of the form \( \pm r \) or \( \pm ri \), where \( r \in \mathbb{R} \). But we know each root of \( f(x) \) generates a sextic field (the same field) which contains \( i \) and so each root must be complex. Thus, \( f(x) \) has six pure imaginary roots, namely \( \pm r_k i \) for \( k = 1, 2, 3 \) and where each \( r_k \in \mathbb{R} \).

Consider the monic sextic polynomial \( t(x) \) whose roots are equal to \( i \) times the roots of \( f(x) \), that is,

\[
\pm i \cdot r_k i = \mp r_k.
\]

We then must have

\[
t(x) = (x - r_1)(x + r_1)(x - r_2)(x + r_2)(x - r_3)(x + r_3)
\]

\[
= x^6 - (r_1^2 + r_2^2 + r_3^2)x^4 + (r_1^2 r_2^2 + r_1^2 r_3^2 + r_2^2 r_3^2)x^2 - r_1^2 r_2^2 r_3^2
\]

\[
= x^6 - ax^4 + bx^2 - 1.
\]

The roots of \( t(x) \) are all real numbers and thus cannot generate the splitting field of \( f(x) \). Now, clearly the squares of the roots of \( t(x) \) generate a cubic field and hence, this cubic field is cyclic. Clearly, the roots of \( t(x) \) are in the splitting field of \( f(x) \) and so these roots of \( t(x) \) must generate the same cyclic cubic field defined by

\[
g(x) = x^3 + ax^2 + bx + 1.
\]

Hence, \( t(x) \) must factor over \( \mathbb{Z} \) into two monic cubic polynomials. We note that if \( \alpha \) is a root of \( t(x) \) then \( -\alpha \) is also a root of \( t(x) \) and so we have

\[
t(x) = (x^3 + ux^2 + vx + 1)(x^3 - ux^2 + vx - 1)
\]
where $u, v \in \mathbb{Z}$. Denote one of these cubic factors as $c(x)$, say

$$c(x) = x^3 + ux^2 + vx + 1,$$

and assume $\beta$ is a root of this polynomial $c(x)$ and hence of $t(x)$. Thus,

$$t(\beta) = \beta^6 - a\beta^4 + b\beta^2 - 1 = 0.$$  

This implies

$$g(-\beta^2) = (-\beta^2)^3 + a(-\beta^2)^2 + b(-\beta^2) + 1 = \beta^6 + a\beta^4 - b\beta^2 + 1 = -\beta^6 + a\beta^4 + b\beta^2 - 1 = 0$$

and so $-\beta^2$ is a root of $g(x)$.

By assumption, the ring of integers of the cyclic cubic field is $\mathbb{Z}[-\beta^2] = \mathbb{Z}[\beta^2]$. Of course, $\mathbb{Z}[\beta^2] = \mathbb{Z}[\beta]$ in this case. As a result, the discriminants of the minimal polynomials of $\beta$ and $\beta^2$ are equal. Since $c(x)$ is irreducible over $\mathbb{Z}$, it follows that $c(x)$ is the minimal polynomial of $\beta$. The discriminant of $c(x)$ is equal to

$$-27 + 18uv + u^2v^2 - 4u^3 - 4v^3,$$

and moreover, we have

$$t(x) = (x^3 + ux^2 + vx + 1)(x^3 - ux^2 + vx - 1) = x^6 + (2v - u^2)x^4 - (2u - v^2)x^2 - 1.$$  

We wish to find the minimal polynomial of $\beta^2$. Assume the minimal polynomial of
$\beta^2$ is

$$h(x) = x^3 + Ax^2 + Bx + C$$

and so

$$h(\beta^2) = \beta^6 + A\beta^4 + B\beta^2 + C = 0.$$ 

Since $c(x)$ is the minimal polynomial of $\beta$ it follows that

$$c(\beta) \mid h(\beta^2).$$

Setting each coefficient of the remainder equal to zero and solving for the coefficients $A, B, C$ we find

$$A = 2v - u^2$$
$$B = v^2 - 2u$$
$$C = -1.$$ 

Hence, the minimal polynomial of $\beta^2$ is equal to

$$h(x) = x^3 + (2v - u^2)x^2 + (v^2 - 2u)x - 1$$

with discriminant equal to

$$(-27 + 18uv + u^2v^2 - 4u^3 - 4v^3)(uv - 1)^2.$$

Thus, the discriminant of the minimal polynomial of $\beta^2$ is equal to

$$D(c(x)) \cdot (uv - 1)^2,$$

which implies

$$uv - 1 = \pm 1.$$
Since $u, v \in \mathbb{Z}$, we have either $u = 0$ or $v = 0$ or

$$(u, v) = (-2, -1), (1, 2), (2, 1), (-1, -2).$$

If $u = 0$ then

$$c(x) = x^3 + vx + 1$$

with discriminant equal to

$$-4v^3 - 27$$

and if $v = 0$ then

$$c(x) = x^3 + ux^2 + 1$$

with discriminant equal to

$$-4u^3 - 27.$$ 

These are only square if $u = v = -3$ and cannot generate infinitely many cyclic cubic fields. Therefore, only finitely many choices remain, a contradiction. Hence, there exist at most finitely many polynomials

$$f(x) = x^6 + ax^4 + bx^2 + 1$$

irreducible over $\mathbb{Q}$ with the Galois group of $f$ equal to $C_6$ and such that a root of $f(x)$ is a monogenic generator of a sextic field and a root of $x^3 + ax^2 + bx + 1$ is a monogenic generator of a cubic field.

Now we treat the case when the Galois group is $S_3$. Assume $f(x) = x^6 + ax^4 + bx^2 + 1$ is irreducible over $\mathbb{Q}$ with Galois group $S_3$ and such that a root of $f(x)$ is a monogenic generator of a sextic field and a root of $x^3 + ax^2 + bx + 1$ is a monogenic generator of a cubic field. By way of contradiction, assume there are infinitely many such polynomials. According to [6] (see. p. 330), the discriminant of the polynomial $f(x)$
cannot be a square in \( \mathbb{Q} \). As the discriminant of \( x^6 + ax^4 + bx^2 - 1 \) is

\[
2^6(-27 - 18ab + a^2b^2 + 4a^3 - 4b^3)^2 = [2^3(-27 - 18ab + a^2b^2 + 4a^3 - 4b^3)]^2,
\]

this forces \( f(x) = x^6 + ax^4 + bx^2 + 1 \). Moreover, the discriminant of \( f(x) \) is equal to

\[
-2^6(27 - 18ab - a^2b^2 + 4a^3 + 4b^3)^2 = -z^2
\]

for some integer \( z \) and so the splitting field of \( f(x) \) contains \( i \). By assumption, the splitting field must be equal to the compositum of a cubic field defined by

\[
g(x) = x^3 + ax^2 + bx + 1
\]

and the quadratic subfield \( \mathbb{Q}(i) \). Moreover, since the Galois group of \( f(x) \) is \( S_3 \), this cubic subfield is nonabelian (and hence noncyclic).

We note that if \( f(x) \) had a real root \( \theta \) then the splitting field of \( f(x) \) would be \( \mathbb{Q}(\theta) \) (since the Galois group of \( f(x) \) is \( S_3 \), a group of order six). This then would imply the splitting field of \( f(x) \) is real which contradicts the fact that \( i \) belongs to the splitting field. We conclude then that \( f(x) \) has six nonreal roots.

We also note that if \( \theta \) is a root of \( g(x) \) then it follows that \( \sqrt{\theta} \) is a root of \( f(x) \). At least one root of \( g(x) \) must be real and denote it by \( t \). Since all the roots of \( f(x) \) are nonreal it follows that \( \sqrt{t} = ri \) is a root of \( f(x) \) where \( r \in \mathbb{R} \). Thus, \( t = \pm r^2 \) and so \( \mathbb{Q}(t) = \mathbb{Q}(r^2) \). Since \( t \) is a root of \( g(x) \), it follows that \( \mathbb{Q}(r^2) \) is a cubic field.

Moreover, if \( ri \) is a root of \( f(x) \) it follows that \( r \) is in the splitting field of \( f(x) \) as the splitting field contains \( i \). We cannot have the splitting field equal to \( \mathbb{Q}(r) \) since the splitting field contains \( i \) and hence is nonreal. This implies the degree of \( \mathbb{Q}(r) \) divides six. Since \( \mathbb{Q}(r) \supseteq \mathbb{Q}(r^2) \), we must have the degree of \( \mathbb{Q}(r) \) equal to three.
Thus, the minimal polynomial of $r$ must have degree 3 over $\mathbb{Q}$ and we denote it as

$$c(x) = x^3 + ux^2 + vx + w$$

where $u, v, w \in \mathbb{Z}$.

Recall that $t = \pm r^2$ is a root of the cubic polynomial $g(x) = x^3 + ax^2 + bx + 1$ and so the norm of $r^2$ is $\pm 1$. By properties of norms, we must also have the norm of $r$ equal to $\pm 1$. This implies

$$c(x) = x^3 + ux^2 + vx \pm 1.$$ 

Without loss of generality, assume $c(x) = x^3 + ux^2 + vx + 1$. Since the cubic field defined by $g(x)$ is monogenic with integral basis $\{1, r^2, r^4\}$, the polynomial discriminants of $r$ and $r^2$ must be equal. That is,

$$D(c(x)) = D(g(x)).$$

Consider the polynomial

$$j(x) = -c(x) \cdot c(-x) = x^6 - (u^2 - 2v)x^4 - (2u - v^2)x^2 - 1.$$ 

Making a change of variables, we obtain the polynomial

$$k(x) = j(\sqrt{x}) = x^3 - (u^2 - 2v)x^2 - (2u - v^2)x - 1.$$ 

Note that

$$k(r^2) = -c(\sqrt{r^2}) \cdot c(-\sqrt{r^2}) = -c(r) \cdot c(-r) = 0$$

as $r$ is a root of $c(x)$. Since $r^2$ is a root of both the monic cubic polynomials $g(x)$ and $k(x)$, it follows that they must have equal polynomial discriminants. Moreover, we
must have \(-k(-x) = g(x)\) as both are monic, cubic polynomials with constant equal to 1 with \(r^2\) a root.

Thus,

\[ D(c(x)) = D(k(x)). \]

Using MAPLE\textsuperscript{TM}, we find

\[
D(k(x)) = -(4u^3 - u^2v^2 - 18uv + 4v^3 + 27)(uv - 1)^2 \\
= D(c(x)) \cdot (uv - 1)^2
\]

and so

\[ D(c(x)) = D(c(x)) \cdot (uv - 1)^2. \]

This yields

\[(uv - 1)^2 = 1 \iff uv - 1 = \pm 1 \iff uv = 0 \text{ or } 2.\]

Since \(u, v \in \mathbb{Z}\), we have either \(u = 0\) or \(v = 0\) or obtain a finite number of integral solutions

\[(u, v) = (1, 2), (-1, -2), (2, 1), (-2, -1).\]

Note the case when \(c(x) = x^3 + ux^2 + vx - 1\) yields the equation

\[
D(c(x)) = D(c(x)) \cdot (uv + 1)^2 \iff (uv + 1)^2 = 1 \\
\iff uv + 1 = \pm 1 \\
\iff uv = 0 \text{ or } -2
\]

which gives either \(u = 0\) or \(v = 0\) or the finite number of integral solutions \((u, v) = (-1, 2), (1, -2), (-2, 1), (2, -1).\)

If \(u = 0\) then

\[ c(x) = x^3 + vx + 1 \]
with discriminant equal to

$$-4v^3 - 27$$

and if $v = 0$ then

$$c(x) = x^3 + ux^2 + 1$$

with discriminant equal to

$$-4u^3 - 27.$$  

By [6], the general formula for the discriminant of a cubic field has the form $df^2$ (where $d$ is referred to as a fundamental discriminant). Since the unique quadratic subfield is $\mathbb{Q}(i)$, this implies $d = -4$. Thus, the field discriminant of the cubic field defined by $g(x)$ is of the form

$$-4f^2 = -(2f)^2.$$

This implies the squarefree part of the discriminant of $g(x)$ must be equal to $-1$. Since there exists only finitely many integral solutions to the equation

$$-4u^3 - 27 = -n^2,$$

we cannot have infinitely many nonabelian cubic fields if $u = 0$ or $v = 0$. Therefore, only finitely many choices remain for $u$ and $v$. Equating $k(-x)$ to $g(x)$, only finitely many choices remain for $a$ and $b$, a contradiction. Hence, there exist at most finitely many polynomials

$$f(x) = x^6 + ax^4 + bx^2 + 1$$

irreducible over $\mathbb{Q}$ with the Galois group of $f$ equal to $S_3$ and such that a root of $f(x)$ is a monogenic generator of a sextic field and a root of $x^3 + ax^2 + bx + 1$ is a monogenic generator of a cubic field.

Lastly, we treat the case when the Galois group is $(S_4, -)$. Assume $f(x) = x^6 + ax^4 + bx^2 + 1$ is irreducible over $\mathbb{Q}$ with Galois group $(S_4, -)$ and such that a root of $f(x)$ is
a monogenic generator of a sextic field and a root of \(x^3 + ax^2 + bx \pm 1\) is a monogenic generator of a cubic field. By way of contradiction, assume there are infinitely many such polynomials. According to [6] (p. 330), the discriminant of the polynomial \(f(x)\) cannot be a square in \(\mathbb{Q}\). As the discriminant of \(x^6 + ax^4 + bx^2 - 1\) is

\[
2^6(-27 - 18ab + a^2b^2 + 4a^3 - 4b^3)^2 = [2^3(-27 - 18ab + a^2b^2 + 4a^3 - 4b^3)]^2,
\]

this forces \(f(x) = x^6 + ax^4 + bx^2 + 1\). Moreover, the discriminant of \(f(x)\) is equal to

\[-2^6(27 - 18ab - a^2b^2 + 4a^3 + 4b^3)^2 = -z^2\]

for some integer \(z\) and so the splitting field of \(f(x)\) contains \(i\). Since \(S_4\) contains a unique subgroup of index two, the quadratic subfield \(\mathbb{Q}(i)\) of the splitting field of \(f(x)\) is unique. Moreover, since the group \(S_4\) does not contain a normal subgroup of index three, the cubic subfield defined by \(g(x) = x^3 + ax^2 + bx + 1\) is noncyclic.

Again, by [6], the general formula for the discriminant of a cubic field has the form \(df^2\) (where \(d\) is referred to as a fundamental discriminant). Since the unique quadratic subfield is \(\mathbb{Q}(i)\), this implies \(d = -4\). Thus, the field discriminant of the cubic field defined by \(g(x)\) is of the form

\[-4f^2.\]

Moreover, since \(g(x)\) defines a monogenic field, we must have the discriminant of \(g(x)\) equal to the field discriminant given by the formula \(-4f^2\).

The discriminant of \(g(x)\) is

\[-27 + 18ab + a^2b^2 - 4a^3 - 4b^3\]

which is even if and only if \(a, b\) are both odd. By assumption, a root of \(f(x)\) is a
monogenic generator of a sextic field and so we can apply Lemma 6.2.1 to conclude

\((a, b) \not\equiv (1, 1), (3, 3)(\mod 4)\).

Thus,

\((a, b) \equiv (1, 3) \text{ or } (3, 1)(\mod 4)\).

In both these cases, we have

\[2^2 \parallel -27 + 18ab + a^2b^2 - 4a^3 - 4b^3\]

where \(-27 + 18ab + a^2b^2 - 4a^3 - 4b^3\) is equal to the discriminant of \(g(x)\) and so

\[2^2 \parallel -4f^2\]

Thus, we conclude

\[2 \nmid f\].

By [6] (p. 351), we have the ideal factorization

\[\langle 2 \rangle = \varphi_1\varphi_2^2\]

for distinct prime ideals \(\varphi_1, \varphi_2\).

On the other hand, we can easily check that

\[g(x) \equiv (x + 1)^3(\mod 2)\]

for \(a, b\) odd and so by Dedekind’s Theorem (as \(g(x)\) defines a monogenic field) we must have

\[\langle 2 \rangle = \varphi^3\]

This contradicts the unique factorization into ideals and so no such \(a, b\) exist. Thus,
there are finitely many polynomials 
\[ f(x) = x^6 + ax^4 + bx^2 + 1 \] irreducible over \( \mathbb{Q} \) with
Galois group \((S_4, -)\) such that a root of \( f(x) \) is a monogenic generator of a sextic
field and a root of \( x^3 + ax^2 + bx + 1 \) is a monogenic generator of a cubic field. ■

We now state an important result by Llorente and Nart (see [19] for proof) which
gives the discriminant of a cubic field. In this result, for a prime \( p \) and a nonzero
integer \( m \) we denote the largest integer \( k \) such that \( p^k \mid m \) by \( v_p(m) \).

**Lemma 6.2.6** Let \( f(x) = x^3 - ax + b \in \mathbb{Z}[x] \) be irreducible over \( \mathbb{Z} \). Let

\[ \Delta = 4a^3 - 27b^2 \neq 0. \]

For a prime \( p \) set

\[ s_p = v_p(\Delta) \]

and

\[ \Delta_p = \frac{\Delta}{p^{s_p}}. \]

Suppose further that \( f(x) \) satisfies the simplifying assumption, that is, if \( p \) is a prime
then

\[ v_p(a) < 2 \text{ or } v_p(b) < 3. \]

Let \( \theta \in \mathbb{C} \) be a root of \( f(x) \) and set \( K = \mathbb{Q}(\theta) \). Then

\[
d(K) = sgn(\Delta)2^{\alpha}3^{\frac{1}{3}} \prod_{p > 3} p^{s_p \text{ odd}} \prod_{p > 3} p^{2 \text{ if } v_p(b) \leq v_p(a) \text{ odd}} \]

where

\[
\alpha = \begin{cases} 
3 & \text{if } s_2 \equiv 1 \pmod{2} \\
2 & \text{if } 1 \leq v_2(b) \leq v_2(a) \text{ or } s_2 \equiv 0 \pmod{2} \text{ and } \Delta_2 \equiv 3 \pmod{4} \\
0 & \text{otherwise}
\end{cases}
\]
and

\[
\beta = \begin{cases} 
5 & \text{if } 1 \leq v_3(b) < v_3(a) \\
4 & \text{if } v_3(a) = v_3(b) = 2 \text{ or } \\
3 & \text{if } v_3(a) = v_3(b) = 1 \text{ or } \\
1 & \text{if } 1 = v_3(a) < v_3(b) \text{ or } \\
0 & \text{if } 3 \nmid a \text{ or } \\
& a \equiv 3 \pmod{9}, b \not\equiv 0 \pmod{3} \text{ and } b^2 \not\equiv 4 \pmod{9} \\
& a \equiv 0 \pmod{3}, b \not\equiv 0 \pmod{3}, a \not\equiv 3 \pmod{9} \text{ and } \\
& b^2 \not\equiv a + 1 \pmod{9} \text{ or } \\
& a \equiv 0 \pmod{3}, a \not\equiv 3 \pmod{9} \text{ and } b^2 \equiv a + 1 \pmod{27} \text{ or } \\
& a \equiv 3 \pmod{9}, b^2 \equiv a + 1 \pmod{27} \text{ and } s_3 \equiv 1 \pmod{2} \\
& a \equiv 3 \pmod{9}, b^2 \equiv a + 1 \pmod{27} \text{ and } s_3 \equiv 0 \pmod{2} \\
\end{cases}
\]

We will use the above Lemma to help us prove the following.

**Lemma 6.2.7** For the values of \( d \) specified in column 1 of TABLE 6.2.5, define \( g_d(x) \) as in column 2. Then \( g_d(x) \) is irreducible and the discriminant of the cubic field defined by \( g_d(x) \) is given in column 3.

<table>
<thead>
<tr>
<th>( d \in \mathbb{Z} )</th>
<th>( g_d(x) )</th>
<th>Field Discriminant</th>
</tr>
</thead>
<tbody>
<tr>
<td>( 4d^2 + 2d + 7 ) squarefree</td>
<td>( x^3 + (2d + 2)x^2 + (2d - 1)x - 1 )</td>
<td>( (4d^2 + 2d + 7)^2 )</td>
</tr>
<tr>
<td>( 4d^2 + 2d + 7 ) squarefree</td>
<td>( x^3 - (2d + 2)x^2 + (2d - 1)x + 1 )</td>
<td>( (4d^2 + 2d + 7)^2 )</td>
</tr>
<tr>
<td>( d \equiv 1 \pmod{2}, d &gt; 3, 4d^3 - 27 ) squarefree</td>
<td>( x^3 - dx - 1 )</td>
<td>( 4d^3 - 27 )</td>
</tr>
<tr>
<td>( d \equiv 1 \pmod{2}, d &gt; 3, 4d^3 - 27 ) squarefree</td>
<td>( x^3 - dx + 1 )</td>
<td>( 4d^3 - 27 )</td>
</tr>
<tr>
<td>( d \equiv 1 \pmod{2}, d &gt; 3, 4d^3 - 27 ) squarefree</td>
<td>( x^3 + 2dx^2 + d^2x + 1 )</td>
<td>( 4d^3 - 27 )</td>
</tr>
</tbody>
</table>

**Proof.** The proof of the assertion of the first row of TABLE 6.2.5 was done in [8].
We begin with the proof of the assertion of the second row of TABLE 6.2.5. Assume for \( d \in \mathbb{Z} \) we have \( 4d^2 + 2d + 7 \) squarefree and define

\[
g_d(x) = x^3 - (2d + 2)x^2 + (2d - 1)x + 1.
\]

Since

\[
g_d(1) = -1 \neq 0
\]

and

\[
g_d(-1) = -1 - 4d \neq 0,
\]

by the Rational Root theorem, we deduce \( g_d(x) \) is irreducible over \( \mathbb{Q} \) for \( d \in \mathbb{Z} \).

Now we need to find the field discriminant of the cubic field defined by \( g_d(x) \). First we reduce \( g_d(x) \), that is, eliminate the \( x^2 \) term, by using the transformation

\[
x \rightarrow x + \frac{2d + 2}{3}
\]

followed by the scaling transformation

\[
x \rightarrow \frac{x}{3}.
\]

We obtain the polynomial

\[
h_d(x) = x^3 - 3(4d^2 + 2d + 7)x - (4d + 1)(4d^2 + 2d + 7)
\]

with discriminant \( \Delta \) given by

\[
\Delta = 3^6(4d^2 + 2d + 7)^2.
\]

Now we evaluate the field discriminant of the cubic field defined by \( h_d(x) \) using Lemma
6.2.6, that is,
\[ d(K) = \text{sgn}(\Delta) 2^\alpha 3^\beta \prod_{p > 3} p \prod_{p > 3, p \text{ odd}} p^2. \]

We note that we are using
\[ a = 3(4d^2 + 2d + 7) \]
\[ b = -(4d + 1)(4d^2 + 2d + 7). \]

Consider the prime \( p = 2 \) then
\[ v_2(a) = v_2(3(4d^2 + 2d + 7)) = 0 < 2 \]
\[ v_2(b) = v_2(-(4d + 1)(4d^2 + 2d + 7)) = 0 < 3 \]

and so our polynomial \( h_d(x) \) satisfies the simplifying assumption in Lemma 6.2.6 for \( p = 2 \). We also note that by completing the square we obtain
\[ 4d^2 + 2d + 7 = \frac{(4d + 1)^2 + 27}{4}. \]

By way of contradiction, assume \( 3 \mid 4d^2 + 2d + 7 \). Then \( 3 \mid (4d + 1)^2 + 27 \) which implies \( 3 \mid 4d + 1 \). Hence, we have \( 9 \mid (4d + 1)^2 + 27 \) and so \( 9 \mid 4d^2 + 2d + 7 \), a contradiction as \( 4d^2 + 2d + 7 \) is squarefree. Thus, \( 3 \nmid 4d^2 + 2d + 7 \). Moreover, \( 3 \nmid 4d + 1 \). This implies
\[ v_3(a) = v_3(3(4d^2 + 2d + 7)) = 1 < 2 \]
\[ v_3(b) = v_3(-(4d + 1)(4d^2 + 2d + 7)) = 0 < 3 \]

and so our polynomial \( h_d(x) \) satisfies the simplifying assumption in Lemma 6.2.6 for \( p = 3 \). It remains to show the simplifying assumption is satisfied for \( p > 3 \). Since
$4d^2 + 2d + 7$ is squarefree,

$$v_p(a) = v_p(3(4d^2 + 2d + 7)) = 0 \text{ or } 1 < 2.$$ 

Thus, our polynomial $h_d(x)$ satisfies the simplifying assumption in Lemma 6.2.6 for all primes $p$.

Since $4d^2 + 2d + 7$ is squarefree, $2 \nmid \Delta$ and so

$$s_2 = v_2(\Delta) = 0.$$ 

Moreover,

$$\Delta_2 = \frac{\Delta}{2^0} = \Delta = 3^6(4d^2 + 2d + 7)^2.$$ 

Since $4d^2 + 2d + 7$ is squarefree, it is not congruent to 0 mod 4. Moreover, as squares are either congruent to 0 or 1 mod 4, we deduce

$$\Delta_2 \equiv 1 \mod 4.$$ 

So $\alpha = 0$. Since $3 \nmid 4d^2 + 2d + 7$, we have

$$d \equiv 0, 1 \mod 3.$$ 

We then note for $d \equiv 0, 1 \mod 3$,

$$a = 3(4d^2 + 2d + 7)$$

$$\equiv 3 \mod 9$$
and

\[ b^2 = (4d + 1)^2(4d^2 + 2d + 7)^2 \]
\[ \equiv a + 1 \pmod{27}. \]

Finally,

\[ s_3 = v_3(\Delta) = 6 \]
as \( 3 \nmid 4d^2 + 2d + 7 \) and so

\[ s_3 \equiv 0 \pmod{2}. \]

Hence, \( \beta = 0 \) and so

\[ d(K) = \prod_{\substack{p > 3 \\ s_p \text{ odd}}} p \prod_{\substack{p > 3 \\ 1 \leq v_p(b) \leq v_p(a)}} p^2. \]

Since \( 4d^2 + 2d + 7 \) is squarefree, we deduce

\[ s_p = v_p(\Delta) = v_p(3^6(4d^2 + 2d + 7)^2) = 0 \text{ or } 2 \]

for prime \( p > 3 \). Hence,

\[ d(K) = \prod_{\substack{p > 3 \\ 1 \leq v_p(b) \leq v_p(a)}} p^2 \]
\[ = (4d^2 + 2d + 7)^2 \]

and so the field discriminant of the cubic field defined by \( h_d(x) \), and hence by \( g_d(x) \), is equal to \( (4d^2 + 2d + 7)^2 \).

Now we give the proof of the assertion of the third row of TABLE 6.2.5. Assume for \( d \in \mathbb{Z}, d \equiv 1 \pmod{2}, d > 3 \) we have \( 4d^3 - 27 \) squarefree and define

\[ g_d(x) = x^3 - dx - 1. \]
Since 
\[ g_d(1) = -d \neq 0 \]
and 
\[ g_d(-1) = -2 + d \neq 0, \]
by the Rational Root theorem, we deduce \( g_d(x) \) is irreducible over \( \mathbb{Q} \) for the specified \( d \) above.

Now we need to find the field discriminant of the cubic field defined by \( g_d(x) \). First we note that \( g_d(x) \) is already in reduced form, that is, it does not have an \( x^2 \) term. The discriminant \( \Delta \) of \( g_d(x) \) is given by 
\[ \Delta = 4d^3 - 27. \]

Now we evaluate the field discriminant of the cubic field defined by \( g_d(x) \) using Lemma 6.2.6, that is, 
\[ d(K) = sgn(\Delta)2^2\alpha^3 \prod_{p>3} p^{\nu_p(\Delta)} \prod_{p>3} p^{2\nu_p(\Delta)}. \]

We note that we are using 
\[ a = d \]
\[ b = -1. \]

Consider the prime \( p = 2 \) and recall \( d \equiv 1 \pmod{2} \). Then 
\[ v_2(a) = v_2(d) = 0 < 2 \]
\[ v_2(b) = v_2(-1) = 0 < 3 \]
and so our polynomial \( g_d(x) \) satisfies the simplifying assumption in Lemma 6.2.6 for
\( p = 2. \) Moreover, for \( p \geq 3, \) we have

\[
v_p(b) = v_p(-1) = 0 < 3
\]

and so our polynomial \( g_d(x) \) satisfies the simplifying assumption in Lemma 6.2.6 for all \( p. \)

Since \( 4d^3 - 27 \) is odd, \( 2 \nmid \Delta \) and so

\[
s_2 = v_2(\Delta) = 0.
\]

Moreover,

\[
\Delta_2 = \frac{\Delta}{20} = \Delta = 4d^3 - 27 \equiv 1 \pmod{4}.
\]

So \( \alpha = 0. \)

By way of contradiction, assume \( 3 \mid d. \) Then \( 9 \mid d^3 \) which implies \( 9 \mid 4d^3 - 27, \) a contradiction as \( 4d^3 - 27 \) is squarefree. Thus, \( 3 \nmid d \) and so

\[
3 \nmid a.
\]

Hence, \( \beta = 0 \) and so

\[
d(K) = \prod_{p > 3} p \prod_{p > 3} p^2.
\]
Since $4d^3 - 27$ is squarefree, we deduce

$$s_p = v_p(\Delta) = v_p(4d^3 - 27) = \begin{cases} 
0 & \text{if } p \nmid 4d^3 - 27 \\
1 & \text{if } p \mid 4d^3 - 27 
\end{cases}$$

for prime $p > 3$. Hence,

$$d(K) = (4d^3 - 27) \prod_{\substack{p \mid 3 \\text{ and } \ 1 \leq v_p(b) \leq v_p(a)}} p^2.$$  

Now

$$v_p(b) = v_p(-1) = 0$$

and so

$$d(K) = 4d^3 - 27.$$  

The field discriminant of the cubic field defined by $g_d(x)$ is equal to $4d^3 - 27$.

Now we give the proof of the assertion of the fourth row of TABLE 6.2.5. Assume for $d \in \mathbb{Z}, d \equiv 1 \pmod{2}$, $d > 3$ we have $4d^3 - 27$ squarefree and define

$$g_d(x) = x^3 - dx + 1.$$  

Since

$$g_d(1) = 2 - d \neq 0$$

and

$$g_d(-1) = d \neq 0,$$

by the Rational Root theorem, we deduce $g_d(x)$ is irreducible over $\mathbb{Q}$ for the specified $d$ above.

Now we need to find the field discriminant of the cubic field defined by $g_d(x)$. First we note that $g_d(x)$ is already in reduced form, that is, it does not have an $x^2$ term.
The discriminant \( \Delta \) of \( g_d(x) \) is given by

\[
\Delta = 4d^3 - 27.
\]

Now we evaluate the field discriminant of the cubic field defined by \( g_d(x) \) using Lemma 6.2.6, that is,

\[
d(K) = sgn(\Delta)2^{\alpha_3}3^{\beta} \prod_{p \mid 3} p \prod_{p \mid 3} p^2.
\]

We note that we are using

\[
a = d \quad b = 1.
\]

Consider the prime \( p = 2 \) and recall \( d \equiv 1 \pmod{2} \). Then

\[
\begin{align*}
v_2(a) &= v_2(d) = 0 < 2 \\
v_2(b) &= v_2(1) = 0 < 3
\end{align*}
\]

and so our polynomial \( g_d(x) \) satisfies the simplifying assumption in Lemma 6.2.6 for \( p = 2 \). Moreover, for \( p \geq 3 \), we have

\[
v_p(b) = v_p(1) = 0 < 3
\]

and so our polynomial \( g_d(x) \) satisfies the simplifying assumption in Lemma 6.2.6 for all primes \( p \).

Since \( 4d^3 - 27 \) is odd, \( 2 \nmid \Delta \) and so

\[
s_2 = v_2(\Delta) = 0.
\]
Moreover,

\[ \Delta_2 = \frac{\Delta}{2^0} = \Delta = 4d^3 - 27 \equiv 1 \pmod{4}. \]

So \( \alpha = 0 \).

By way of contradiction, assume \( 3 \mid d \). Then \( 9 \mid d^3 \) which implies \( 9 \mid 4d^3 - 27 \), a contradiction as \( 4d^3 - 27 \) is squarefree. Thus, \( 3 \nmid d \) and so \( 3 \nmid a \).

Hence, \( \beta = 0 \) and so

\[ d(K) = \prod_{p > 3} p \prod_{s_p \text{ odd}} p^2. \]

Since \( 4d^3 - 27 \) is squarefree, we deduce

\[ s_p = v_p(\Delta) = v_p(4d^3 - 27) = \begin{cases} 0 & \text{if } p \nmid 4d^3 - 27 \\ 1 & \text{if } p \mid 4d^3 - 27 \end{cases} \]

for prime \( p > 3 \). Hence,

\[ d(K) = (4d^3 - 27) \prod_{p > 3} p^2. \]

Now

\[ v_p(b) = v_p(1) = 0 \]
and so

$$d(K) = 4d^3 - 27.$$ 

The field discriminant of the cubic field defined by $g_d(x)$ is equal to $4d^3 - 27$.

Lastly we give the proof of the assertion of the fifth row of TABLE 6.2.5. Assume for $d \in \mathbb{Z}, d \equiv 1 \pmod{2}, d > 3$ we have $4d^3 - 27$ squarefree and define

$$g_d(x) = x^3 + 2dx^2 + d^2x + 1.$$ 

Since

$$g_d(1) = d^2 + 2d + 2 \neq 0$$

and

$$g_d(-1) = -d(-2 + d) \neq 0,$$

by the Rational Root theorem, we deduce $g_d(x)$ is irreducible over $\mathbb{Q}$ for the specified $d$ above.

Now we need to find the field discriminant of the cubic field defined by $g_d(x)$. First we reduce $g_d(x)$, that is, eliminate the $x^2$ term, by using the transformation

$$x \to x - \frac{2d}{3}$$

followed by the scaling transformation

$$x \to \frac{x}{3}.$$ 

We obtain the polynomial

$$h_d(x) = x^3 - 3d^2x - 2d^3 + 27.$$
with discriminant $\Delta$ given by

$$\Delta = 3^6(4d^3 - 27).$$

Now we evaluate the field discriminant of the cubic field defined by $h_d(x)$ using Lemma 6.2.6, that is,

$$d(K) = \text{sgn}(\Delta)2^\alpha 3^\beta \prod_{\substack{p > 3 \\text{odd}}} p \prod_{\substack{p > 3 \\text{odd}}} p^2.$$

We note that we are using

$$a = 3d^2$$

$$b = -2d^3 + 27.$$

Consider the prime $p = 2$ then

$$v_2(a) = v_2(3d^2) = 0 < 2$$

$$v_2(b) = v_2(-2d^3 + 27) = 0 < 3$$

and so our polynomial $h_d(x)$ satisfies the simplifying assumption in Lemma 6.2.6 for $p = 2$. By way of contradiction, assume $3 \mid d$. Then $9 \mid d^3$ which implies $9 \mid 4d^3 - 27$, a contradiction as $4d^3 - 27$ is squarefree. Thus, $3 \nmid d$ and so

$$v_3(a) = v_3(3d^2) = 1 < 2$$

and so our polynomial $h_d(x)$ satisfies the simplifying assumption in Lemma 6.2.6 for $p = 3$. Assume $p > 3$. Since

$$\gcd(a, b) = \gcd(3d^2, -2d^3 + 27) = 1,$$
we have either

\[ v_p(a) = 0 < 2 \text{ or } v_p(b) = 0 < 3. \]

In either case, our polynomial \( h_d(x) \) satisfies the simplifying assumption in Lemma 6.2.6 for \( p > 3 \).

Since \( 4d^3 - 27 \) is odd, \( 2 \nmid \Delta \) and so

\[ s_2 = v_2(\Delta) = 0. \]

Moreover,

\[
\Delta_2 \quad = \quad \frac{\Delta}{2^9} \\
\quad = \quad \Delta \\
\quad = \quad 3^6(4d^3 - 27) \\
\quad \equiv \quad 1 \pmod{4}
\]

So \( \alpha = 0 \).

Since \( 3 \nmid d \), we have

\[ d \equiv 1, 2 \pmod{3}. \]

We then note for \( d \equiv 1, 2 \pmod{3} \),

\[ a = 3d^2 \equiv 3 \pmod{9} \]

and

\[ b^2 \equiv a + 1 \pmod{27}. \]

Finally,

\[ s_3 = v_3(\Delta) = 6 \]
as $3 \nmid 4d^3 - 27$ and so

$$s_3 \equiv 0 \pmod{2}.$$ 

Hence, $\beta = 0$ and so

$$d(K) = \prod_{p > 3} p \prod_{s_p \text{ odd}} p^2.$$ 

Since $4d^3 - 27$ is squarefree, we deduce

$$s_p = v_p(\Delta) = v_p(3^6(4d^3 - 27)) = \begin{cases} 0 & \text{if } p \nmid 4d^3 - 27 \\ 1 & \text{if } p \mid 4d^3 - 27 \end{cases}$$ 

for prime $p > 3$. Hence,

$$d(K) = (4d^3 - 27) \prod_{p > 3} p^2.$$ 

Recall we have either

$$v_p(a) = 0 \text{ or } v_p(b) = 0$$ 

for prime $p > 3$. Thus,

$$d(K) = 4d^3 - 27$$

and so the field discriminant of the cubic field defined by $h_d(x)$, and hence by $g_d(x)$, is equal to $4d^3 - 27$. ■

### 6.3 Main Theorem

We are now ready to prove our main theorem given below.

**Theorem 6.3.1** For those values of $d$ specified in column 1 of TABLE 6.3.6 define $f_d(x)$ as in column 2. Let $\theta_d$ be a root of $f_d(x)$. Let $K_d = \mathbb{Q}(\theta_d)$. Then there are infinitely many $d$ such that
(i) \([K_d : \mathbb{Q}] = 6\),

(ii) The Galois group of \(f_d\) is as given in column 3 of TABLE 6.3.6,

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

Table 6.3.6: Lifting Monogenic Cubic Fields - Theorem 6.3.1

<table>
<thead>
<tr>
<th>(d \in \mathbb{Z})</th>
<th>(f_d(x))</th>
<th>(\text{Gal}(f_d))</th>
</tr>
</thead>
<tbody>
<tr>
<td>(4d^2 + 2d + 7) squarefree</td>
<td>(x^6 + (2d + 2)x^4 + (2d - 1)x^2 - 1)</td>
<td>(A_4)</td>
</tr>
<tr>
<td>(4d^2 + 2d + 7) squarefree</td>
<td>(x^6 - (2d + 2)x^4 + (2d - 1)x^2 + 1)</td>
<td>(A_4 \times C_2)</td>
</tr>
<tr>
<td>(d \equiv 1) (mod 2), (d &gt; 3, 4d^3 - 27) squarefree</td>
<td>(x^6 - dx^2 - 1)</td>
<td>((S_4, +))</td>
</tr>
<tr>
<td>(d \equiv 1) (mod 2), (d &gt; 3, 4d^3 - 27) squarefree</td>
<td>(x^6 - dx^2 + 1)</td>
<td>(S_4 \times C_2)</td>
</tr>
<tr>
<td>(d \equiv 1) (mod 2), (d &gt; 3, 4d^3 - 27) squarefree</td>
<td>(x^6 + 2dx^4 + d^2x^2 + 1)</td>
<td>(D_6)</td>
</tr>
</tbody>
</table>

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

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

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

(vi) The Galois group of \(f\) is isomorphic to \(C_6, S_3\) or \((S_4, -)\).

Proof. We first prove statements (i), (ii) and (iii). The proof of the assertion of statements (i), (ii) and (iii) for the first row of TABLE 6.3.6 was done in [8].

We now give the proof of the assertion of statements (i), (ii) and (iii) for the second row of TABLE 6.3.6. Assume \(d \in \mathbb{Z}\) with \(4d^2 + 2d + 7\) squarefree. We note that, by Nagel’s Theorem (see Theorem 6.1.10), there exists infinitely many values of \(d\) such that \(4d^2 + 2d + 7\) is squarefree. Set

\[g_d(x) = x^3 - (2d + 2)x^2 + (2d - 1)x + 1\]
and let $\alpha_d \in \mathbb{C}$ be a root of $g_d(x)$. Set $C_d = \mathbb{Q}(\alpha_d)$. By the Rational Root theorem, $g_d(x)$ is irreducible over $\mathbb{Q}$ so that $C_d$ is a cubic field. The discriminant of $g_d(x)$ is equal to

$$(4d^2 + 2d + 7)^2$$

and by Lemma 6.2.7, this polynomial discriminant is equal to the field discriminant of $C_d$. That is,

$$D(g_d(x)) = d(C_d) = (4d^2 + 2d + 7)^2$$

and so

$$(\text{ind}(\alpha_d))^2 = \frac{D(g_d)}{d(C_d)} = 1.$$ 

By Theorem 5.1.8, we deduce that $\{1, \alpha_d, \alpha_d^2\}$ is a power basis of $C_d$. Let

$$f_d(x) = x^6 - (2d + 2)x^4 + (2d - 1)x^2 + 1$$

and let $\theta_d$ be a root of $f_d(x)$ and set $K = \mathbb{Q}(\theta_d)$. By Lemma 6.2.4, $f_d(x)$ is irreducible over $\mathbb{Q}$, $[K_d : \mathbb{Q}] = 6$ and the Galois group of $f_d(x)$ is equal to $A_4 \times C_2$. Since the cubic subfields $C_d$ have distinct discriminants, they are distinct fields and so the sextic fields $K_d$ are also distinct. By Lemma 6.2.1, $K_d$ is monogenic with power basis $\{1, \theta_d, \theta_d^2, \theta_d^3, \theta_d^4, \theta_d^5\}$ if and only if

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

and so there exists infinitely many $d \in \mathbb{Z}$ with $4d^2 + 2d + 7$ squarefree such that $K_d$ is monogenic with power basis $\{1, \theta_d, \theta_d^2, \theta_d^3, \theta_d^4, \theta_d^5\}$. This finishes the proofs of statements (i), (ii) and (iii) for this case.

We now give the proof of the assertion of statements (i), (ii) and (iii) for the third row of TABLE 6.3.6. Assume $d \equiv 1 \pmod{2}$, $d > 3$, $d \in \mathbb{Z}$ with $4d^3 - 27$ squarefree. We note that, by Erdös, there exists infinitely many values of $d$ such that $4d^3 - 27$ is
squarefree. Set
\[ g_d(x) = x^3 - dx - 1 \]
and let \( \alpha_d \in \mathbb{C} \) be a root of \( g_d(x) \). Set \( C_d = \mathbb{Q}(\alpha_d) \). By the Rational Root theorem, \( g_d(x) \) is irreducible over \( \mathbb{Q} \) so that \( C_d \) is a cubic field. The discriminant of \( g_d(x) \) is equal to
\[ 4d^3 - 27 \]
and by Lemma 6.2.7, this polynomial discriminant is equal to the field discriminant of \( C_d \). That is,
\[ D(g_d(x)) = d(C_d) = 4d^3 - 27 \]
and so
\[ (\text{ind}(\alpha_d))^2 = \frac{D(g_d)}{d(C_d)} = 1. \]

By Theorem 5.1.8, we deduce that \( \{1, \alpha_d, \alpha_d^2\} \) is a power basis of \( C_d \). Let \( f_d(x) = x^6 - dx^2 - 1 \)
and let \( \theta_d \) be a root of \( f_d(x) \) and set \( K = \mathbb{Q}(\theta_d) \). By Lemma 6.2.4, \( f_d(x) \) is irreducible over \( \mathbb{Q} \), \( [K_d : \mathbb{Q}] = 6 \) and the Galois group of \( f_d(x) \) is equal to \((S_4, +)\). Since the cubic subfields \( C_d \) have distinct discriminants, they are distinct fields and so the sextic fields \( K_d \) are also distinct. By Lemma 6.2.2, \( K_d \) is monogenic with power basis \( \{1, \theta_d, \theta_d^2, \theta_d^3, \theta_d^4, \theta_d^5\} \) if and only if
\[ (a, b) = (0, -d) \not\equiv (0, 0), (2, 1), (2, 2), (1, 3), (3, 1), (3, 2) \pmod{4} \]
and so there exists infinitely many \( d \equiv 1 \pmod{2}, \ d > 3, \ d \in \mathbb{Z} \) with \( 4d^3 - 27 \) squarefree such that \( K_d \) is monogenic with power basis \( \{1, \theta_d, \theta_d^2, \theta_d^3, \theta_d^4, \theta_d^5\} \). This finishes the proofs of statements (i), (ii) and (iii) for this case.
We now give the proof of the assertion of statements (i), (ii) and (iii) for the fourth row of TABLE 6.3.6. Assume \( d \equiv 1 \pmod{2} \), \( d > 3 \), \( d \in \mathbb{Z} \) with \( 4d^3 - 27 \) squarefree.

We note that, by Erdős, there exists infinitely many values of \( d \) such that \( 4d^3 - 27 \) is squarefree. Set

\[
g_d(x) = x^3 - dx + 1
\]

and let \( \alpha_d \in \mathbb{C} \) be a root of \( g_d(x) \). Set \( C_d = \mathbb{Q}(\alpha_d) \). By the Rational Root theorem, \( g_d(x) \) is irreducible over \( \mathbb{Q} \) so that \( C_d \) is a cubic field. The discriminant of \( g_d(x) \) is equal to

\[
4d^3 - 27
\]

and by Lemma 6.2.7, this polynomial discriminant is equal to the field discriminant of \( C_d \). That is,

\[
D(g_d(x)) = d(C_d) = 4d^3 - 27
\]

and so

\[
(ind(\alpha_d))^2 = \frac{D(g_d)}{d(C_d)} = 1.
\]

By Theorem 5.1.8, we deduce that \( \{1, \alpha_d, \alpha_d^2\} \) is a power basis of \( C_d \). Let

\[
f_d(x) = x^6 - dx^2 + 1
\]

and let \( \theta_d \) be a root of \( f_d(x) \) and set \( K = \mathbb{Q}(\theta_d) \). By Lemma 6.2.4, \( f_d(x) \) is irreducible over \( \mathbb{Q} \), \( [K_d : \mathbb{Q}] = 6 \) and the Galois group of \( f_d(x) \) is equal to \( S_4 \times C_2 \). Since the cubic subfields \( C_d \) have distinct discriminants, they are distinct fields and so the sextic fields \( K_d \) are also distinct. By Lemma 6.2.1, \( K_d \) is monogenic with power basis \( \{1, \theta_d, \theta_d^2, \theta_d^3, \theta_d^4, \theta_d^5\} \) if and only if

\[
(a, b) = (0, -d) \not\equiv (0, 2), (1, 1), (2, 0), (2, 2), (3, 3) \pmod{4}
\]
and so there exists infinitely many \( d \equiv 1 \pmod{2}, \ d > 3, \ d \in \mathbb{Z} \) with \( 4d^3 - 27 \) squarefree such that \( K_d \) is monogenic with power basis \( \{1, \theta_d, \theta_d^2, \theta_d^3, \theta_d^4, \theta_d^5\} \). This finishes the proofs of statements (i), (ii) and (iii) for this case.

We now give the proof of the assertion of statements (i), (ii) and (iii) for the fifth row of TABLE 6.3.6. Assume \( d \equiv 1 \pmod{2}, \ d > 3, \ d \in \mathbb{Z} \) with \( 4d^3 - 27 \) squarefree. We note that, by Erdös, there exists infinitely many values of \( d \) such that \( 4d^3 - 27 \) is squarefree. Set

\[
g_d(x) = x^3 + 2dx^2 + d^2x + 1
\]

and let \( \alpha_d \in \mathbb{C} \) be a root of \( g_d(x) \). Set \( C_d = \mathbb{Q}(\alpha_d) \). By the Rational Root theorem, \( g_d(x) \) is irreducible over \( \mathbb{Q} \) so that \( C_d \) is a cubic field. The discriminant of \( g_d(x) \) is equal to

\[
4d^3 - 27
\]

and by Lemma 6.2.7, this polynomial discriminant is equal to the field discriminant of \( C_d \). That is,

\[
D(g_d(x)) = d(C_d) = 4d^3 - 27
\]

and so

\[
(ind(\alpha_d))^2 = \frac{D(g_d)}{d(C_d)} = 1.
\]

By Theorem 5.1.8, we deduce that \( \{1, \alpha_d, \alpha_d^2\} \) is a power basis of \( C_d \). Let

\[
f_d(x) = x^6 + 2dx^4 + d^2x^2 + 1
\]

and let \( \theta_d \) be a root of \( f_d(x) \) and set \( K = \mathbb{Q}(\theta_d) \). By Lemma 6.2.4, \( f_d(x) \) is irreducible over \( \mathbb{Q}, \ [K_d : \mathbb{Q}] = 6 \) and the Galois group of \( f_d(x) \) is equal to \( D_6 \). Since the cubic subfields \( C_d \) have distinct discriminants, they are distinct fields and so the sextic fields \( K_d \) are also distinct. By Lemma 6.2.1, \( K_d \) is monogenic with power basis
\{1, \theta_d, \theta_d^2, \theta_d^3, \theta_d^4, \theta_d^5\} \text{ if and only if}

(a, b) = (2d, d^2) \neq (0, 2), (1, 1), (2, 0), (2, 2), (3, 3) \pmod{4}

and so there exists infinitely many \(d \equiv 1 \pmod{2}, d > 3, d \in \mathbb{Z}\) with \(4d^3 - 27\) squarefree such that \(K_d\) is monogenic with power basis \(\{1, \theta_d, \theta_d^2, \theta_d^3, \theta_d^4, \theta_d^5\}\). This finishes the proofs of statements (i), (ii) and (iii) for this case and hence for the theorem. It remains to show the proofs of statements (iv), (v) and (vi). These statements follow from Lemma 6.2.5 and the proof is complete.

\section*{6.4 Future Research}

We note that in this chapter we were looking at monogenic cubic fields defined by cubic polynomials of the form \(x^3 + ax^2 + bx \pm 1\). However, it is not necessary (in some cases) for the constant term of this cubic polynomial to be equal to \(\pm 1\). On the other hand, we suspect we won’t obtain any new sextic Galois groups and the analysis would be difficult. But this would need further investigation and proof in order to confirm our suspicions. For example, consider the general cubic polynomial

\(g(x) = x^3 + ax^2 + bx + c \in \mathbb{Z}[x]\)

with discriminant equal to

\[D(g) = -27c^2 + 18cab + a^2b^2 - 4a^3c - 4b^3.\]

We then wish to lift \(g(x)\) to obtain the sextic polynomial

\(f(x) = x^6 + ax^4 + bx^2 + c \in \mathbb{Z}[x]\)
whose discriminant is equal to

\[ D(f) = -64c(27c^2 - 18c - a^2b^2 + 4a^3c + 4b^3)^2. \]

For \((a, b, c) = (-3, 2, -2)\),

\[ g(x) = x^3 - 3x^2 + 2x - 2 \]

defines a monogenic cubic field \(C\) whose Galois group is \(S_3\) and

\[ f(x) = x^6 - 3x^4 + 2x^2 - 2 \]

defines a monogenic sextic field \(K\) whose Galois group is \(S_4 \times C_2\). Therefore, this lifting technique for obtaining monogenic sextics still applies to a constant term other than \(\pm 1\) but we remain in one of our five original Galois groups. It would be interesting to know what constant terms do yield monogenic sextic fields via lifting and be able to parametrize such constants.

It would also be an interesting study to try this lifting technique on quartics. That is, consider the general reduced quartic polynomial

\[ g(x) = x^4 + ax^2 + bx + c \in \mathbb{Z}[x] \]

defining a monogenic quartic field. We then wish to lift \(g(x)\) to obtain the octic polynomial

\[ f(x) = x^8 + ax^4 + bx^2 + c \in \mathbb{Z}[x] \]

defining a monogenic octic field. We would then like to parametrize \(a, b, c\) and determine what type of Galois groups are obtained and if there exist infinitely many or finitely many such octic fields. It may be useful to begin with a constant term of \(\pm 1\) to simplify the algebra when investigating this problem. For example, for
\[(a, b, c) = (2, 1, -1),\]
\[g(x) = x^4 + 2x^2 + x - 1\]
defines a monogenic quartic field whose Galois group is \(S_4, -\) and
\[f(x) = x^8 + 2x^4 + x^2 - 1\]
defines a monogenic octic field whose Galois group (in transitive form) is 6T44. Therefore, the technique of lifting monogenic quartics to monogenic octics still applies and it would be an interesting study to see what octics can be obtained this way. However, there are fifty possible Galois groups for an octic polynomial and the algebra would be more intense.
Chapter 7

Intersective Polynomials with
Galois Group $D_5$

We now illustrate another application that can be obtained from a parametric family of polynomials (using both our own and already established constructions). Such a family may yield an infinite number of intersective polynomials. Again, such a characterization is rare and obtaining an infinite number of such polynomials proves to be of great significance in studies with a long history.

**Definition 7.0.1** A polynomial $f(x)$ with integer coefficients is said to be intersective if it has a root modulo $m$ for all positive integers $m$.

Equivalently, $f(x)$ has a root in the field of $p$-adic numbers $\mathbb{Q}_p$ for all primes $p$. We say $f(x)$ is nontrivially intersective if it is intersective but has no rational root. Henceforth in this chapter, our polynomials are nontrivially intersective.

Examples of intersective polynomials in general seem to be scarce. A single example of an intersective polynomial with Galois group $D_5$ (another notation for this group is $D_{10}$) is given in [32]. We will make use of his method given in [31] (see Proposition 2.1) when we construct intersective polynomials.

In particular, in this chapter, we give an infinite family of intersective polynomials with Galois group $D_5$. We do so by making use of a parametric family of quintic polynomials with Galois group $D_5$ studied in [18] and Sonn’s method given in [31]. These polynomials give rise to monogenic quintic fields. While the property of monogeneity is not necessary when constructing intersective polynomials, it is helpful when dealing with parametric families.
However, as stated, monogeneity is not required for a polynomial to be intersective. For example, consider dihedral quintic trinomials $x^5 + ax + b$ where $a, b \in \mathbb{Q}$. A parametrization of these polynomials was given in [28]. It was shown in [36] that the quintic fields defined by these polynomials have a common index divisor of two, so that none of these fields are monogenic. Nevertheless, some of them give rise to intersective polynomials. For example, using Sonn’s method of constructing intersective polynomials, the polynomial

$$f(x) = x^5 + 11x + 44$$

with Galois group $D_5$ gives rise to the intersective polynomial

$$(x^5 + 11x + 44)(x^2 + 2).$$

In order to apply this method, certain conditions (described later) must be met. If we try to apply the method without these conditions being satisfied, the method may give rise to non-intersective polynomials. For example, using this method (without having these certain conditions being satisfied) on the polynomial

$$f(x) = x^5 - 5x + 12$$

with Galois group $D_5$ gives rise to the polynomial

$$(x^5 - 5x + 12)(x^2 + 10),$$

which is not intersective (since it has no root modulo 25). We will see that the reason for this is due to the fact that the decomposition group of the single ideal lying above 5 in the splitting field of $f(x)$ is all of $D_5$. 

172
The purpose of this chapter is to illustrate another application to constructing parametric families of polynomials and the usefulness in having monogeneity in dealing with such families.

## 7.1 Preliminaries

We begin with a definition from Ideal theory.

**Definition 7.1.1** Let $L/K$ be a Galois extension of number fields and let $O_L, O_K$ denote the ring of integers of $L$ and $K$, respectively. A prime ideal $\mathfrak{p}$ of $O_K$ is said to be ramified in $O_L$ (or in $L/K$) if the prime ideal factorization

$$\mathfrak{p}O_L = \mathfrak{p} = \mathfrak{p}_1^{e_1} \mathfrak{p}_2^{e_2} \cdots \mathfrak{p}_r^{e_r},$$

for distinct prime ideals $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_r$ in $O_L$, has some $e_i$ greater than 1. If every $e_i$ equals 1 then we say $\mathfrak{p}$ is unramified in $O_L$ (or in $L/K$).

Moreover, assume $p$ is a rational prime (and hence $(p)$ is a prime ideal of $O_K$) and assume $P$ is a prime ideal of $O_L$. We say $P$ lies over (or lies above) $p$ in $L/K$ if

$$P \mid (p)O_L \Leftrightarrow P \mid (p).$$

Next we state an important result by P. Erdös (see [12]).

**Theorem 7.1.2** Let $f(x)$ be a polynomial with integer coefficients whose highest common factor is 1 and assume the highest coefficient of $f(x)$ is positive. Let $n$ denote the degree of $f(x)$ and assume $n \geq 3$. If $f(x)$ is not divisible by the $(n - 1)^{st}$ power of a linear polynomial with integer coefficients then there are infinitely many positive integers $k$ for which $f(k)$ is $(n - 1)^{st}$ power free.

We illustrate Erdös’ theorem with an example.
Example 7.1.3 Assume

\[
f(x) = 4x^3 + 28x^2 + 24x + 47 \in \mathbb{Z}
\]

whose coefficients have a highest common factor of 1 and whose degree \( n = 3 \). By the Rational Root theorem, \( f(x) \) is irreducible over \( \mathbb{Z} \) and so \( f(x) \) is not divisible by a square power of a linear polynomial with integer coefficients. Thus, by Erdős’ theorem, we conclude that there exist infinitely many positive integers \( k \) for which \( f(k) \) is squarefree.

Remark 7.1.4 From the above example, this implies there exist infinitely many positive integers \( b \) for which

\[
f(b) = -(4b^3 + 28b^2 + 24b + 47)
\]

is squarefree.

Recall a polynomial \( f(x) \) with integer coefficients is said to be intersective if it has a root modulo \( m \) for all positive integers \( m \) or equivalently, \( f(x) \) has a root in the field of \( p \)-adic numbers \( \mathbb{Q}_p \) for all primes \( p \). We say \( f(x) \) is nontrivially intersective if it is intersective but has no rational root.

We note that if \( f(x) \) is intersective then \( f(x) \) cannot be irreducible over \( \mathbb{Q} \). This follows from the fact that if \( f(x) \) is irreducible over \( \mathbb{Q} \) then there exists a prime number \( p \) for which the congruence

\[
f(x) \equiv 0 \pmod{p}
\]

cannot be solved in \( \mathbb{Z} \) (see Proposition 1.3, [3]).

The existence of intersective polynomials depends on properties of their Galois group. Let \( L \) denote the splitting field of \( f(x) \). In [2], the authors give a simple condition to
decide whether or not a polynomial is intersective. This condition can also be found in [31] (see Proposition 2.1) but the author also gives a method for constructing such polynomials. However, in order to apply this method, we must check to see if the following conditions are satisfied.

1. The Galois group of \( f \) is the union of conjugates of \( n \) proper subgroups.
2. The intersection of all the conjugates is trivial.
3. Every decomposition group \( G(\wp) \) for \( \wp \) a prime ideal in \( L \) is contained in a conjugate of one of these proper subgroups.

Note that \( G(\wp) \) is the set of elements \( \sigma \) in the Galois group of \( f \) such that \( \sigma(\wp) = \wp \) for \( \wp \) a prime ideal in \( L \).

Now we introduce the following definition which will enable us to check if the above conditions hold for a given polynomial.

**Definition 7.1.5** A group is \( n \)-coverable if it is the union of \( n \) conjugacy classes of proper subgroups.

It follows that the above conditions hold if the Galois group of \( f \) is \( n \)-coverable and every decomposition group is cyclic. Then having checked this condition, we apply the method given in [31] to construct intersective polynomials. That is, it remains to find a set of \( n \) monic polynomials with integer coefficients defining those subfields of \( L \) corresponding to the \( n \) chosen proper subgroups. The product of these polynomials will then be intersective.

If we have the property of monogeneity, then we can employ a well known theorem of Dedekind on ideal factorization to assist with the study of the decomposition groups. We will look at this theorem as well as some more facts about ideal factorization in number fields in the following section.
7.2 Important Lemmas

We use the following notation in our first lemma of this section. Let $K$ and $F$ be algebraic number fields and let $\mathcal{O}_K$ denote the ring of integers of $K$. The proof of our first Lemma can be found in [23] (see Corollary 4.100) and note that we only state the part of the proposition that we will be using.

**Lemma 7.2.1** Let $K/F$ be a Galois extension of number fields with $\mathfrak{p}$ a prime $\mathcal{O}_K$-ideal. If $\mathfrak{p}$ is unramified in $K/F$ then the decomposition group of $\mathfrak{p}$ is cyclic.

Our next proposition concerns the factorization of primes in a composite of two extensions of the same field (see p. 159, [27]). For notation, $K, K_1$ and $K_2$ denote algebraic number fields and $\mathcal{O}_K$ denotes the ring of integers of $K$.

**Lemma 7.2.2** If $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$ unramified in both $K_1/K$ and $K_2/K$ then it is also unramified in the composite extension $K_1K_2/K$.

Note that the contrapositive of Lemma 7.2.2 then states that if $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$ ramified in the composite extension $K_1K_2/K$ then $\mathfrak{p}$ is ramified in either $K_1/K$ or $K_2/K$.

For our last lemma, we use the notation $\text{irr}_\mathbb{Q}(\theta)$ to denote the monic minimal polynomial in $\mathbb{Z}[x]$ of the algebraic integer $\theta$. In addition, recall we used the notation $\text{ind}(\theta)$ to denote the index of $\theta$ as defined previously by the equation

$$\text{ind}(\theta) = \sqrt{\frac{D(\theta)}{d(K)}}$$

where $D(\theta)$ is the polynomial discriminant of $\text{irr}_\mathbb{Q}(\theta)$ and $d(K)$ is the field discriminant of $K = \mathbb{Q}(\theta)$. The following lemma is also known as Dedekind’s Theorem and can be found on p. 257, [1] (see Theorem 10.5.1).
Lemma 7.2.3 Let $K = \mathbb{Q}(\theta)$ be an algebraic number field with $\theta \in O_K$, the ring of integers of $K$. Let $p$ be a rational prime. Let

$$f(x) = \text{irr}_{\mathbb{Q}}(\theta) \in \mathbb{Z}[x].$$

Let $f(x) \mapsto \overline{f}(x)$ denote the natural map $\mathbb{Z}[x] \to \mathbb{Z}_p[x]$ where $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$ such that

$$\overline{f}(x) = g_1(x)^{e_1} g_2(x)^{e_2} \cdots g_r(x)^{e_r}$$

where $g_1(x), g_2(x), \ldots, g_r(x)$ are distinct monic irreducible polynomials in $\mathbb{Z}_p[x]$ and $e_1, e_2, \ldots, e_r$ are positive integers. For $i = 1, 2, \ldots, r$, let $f_i(x)$ be any monic polynomial of $\mathbb{Z}[x]$ such that

$$\overline{f}_i = g_i$$

and

$$\deg(f_i) = \deg(g_i).$$

Set

$$P_i = \langle p, f_i(\theta) \rangle$$

for $i = 1, 2, \ldots, r$. If $\text{ind}(\theta) \not\equiv 0 \pmod{p}$ then $P_1, P_2, \ldots, P_r$ are distinct prime ideals of $O_K$ with

$$\langle p \rangle = P_1^{e_1} P_2^{e_2} \cdots P_r^{e_r}$$

and

$$N(P_i) = p^{\deg(f_i)}$$

for $i = 1, 2, \ldots, r$. 
7.3 Main Theorem

Theorem 7.3.1 There exist infinitely many integers $b$ such that

$$d_b = -4b^3 - 28b^2 - 24b - 47$$

is squarefree. Let $b$ be such an integer. If we set

$$f_b(x) = x^5 - 2x^4 + (b + 2)x^3 - (2b + 1)x^2 + bx + 1$$

then the polynomial

$$g_b(x) = f_b(x)(x^2 - d_b)$$

is intersective and has Galois group $D_5$. Moreover, for infinitely many of the integers $b$ for which $d_b$ is squarefree, the splitting fields of $g_b(x)$ are distinct.

Proof. By Remark 7.1.4, there are infinitely many integers $b$ such that

$$d_b = -4b^3 - 28b^2 - 24b - 47$$

is squarefree.

In [18], it is proved that the polynomial $f_b(x)$ is irreducible over $\mathbb{Q}$ for all integers $b$ (see Lemma 5.1) and if $d_b$ is squarefree then the Galois group of $f_b$ is isomorphic to the dihedral group $D_5$ (see Lemma 5.4). Using the notation of Lemma 7.2.3, this implies

$$f_b(x) = \text{irr}_{\mathbb{Q}}(\theta) \in \mathbb{Z}[x].$$

Moreover, assuming $d_b$ is squarefree, the quadratic subfield of the splitting field of $f_b(x)$ is $\mathbb{Q}(\sqrt{d_b})$ with field discriminant $d_b$ (see Lemma 5.5). Lastly, if $\theta$ is a root of $f_b(x)$ then $\mathbb{Q}(\theta)$ has field discriminant $d_b^2$ and is monogenic with ring of integers $\mathbb{Z}[\theta]$ and there are infinitely many of these distinct fields $\mathbb{Q}(\theta)$ (see Theorem 5.2).
Let $L$ denote the splitting field of $f_b(x)$. Let $\theta$ denote a root of $f_b$ and let $K = \mathbb{Q}(\theta)$. Let $O_L, O_K$ denote the ring of integers of $L$ and $K$, respectively.

It was noted in [32] that $D_5$ is 2-coverable with a subgroup of order 5 and a subgroup of order 2. So we now must show that the decomposition group $G(\wp)$ is cyclic for each prime ideal $\wp$ in the splitting field $L$ of $f_b(x)$. If $\wp$ is unramified, then by Lemma 7.2.1, $G(\wp)$ is cyclic.

Assume $p$ is a rational prime and assume $\wp$ is a prime ideal in $L$. Also assume $\wp$ is ramified in $L$ and $\wp$ lies above $p$. Note that the proper subgroups of $D_5$ have order 1, 2 or 5. Clearly the trivial subgroup is cyclic. Moreover, orders 2 and 5 are prime numbers and hence the subgroups of these orders must be cyclic. Since the Galois group of $f_b$ is isomorphic to $D_5$, $G(\wp)$ is a proper subgroup of $D_5$ if and only if $G(\wp)$ is cyclic. As the Galois group of $f_b$ acts transitively on the set of prime ideals in $L$ lying above $p$, this implies for any prime ideals $P, P'$ in $L$ lying above $p$, there exists $\sigma$ in the Galois group of $f_b$ such that

$$\sigma(P) = P'.$$

So we deduce that $G(\wp)$ is a proper subgroup of $D_5$ if there are at least two prime ideals in $L$ lying above $p$. We will show that this is the case.

By way of contradiction, assume there is only one prime ideal in $L$ lying above $p$, namely $\wp$. Firstly, since $L$ is the splitting field of $f_b$, $L$ must be the compositum of $K = \mathbb{Q}(\theta)$ and $\mathbb{Q}(\sqrt{d_b})$. By the contrapositive of Lemma 7.2.2, this implies $\wp$ must ramify in at least one of these fields. Recall that the field discriminant of $K$ is $d^2_b$ and the field discriminant of $\mathbb{Q}(\sqrt{d_b})$ is $d_b$. Since these field discriminants contain the same prime factors, it follows that $\langle p \rangle$ must ramify in both of these fields and in particular $K$. Hence, since only one prime ideal $\wp$ in $L$ lies above $p$, it follows that only one prime ideal in $K$ lies above $p$. Moreover,

$$\langle p \rangle = P_1^{e_1}.$$
for a prime ideal $P_1$ of $O_K$ and positive integer $e_1 > 1$.

Secondly, $K = \mathbb{Q}(\theta)$ is monogenic with ring of integers $O_K = \mathbb{Z}[\theta]$, and so we have

$$ind(\theta) = \pm 1$$

so that

$$ind(\theta) \not\equiv 0 \pmod{p}.$$ 

Therefore, we can apply Lemma 7.2.3 and conclude that the only possible factorization of $f_b(x)$ modulo $p$, consistent with the previous statements about the factorization of a ramified ideal $(p)$, leads to $r = 1$ and $e_1 = 5$ so that

$$f_b(x) \equiv (x + t)^5 \pmod{p},$$

where $t \in \mathbb{Z}$. Equating each coefficient of $f_b(x) - (x + t)^5$ to zero modulo $p$ gives us a set of congruences from which we will derive a contradiction. These congruences are as follows:

<table>
<thead>
<tr>
<th>Coefficient of</th>
<th>Congruence</th>
</tr>
</thead>
<tbody>
<tr>
<td>$x^4$</td>
<td>$-2 - 5t \equiv 0 \pmod{p}$</td>
</tr>
<tr>
<td>$x^3$</td>
<td>$b + 2 - 10t^2 \equiv 0 \pmod{p}$</td>
</tr>
<tr>
<td>$x^2$</td>
<td>$-2b - 1 - 10t^3 \equiv 0 \pmod{p}$</td>
</tr>
<tr>
<td>$x$</td>
<td>$b - 5t^4 \equiv 0 \pmod{p}$</td>
</tr>
<tr>
<td>$x^0$</td>
<td>$1 - t^5 \equiv 0 \pmod{p}$</td>
</tr>
</tbody>
</table>

The first and last congruences imply

$$p \mid -2 - 5t$$

and

$$p \mid 1 - t^5.$$
From the identity

\[(625t^4 - 250t^3 + 100t^2 - 40t + 16)(-2 - 5t) - 5^5(1 - t^5) = -7 \cdot 11 \cdot 41\]

we deduce that the prime \( p \) must be one of 7, 11 or 41.

Suppose \( p = 7 \). Then

\[-2 - 5t \equiv 0 \pmod{7}\]

implies

\[t \equiv 1 \pmod{7}.
\]

Since \( \langle p \rangle = \langle 7 \rangle \) is ramified in \( O_K \) it follows that

\[d_b \equiv 0 \pmod{7}\]

and so

\[b \equiv 4 \pmod{7}.
\]

However, the congruence

\[b + 2 - 10t^2 \equiv 0 \pmod{7}\]

does not hold if

\[\begin{cases} 
  t \equiv 1 \pmod{7} \\
  b \equiv 4 \pmod{7}.
\end{cases} \]

Therefore, \( p \neq 7 \).

Now assume \( p = 11 \). Then

\[-2 - 5t \equiv 0 \pmod{11}\]

implies

\[t \equiv 4 \pmod{11}.
\]
Since \( \langle p \rangle = \langle 11 \rangle \) is ramified in \( \mathcal{O}_K \) it follows that
\[
d_b \equiv 0 \pmod{11}
\]
and so
\[
b \equiv 4, 7 \pmod{11}.
\]

We omit the case
\[
\begin{align*}
  t &\equiv 4 \pmod{11} \\
  b &\equiv 4 \pmod{11}
\end{align*}
\]
as
\[
d_b = 0 \pmod{11^2}.
\]

Moreover, the congruence
\[
b + 2 - 10t^2 \equiv 0 \pmod{11}
\]
does not hold if
\[
\begin{align*}
  t &\equiv 4 \pmod{11} \\
  b &\equiv 7 \pmod{11}
\end{align*}
\]
Therefore, \( p \neq 11 \).

Therefore, we must have \( p = 41 \). Then
\[
-2 - 5t \equiv 0 \pmod{41}
\]
implies
\[
t \equiv 16 \pmod{41}.
\]

Since \( \langle p \rangle = \langle 41 \rangle \) is ramified in \( \mathcal{O}_K \) it follows that
\[
d_b \equiv 0 \pmod{41}
\]
and so

\[ b \equiv 25 \pmod{41}. \]

However, the congruence

\[ b + 2 - 10t^2 \equiv 0 \pmod{41} \]

does not hold if

\[ \begin{cases} t \equiv 16 \pmod{41} \\ b \equiv 25 \pmod{41} \end{cases}. \]

Therefore, \( p \neq 41 \), a contradiction. Therefore, there are at least two prime ideals in \( L \) lying above \( p \) and so \( G(\varphi) \) is a proper subgroup of \( D_5 \). Hence, \( G(\varphi) \) is cyclic.

Having proved the above, we are now able to use the method in [31] (see Proposition 2.1, p. 2) to construct an intersective polynomial where the Galois group under consideration is \( D_5 \). Since \( L \) must be the compositum of \( K = \mathbb{Q}(\theta) \) and \( \mathbb{Q}(\sqrt{d_b}) \), we construct a polynomial whose factors define these two subfields. This then requires us to form the product of \( f_b(x) \) with a defining polynomial for \( \mathbb{Q}(\sqrt{d_b}) \) to obtain an intersective polynomial with Galois group \( D_5 \). Thus

\[ g_b(x) = f_b(x)(x^2 - d_b) \]

is intersective and has Galois group \( D_5 \).

Finally, since infinitely many of the algebraic number fields \( \mathbb{Q}(\theta) \) are distinct as noted previously, we have infinitely many of the splitting fields \( \mathbb{Q}(\theta, \sqrt{d_b}) \) of \( g_b(x) \) are distinct. □

We close this section with some examples of intersective polynomials obtained from our main theorem.

**Example 7.3.2** For the following values of \( b \) in TABLE 7.3.7, we construct intersective polynomials using our theorem. All of the roots in \( \mathbb{C} \) of the first two intersective
polynomials are real, while in the last two examples only one root is real. The splitting fields of these polynomials are distinct.

Table 7.3.7: Intersective Polynomials - Example 7.3.2

<table>
<thead>
<tr>
<th>b</th>
<th>( d_b )</th>
<th>Intersective Polynomial</th>
</tr>
</thead>
<tbody>
<tr>
<td>-9</td>
<td>817</td>
<td>((x^5 - 2x^4 - 7x^3 + 17x^2 - 9x + 1)(x^2 - 817))</td>
</tr>
<tr>
<td>-8</td>
<td>401</td>
<td>((x^5 - 2x^4 - 6x^3 + 15x^2 - 8x + 1)(x^2 - 401))</td>
</tr>
<tr>
<td>0</td>
<td>-47</td>
<td>((x^5 - 2x^4 + 2x^3 - x^2 + 1)(x^2 + 47))</td>
</tr>
<tr>
<td>2</td>
<td>-239</td>
<td>((x^5 - 2x^4 + 4x^3 - 5x^2 + 2x + 1)(x^2 + 239))</td>
</tr>
</tbody>
</table>

7.4 Future Research

For future studies, one might continue searching for examples of intersective polynomials. Moreover, constructing parametric families of polynomials and confirming such polynomials indeed yield intersective polynomials would provide the researcher with an infinite number of examples.

We have given many examples of parametric families of polynomials. In the Lifting Monogenic Cubic Fields to Sextic Fields chapter, we have given an example of a parametric family of sextic polynomials whose Galois group is isomorphic to \( D_6 \) (recall \( f_d(x) = x^6 + 2dx^4 + d^2x^2 + 1 \) for \( d \equiv 1 \pmod{2} \), \( d > 3 \), \( 4d^3 - 27 \) squarefree). Using a similar method to the one used in this chapter, we might show that this family gives rise to an infinite family of intersective polynomials with Galois group \( D_6 \) (note that \( D_6 \) is 3-coverable). This analysis will give another infinite family of intersective polynomials. Presently, our family of polynomials with Galois group \( D_5 \) is the only infinite family of intersective polynomials in existence.
7.5 Conclusion

The purpose of the latter part of this thesis was to illustrate applications in the construction of parametric families of polynomials. Two important applications obtained from such families of polynomials were given. We first illustrated that families of polynomials can yield an infinite number of monogenic fields. Specifically, we showed that there are infinitely many septimic fields with Galois group isomorphic to $\text{PSL}(2, 7)$ that have a power basis. We also constructed infinitely many monogenic sextic fields containing a cubic subfield for five of the eight Galois groups of a sextic polynomial defining such fields. We did so via a lifting technique by taking monogenic cubic fields and lifting them into monogenic sextic fields. Moreover, for the remaining three possible Galois groups, we showed that there are at most finitely many such monogenic sextic fields. For the second application, we showed that a certain family of polynomials yield an infinite number of intersective polynomials. We began with another established parametric family of degree five polynomials that yield an infinite number of monogenic quintic fields whose Galois group is $D_5$. We showed that such polynomials gave rise to intersective polynomials. Lastly, we also provided the reader with future work in both application problems.
Bibliography


   <http://www.secamlocal.ex.ac.uk/people/staff/rjchapman/rjc.html>.


Appendix A: Maple Code

The following is the Maple code used to obtain the results in Lemma 6.2.2.

Case00000-

```maple
restart: element:=(a0+a1*x+a2*x^2+a3*x^3+a4*x^4+x^5)/2:
poly:=x^6+a*x^4+b*x^2-1:
e1:=subs(a0=0,a1=0,a2=0,a3=0,a4=0,element):
e2:=x^6+c5*x^5+c4*x^4+c3*x^3+c2*x^2+c1*x+c0:
e3:=subs(x=e1,e2):
e4:=rem(e3,poly,x):
e5:=coeff(e4,x,5):
e6:=coeff(e4,x,4):
e7:=coeff(e4,x,3):
e8:=coeff(e4,x,2):
e9:=coeff(e4,x,1):
e10:=coeff(e4,x,0):
e11:=solve({e5,e6,e7,e8,e9,e10},{c5,c4,c3,c2,c1,c0}):
assign(e11):
e2:
```

Clearly the constant term is not in Z so we do not have an algebraic integer.

End of case.

Case00001-

```maple
restart: element:=(a0+a1*x+a2*x^2+a3*x^3+a4*x^4+x^5)/2:
poly:=x^6+a*x^4+b*x^2-1:
e1:=subs(a0=0,a1=0,a2=0,a3=0,a4=1,element):
```
\[ e_2 := x^6 + c_5 x^5 + c_4 x^4 + c_3 x^3 + c_2 x^2 + c_1 x + c_0: \]
\[ e_3 := \text{subs}(x = e_1, e_2): \]
\[ e_4 := \text{rem}(e_3, \text{poly}, x): \]
\[ e_5 := \text{coeff}(e_4, x, 5): \]
\[ e_6 := \text{coeff}(e_4, x, 4): \]
\[ e_7 := \text{coeff}(e_4, x, 3): \]
\[ e_8 := \text{coeff}(e_4, x, 2): \]
\[ e_9 := \text{coeff}(e_4, x, 1): \]
\[ e_{10} := \text{coeff}(e_4, x, 0): \]
\[ e_{11} := \text{solve}\{e_5, e_6, e_7, e_8, e_9, e_{10}\}, \{c_5, c_4, c_3, c_2, c_1, c_0\} : \]
\[ \text{assign}(e_{11}): \]
\[ e_2: \]

Now we have to work to see if this poly can be in \( \mathbb{Z}[x] \). From the constant term we see that \( b = -64k - a \), \( k \) in \( \mathbb{Z} \). We subs.
\[ e_{12} := \text{subs}(b = 64k - a, e_2): \]
Now look at the coefficient of \( x^4 \).
\[ e_{13} := \text{factor(coeff}(e_{12}, x, 4)) : \]
\[ e_{14} := \text{numer}(e_{13}) : \text{denom}(e_{13}) : \]
This quantity must be congruent to 0 mod 4.
\[ e_{15} := e_{14} \mod 4 : \text{subs}(a = 0, e_{15}) \mod 4 : \text{subs}(a = 1, e_{15}) \mod 4 : \]
\[ \text{subs}(a = 2, e_{15}) \mod 4 : \text{subs}(a = 3, e_{15}) \mod 4 : \]
Looking at this we deduce that \( a \) must be 0 or 1 mod 4.
Let us do the 0 mod 4 case first.
\[ e_{16} := \text{collect(factor}(\text{subs}(a = 4m, e_{12})), x): \]
\[ e_{17} := \text{coeff}(e_{16}, x, 3): \]
Clearly this is not in \( \mathbb{Z} \) so we do not get an alg integer. Next subcase.
\[ e_{18} := \text{subs}(a = 4m+1, e_{12}): \]
\[ e_{19} := \text{factor(coeff}(e_{18}, x, 2)) : \]
\[ e_{20} := \text{subs}(m = 4n + 3, e_{18}) : \]
\[ e_{21} := \text{denom}(e_{20}) : \]

We have a condition. \((a, b) = (3, 61), (29, 35), (35, 29), (61, 3) \mod 64.\)

Case 00010-

\[ \text{restart; element} := (a_0 + a_1 x + a_2 x^2 + a_3 x^3 + a_4 x^4 + x^5) / 2 : \]
\[ \text{poly} := x^6 + a x^4 + b x^2 - 1 : \]
\[ e_1 := \text{subs}(a_0 = 0, a_1 = 0, a_2 = 0, a_3 = 1, a_4 = 0, \text{element}) : \]
\[ e_2 := x^6 + c_5 x^5 + c_4 x^4 + c_3 x^3 + c_2 x^2 + c_1 x + c_0 : \]
\[ e_3 := \text{subs}(x = e_1, e_2) : \]
\[ e_4 := \text{rem}(e_3, \text{poly}, x) : \]
\[ e_5 := \text{coeff}(e_4, x, 5) : \]
\[ e_6 := \text{coeff}(e_4, x, 4) : \]
\[ e_7 := \text{coeff}(e_4, x, 3) : \]
\[ e_8 := \text{coeff}(e_4, x, 2) : \]
\[ e_9 := \text{coeff}(e_4, x, 1) : \]
\[ e_{10} := \text{coeff}(e_4, x, 0) : \]
\[ e_{11} := \text{solve}\{e_5, e_6, e_7, e_8, e_9, e_{10}\}, \{c_5, c_4, c_3, c_2, c_1, c_0\} : \]
\[ \text{assign}(e_{11}) : \]
\[ e_{12} := e_2 : \]

We now have to see if this is in \( Z. \) Let us look at the coeff of \( x^4 \)
\[ e_{13} := \text{factor}(\text{coeff}(e_{12}, x, 4)) : \]
\[ \text{numer}(e_{13}) : \]
\[ \text{denom}(e_{13}) : \]

We need \( e_{13} = 0 \mod 2, \) to start with.
\[ e_{14} := \text{numer}(e_{13}) \mod 2 : \]

Suppose first that \( a \) is even.
\[ e_{15} := \text{subs}(a = 0, e_{14}) \mod 2 : \]

We see that \( b \) must be odd. Let us try this in \( e_{12} \).
>e16:=factor(subs(a=2*m,b=2*n+1,e12)):
e17:=coeff(e16,x,4):
Now we see that n must be odd.
>e18:=factor(subs(n=2*u+1,e16)):
e19:=coeff(e18,x,2):
e20:=denom(e19):numer(e19) mod 4:
Impossible, so back to a odd.
>e21:=factor(subs(a=2*m+1,e12)):
e22:=factor(coeff(e21,x,4)):
e23:=denom(e22):
e24:=numer(e22) mod 4:
e25:=subs(b=0,e24) mod 4:subs(b=1,e24) mod 4:
>subs(b=2,e24) mod 4:subs(b=3,e24) mod 4:
We observe three possible cases from this. The first one is \( b = 0 \) mod 4.
>e26:=subs(b=4*u,e21):
e27:=coeff(e26,x,2):
Cannot be in Z. Next case.
>e28:=subs(b=4*u+1,m=2*v+1,e21):
e29:=coeff(e26,x,2):
Cannot be in Z. Next case.
>e30:=subs(b=4*u+3,m=2*v,e21):
e31:=coeff(e26,x,2):
Cannot be in Z. End of Case.
Case00011-
>restart:element:=(a0+a1*x+a2*x^2+a3*x^3+a4*x^4+x^5)/2:
poly:=x^6+a*x^4+b*x^2-1:
e1:=subs(a0=0,a1=0,a2=0,a3=1,a4=1,element):
e2:=x^6+c5*x^5+c4*x^4+c3*x^3+c2*x^2+c1*x+c0:
\texttt{\textbackslash e3:=subs(x=e1,e2):}
\texttt{\textbackslash e4:=rem(e3,poly,x):}
\texttt{\textbackslash e5:=coeff(e4,x,5):}
\texttt{\textbackslash e6:=coeff(e4,x,4):}
\texttt{\textbackslash e7:=coeff(e4,x,3):}
\texttt{\textbackslash e8:=coeff(e4,x,2):}
\texttt{\textbackslash e9:=coeff(e4,x,1):}
\texttt{\textbackslash e10:=coeff(e4,x,0):}
\texttt{\textbackslash e11:=solve\{\textbackslash e5,\textbackslash e6,\textbackslash e7,\textbackslash e8,\textbackslash e9,\textbackslash e10\},\{c0,c1,c2,c3,c4,c5\}):}
\texttt{\textbackslash assign(e11):}
\texttt{\textbackslash e12:=e2:}
\texttt{\textbackslash e13:=factor(coeff(e12,x,4)):}
\texttt{\textbackslash e14:=numer(e13):}
\texttt{\textbackslash denom(e13):}
\texttt{\textbackslash e15:=subs(a=0,e14):msolve(e15,4):}
\texttt{\textbackslash e15a:=subs(a=1,e14):}
\texttt{\textbackslash msolve(e15a,4):}
\texttt{\textbackslash e15b:=subs(a=2,e14):msolve(e15b,4):}
\texttt{\textbackslash e15c:=subs(a=3,e14):msolve(e15c,4):}
\texttt{This shows that a must be even and b = 1 mod 4.}
\texttt{\textbackslash e16:=subs(a=2*m,b=4*n+1,e12):}
\texttt{\textbackslash e17:=factor(coeff(e16,x,4)):}
\texttt{\textbackslash e18:=factor(coeff(e16,x,3)):}
\texttt{Cannot be in Z. End of case.}

\texttt{Case00100-}
\texttt{\textbackslash restart:element:=(a0+a1*x+a2*x^2+a3*x^3+a4*x^4+x^5)/2:}
\texttt{\textbackslash poly:=x^6+a*x^4+b*x^2-1:}
\texttt{\textbackslash e1:=subs(a0=0,a1=0,a2=1,a3=0,a4=0,element):}
\[
e_{2} := x^{6} + c_{5}x^{5} + c_{4}x^{4} + c_{3}x^{3} + c_{2}x^{2} + c_{1}x + c_{0}:
\]
\[
e_{3} := \text{subs}(x = e_{1}, e_{2}):
\]
\[
e_{4} := \text{rem}(e_{3}, \text{poly}, x):
\]
\[
e_{5} := \text{coeff}(e_{4}, x, 5):
\]
\[
e_{6} := \text{coeff}(e_{4}, x, 4):
\]
\[
e_{7} := \text{coeff}(e_{4}, x, 3):
\]
\[
e_{8} := \text{coeff}(e_{4}, x, 2):
\]
\[
e_{9} := \text{coeff}(e_{4}, x, 1):
\]
\[
e_{10} := \text{coeff}(e_{4}, x, 0):
\]
\[
e_{11} := \text{solve}\left\{ e_{5}, e_{6}, e_{7}, e_{8}, e_{9}, e_{10} \right\}, \left\{ c_{5}, c_{4}, c_{3}, c_{2}, c_{1}, c_{0} \right\}:
\]
\[
\text{assign}(e_{11}):
\]
\[
e_{12} := e_{2}:
\]
\[
e_{13} := \text{coeff}(e_{12}, x, 4):
\]
\[
e_{14} := \text{numer}(e_{13}) : \text{denom}(e_{13}):
\]
\[
e_{15} := e_{14} \mod 2:
\]
\[
\text{subs}(a = 0, e_{15}) : \text{subs}(a = 1, e_{15}):
\]
We deduce that \(a\) and \(b\) must have the same parity. We subs.
\[
e_{16} := \text{subs}(a = 2m, b = 2n, e_{12}):
\]
\[
e_{17} := \text{factor}(\text{coeff}(e_{16}, x, 4)):
\]
This shows that \(n\) must be odd.
\[
e_{18} := \text{collect}(\text{factor}(\text{subs}(n = 2u, e_{16})), x):
\]
We also see that \(m\) must be even.
\[
e_{19} := \text{factor}(\text{subs}(m = 2v, e_{18})):\]
We have obtained an integer if \(a = b = 0 \mod 4\). Now we try \(a\) and \(b\) both odd.
\[
e_{20} := \text{subs}(a = 2m + 1, b = 2n + 1, e_{12}):
\]
\[
e_{21} := \text{factor}(\text{coeff}(e_{20}, x, 4)):
\]
We see that \(m\) must be even.
\[
e_{22} := \text{factor}(\text{subs}(m = 2u, e_{20})):\]
We see that \( n \) must be odd.

\[ \text{e23} := \text{factor}\left(\text{subs}\left(n=2*\text{v}+1,\text{e22}\right)\right) \]

We see that \( \text{v} \) is a multiple of 4.

\[ \text{e25} := \text{factor}\left(\text{subs}\left(\text{v}=4*\text{w},\text{e23}\right)\right) \]

We see that \( \text{u} \) is of the form \( 4*\text{y}+1 \).

\[ \text{e27} := \text{factor}\left(\text{subs}\left(\text{u}=4*\text{y}+1,\text{e25}\right)\right) \]

We need \( 2\text{y}+1+2\text{w} = 0 \mod 8 \) which is impossible. This gives us no new cases.

Case00101-

\[ \text{e1} := \text{subs}\left(\text{a0}=0,\text{a1}=0,\text{a2}=1,\text{a3}=0,\text{a4}=1,\text{element}\right) \]

\[ \text{e2} := \text{rem}\left(\text{e3},\text{poly},\text{x}\right) \]

\[ \text{e5} := \text{coeff}\left(\text{e4},\text{x},5\right) \]

\[ \text{e6} := \text{coeff}\left(\text{e4},\text{x},4\right) \]

\[ \text{e7} := \text{coeff}\left(\text{e4},\text{x},3\right) \]

\[ \text{e8} := \text{coeff}\left(\text{e4},\text{x},2\right) \]

\[ \text{e9} := \text{coeff}\left(\text{e4},\text{x},1\right) \]

\[ \text{e10} := \text{coeff}\left(\text{e4},\text{x},0\right) \]

\[ \text{e11} := \text{solve}\left(\{\text{e5},\text{e6},\text{e7},\text{e8},\text{e9},\text{e10}\},\{\text{c5},\text{c4},\text{c3},\text{c2},\text{c1},\text{c0}\}\right) \]

\[ \text{assign}\left(\text{e11}\right) \]

\[ \text{e12} := \text{e2} \]

\[ \text{e13} := \text{factor}\left(\text{coeff}\left(\text{e12},\text{x},4\right)\right) \]
\( e_{14} := \text{numer}(e_{13}): \text{denom}(e_{13}): \)
\( e_{15} := e_{14} \mod 2: \)
\( \text{msolve}(e_{15}, 2): \)
\( e_{16} := \text{subs}(b=2c+1, e_{15}) \mod 2: \)
These confirm we need \( b \) even.
\( e_{17} := \text{factor}(\text{subs}(b=2m, e_{12})): \)
\( e_{18} := \text{factor}((e_{17}, x, 4)): \)
\( e_{19} := \text{numer}(e_{18}): \text{denom}(e_{18}): \)
\( e_{20} := e_{19} \mod 2: \)
\( e_{21} := \text{numer}(e_{18}) \mod 4: \)
\( e_{22} := \text{subs}(a=0, e_{21}): \text{subs}(a=1, e_{21}): \text{subs}(a=2, e_{21}) \mod 4: \)
\( \text{subs}(a=3, e_{21}) \mod 4: \)
We see three cases to consider here.
\( e_{23} := \text{subs}(a=4u+0, m=2n+1, e_{17}): \)
\( e_{24} := \text{factor}(\text{coeff}(e_{23}, x, 3)): \)
Cannot be in \( \mathbb{Z} \), next case.
\( e_{25} := \text{subs}(a=4u+2, m=2n+1, e_{17}): \)
\( e_{26} := \text{factor}(\text{coeff}(e_{23}, x, 3)): \)
Cannot be in \( \mathbb{Z} \), next case.
\( e_{27} := \text{factor}(\text{subs}(a=4u+3, e_{17})): \)
\( e_{28} := \text{factor}(\text{coeff}(e_{27}, x, 3)): \)
We see we need \( m \) odd.
\( e_{29} := \text{factor}(\text{subs}(m=2v+1, e_{27})): \)
\( e_{30} := \text{denom}(e_{29}): \)
We have a new case. \( (a,b) = (3,2) \mod 4. \)

Case00110-
\( > \text{restart: element:} := (a_0+a_1*x+a_2*x^2+a_3*x^3+a_4*x^4+x^5)/2: \)
\( > \text{poly:} = x^6+a*x^4+b*x^2-1: \)
\begin{verbatim}
> e1 := subs(a0 = 0, a1 = 0, a2 = 1, a3 = 1, a4 = 0, element):
> e2 := x^6 + c5*x^5 + c4*x^4 + c3*x^3 + c2*x^2 + c1*x + c0:
> e3 := subs(x = e1, e2):
> e4 := rem(e3, poly, x):
> e5 := coeff(e4, x, 5):
> e6 := coeff(e4, x, 4):
> e7 := coeff(e4, x, 3):
> e8 := coeff(e4, x, 2):
> e9 := coeff(e4, x, 1):
> e10 := coeff(e4, x, 0):
> e11 := solve({e5, e6, e7, e8, e9, e10}, {c5,c4,c3,c2,c1,c0}):
> assign(e11):
> e12 := e2:
> e13 := factor(coeff(e12, x, 4)):
> e14 := numer(e13):denom(e13):
> e15 := e14 mod 2:
> e16 := msolve(e15, 2):
> e17 := expand(subs(b = 0, e15)) mod 2:expand(subs(a = 1, e15)) mod 2:
> e18 := expand(subs(a = 2*m, b = 2*n + 1, e12)):
> e19 := coeff(e18, x, 4):
We need n even.
> e20 := subs(n = 2*u, e18):
> e21 := factor(coeff(e20, x, 3)):
> e22 := factor(subs(m = 2*v + 1, e20)):
> denom(e22):
We have a new case a = 2 mod 4 and v = 1 mod 4
Case00111-
> restart:element := (a0+a1*x+a2*x^2+a3*x^3+a4*x^4+x^5)/2:
\end{verbatim}
\texttt{poly:=x^6+a*x^4+b*x^2-1:}
\texttt{e1:=subs(a0=0,a1=0,a2=1,a3=1,a4=1,element):}
\texttt{e2:=x^6+c5*x^5+c4*x^4+c3*x^3+c2*x^2+c1*x+c0:}
\texttt{e3:=subs(x=e1,e2):}
\texttt{e4:=rem(e3,poly,x):}
\texttt{e5:=coeff(e4,x,5):}
\texttt{e6:=coeff(e4,x,4):}
\texttt{e7:=coeff(e4,x,3):}
\texttt{e8:=coeff(e4,x,2):}
\texttt{e9:=coeff(e4,x,1):}
\texttt{e10:=coeff(e4,x,0):}
\texttt{e11:=solve\{e5,e6,e7,e8,e9,e10\},\{c5,c4,c3,c2,c1,c0\}:}
\texttt{assign(e11):}
\texttt{e12:=e2:}
\texttt{e13:=coeff(e12,x,4):}
\texttt{e14:=numer(e13):denom(e13):}
\texttt{e15:=subs(a=0,b=0,e14) mod 2:subs(a=0,b=1,e14) mod 2:}
\texttt{subs(a=1,b=0,e14) mod 2:}
\texttt{subs(a=1,b=1,e14) mod 2:}

We have three cases to check.
\texttt{e16:=expand(subs(a=2*m,b=2*n+1,e14)) mod 4:}
\texttt{e17:=factor(subs(a=2*m,b=4*u+1,e12)):}
\texttt{e18:=factor(coeff(e17,x,3)):}
\texttt{e19:=factor(subs(m=2*v+1,e17)):}
\texttt{e20:=factor(coeff(e19,x,2)):}

No contribution here. Next case.
\texttt{e21:=factor(subs(a=2*m+1,b=2*n,e12)):}
\texttt{e22:=factor(coeff(e21,x,4)):}
Requires \( n \) odd

\[ e_{23} := \text{factor}(\text{subs}(n=2u+1,e_{21})) : \]

\[ e_{24} := \text{factor}(\text{coeff}(e_{23},x,3)) : \]

Cannot be in \( \mathbb{Z} \). Last part.

\[ e_{25} := \text{subs}(a=2m+1,b=2n+1,e_{12}) : \]

\[ e_{26} := \text{factor}(\text{coeff}(e_{25},x,4)) : \]

We require \( n = m + 1 \mod 2 \).

\[ e_{27} := \text{subs}(m=n+1+2w,e_{25}) : \]

\[ e_{28} := \text{factor}(\text{coeff}(e_{27},x,2)) : \]

\[ e_{29} := \text{numer}(e_{28}) \mod 2 : \]

\[ e_{30} := \text{subs}(n=2y+1,e_{27}) : \]

\[ e_{31} := \text{factor}(\text{coeff}(e_{30},x,0)) : \]

\[ \text{denom}(e_{30}) : \]

We get a new case \( a = 1 \mod 4 \) and \( b = 3 \mod 4 \).

Case01000-

\[ \text{restart}: \] element := \( (a0+a1*x+a2*x^2+a3*x^3+a4*x^4+x^5)/2 : \]

\[ \text{poly} := x^6+a*x^4+b*x^2-1 : \]

\[ e_{1} := \text{subs}(a0=0,a1=1,a2=0,a3=0,a4=0,\text{element}) : \]

\[ e_{2} := x^6+c5*x^5+c4*x^4+c3*x^3+c2*x^2+c1*x+c0 : \]

\[ e_{3} := \text{subs}(x=e_{1},e_{2}) : \]

\[ e_{4} := \text{rem}(e_{3},\text{poly},x) : \]

\[ e_{5} := \text{coeff}(e_{4},x,5) : \]

\[ e_{6} := \text{coeff}(e_{4},x,4) : \]

\[ e_{7} := \text{coeff}(e_{4},x,3) : \]

\[ e_{8} := \text{coeff}(e_{4},x,2) : \]

\[ e_{9} := \text{coeff}(e_{4},x,1) : \]

\[ e_{10} := \text{coeff}(e_{4},x,0) : \]

\[ e_{11} := \text{solve} \{ e_{5},e_{6},e_{7},e_{8},e_{9},e_{10}, \{ c5,c4,c3,c2,c1,c0 \} \} : \]
>assign(e11):
>e12:=e2:
>e13:=factor(coeff(e12,x,4)):
>e14:=numer(e13):denom(e13):
>e15:=e14 mod 2:
>e16:=expand(subs(a=0,e15)) mod 2:subs(a=1,e15) mod 2:
>e17:=factor(subs(b=2*m+1+a,e12)):
>e18:=factor(coeff(e17,x,4)):
>e19:=numer(e18) mod 4:
>e20:=subs(a=0,e19):subs(a=1,e19) mod 4:subs(a=2,e19) mod 4:
>subs(a=3,e19) mod 4:
We have three cases to consider. To start with...
>e21:=subs(a=4*u,m=2*v+1,e17):
>e22:=factor(coeff(e21,x,2)):
Clearly not in Z. Next case.
>e23:=subs(a=2*u+1,e17):
>e24:=factor(coeff(e21,x,2)):
Clearly not in Z. Next case.
>e25:=subs(a=4*u+2,m=2*v,e17):
>e26:=factor(coeff(e21,x,2)):
Clearly not in Z. End of case.
Case01001-
>restart:element:=(a0+a1*x+a2*x^2+a3*x^3+a4*x^4+x^5)/2:
>poly:=x^6+a*x^4+b*x^2-1:
>e1:=subs(a0=0,a1=1,a2=0,a3=0,a4=1,element):
>e2:=x^6+c5*x^5+c4*x^4+c3*x^3+c2*x^2+c1*x+c0:
>e3:=subs(x=e1,e2):
>e4:=rem(e3,poly,x):

201
\begin{verbatim}
> e5:=coeff(e4,x,5):
> e6:=coeff(e4,x,4):
> e7:=coeff(e4,x,3):
> e8:=coeff(e4,x,2):
> e9:=coeff(e4,x,1):
> e10:=coeff(e4,x,0):
> e11:=solve({e5,e6,e7,e8,e9,e10},{c5,c4,c3,c2,c1,c0}):
> assign(e11): 
> e12:=e2:
> e13:=factor(coeff(e12,x,4)):
> e14:=numer(e13):denom(e13):
> e15:=msolve(e14,2):
> e16:=expand(subs(b=2*k+1,e14)) mod 2:
> e17:=subs(b=2*m,e12):
> e18:=factor(coeff(e17,x,4)):
> e19:=numer(e18):
> e20:=subs(a=0,e19) mod 4:subs(a=1,e19) mod 4:subs(a=2,e19 mod 4: 
> subs(a=3,e19) mod 4:
We have two cases to consider.
> e21:=subs(a=4*u,m=2*v+1,e17):
> e22:=factor(coeff(e21,x,1)):
Cannot be in Z. Next...
> e23:=subs(a=4*u+2,m=2*v,e17):
> e24:=factor(coeff(e23,x,1)):
Cannot be in Z. Next case.
Case01010-
> restart:element:=(a0+a1*x+a2*x^2+a3*x^3+a4*x^4+x^5)/2:
> poly:=x^6+a*x^4+b*x^2-1:
\end{verbatim}
\[ e_1:=\text{subs}(a_0=0,a_1=1,a_2=0,a_3=1,a_4=0,\text{element}): \]
\[ e_2:=x^6+c_5x^5+c_4x^4+c_3x^3+c_2x^2+c_1x+c_0: \]
\[ e_3:=\text{subs}(x=e_1,e_2): \]
\[ e_4:=\text{rem}(e_3,\text{poly},x): \]
\[ e_5:=\text{coeff}(e_4,x,5): \]
\[ e_6:=\text{coeff}(e_4,x,4): \]
\[ e_7:=\text{coeff}(e_4,x,3): \]
\[ e_8:=\text{coeff}(e_4,x,2): \]
\[ e_9:=\text{coeff}(e_4,x,1): \]
\[ e_{10}:=\text{coeff}(e_4,x,0): \]
\[ e_{11}:=\text{solve}\{e_5,e_6,e_7,e_8,e_9,e_{10}\},\{c_5,c_4,c_3,c_2,c_1,c_0\}: \]
\[ \text{assign}(e_{11}): \]
\[ e_{12}:=e_2: \]
\[ e_{13}:=\text{factor}(\text{coeff}(e_{12},x,4)): \]
\[ e_{14}:=\text{numer}(e_{13}):\text{denom}(e_{13}): \]
\[ e_{15}:=\text{msolve}(e_{14},2): \]
\[ e_{16}:=\text{expand}\left(\text{subs}(a=1,e_{14})\right) \mod 2:\text{expand}\left(\text{subs}(b=0,e_{14})\right) \mod 2: \]
\[ e_{17}:=\text{factor}\left(\text{subs}(a=2*m,b=2*n+1,e_{12})\right): \]
\[ e_{18}:=\text{factor}(e_{17},x,4): \]
\[ e_{19}:=\text{factor}\left(\text{subs}(n=m+2*k,e_{17})\right): \]
\[ e_{20}:=\text{factor}(\text{coeff}(e_{19},x,2)): \]

Cannot be in \( \mathbb{Z} \). End of case.

Case01011-
\[ \text{restart}: \text{element}:=(a_0+a_1*x+a_2*x^2+a_3*x^3+a_4*x^4+x^5)/2: \]
\[ \text{poly}:=x^6+a*x^4+b*x^2-1: \]
\[ e_1:=\text{subs}(a_0=0,a_1=1,a_2=0,a_3=1,a_4=1,\text{element}): \]
\[ e_2:=x^6+c_5x^5+c_4x^4+c_3x^3+c_2x^2+c_1x+c_0: \]
\[ e_3:=\text{subs}(x=e_1,e_2): \]
We have two cases.

We have a new condition. \( a = 2 \text{ mod } 4 \) and \( b = 1 \text{ mod } 4 \).
We still must consider \( a \) odd.
\begin{verbatim}
> e28 := factor(coeff(e27, x, 4)):
> e29 := numer(e28) mod 4:
> e30 := subs(b=0, e29): subs(b=1, e29) mod 4: subs(b=2, e29) mod 4:
> subs(b=3, e29) mod 4:
We have 3 more cases to consider.
> e31 := subs(b=4*u, m=2*v, e27):
> e32 := factor(coeff(e31, x, 4)):
> e33 := factor(coeff(e31, x, 3)):
Cannot be in Z. Next.
> e34 := subs(b=4*u+2, m=2*v+1, e27):
> e35 := factor(coeff(e34, x, 3)):
Cannot be in Z. Next...
> e36 := subs(b=4*u+3, e27):
> e37 := factor(coeff(e36, x, 3)):
Need m even.
> e38 := subs(m=2*v, e36):
> e39 := factor(coeff(e38, x, 3)):
> e40 := factor(coeff(e38, x, 2)):
Need v = 3 mod 4
> e41 := factor(subs(v=4*w+3, e38)):
> e42 := factor(coeff(e41, x, 2)):
> e43 := factor(coeff(e41, x, 1)):
Need u even
> e44 := factor(subs(u=2*y, e41)):
> e45 := factor(coeff(e44, x, 1)):
> e46 := factor(coeff(e44, x, 0)):
> e47 := numer(e46): denom(e46):
> e48 := e47 mod 8:
\end{verbatim}
\[ e_{49} := \text{subs}(y=6+6*w+8*z, e_{44}) : \]
\[ \text{denom}(e_{49}) : \]

We have a new case. It is \((a, b) = (13, 51), (29, 35), (45, 19), (61, 3) \mod 64.\]

Case01100-

\[ \text{restart}: \]
\[ \text{element} := (a_0 + a_1*x + a_2*x^2 + a_3*x^3 + a_4*x^4 + x^5)/2 : \]
\[ \text{poly} := x^6 + a*x^4 + b*x^2 - 1 : \]
\[ e_1 := \text{subs}(a_0=0, a_1=1, a_2=1, a_3=0, a_4=0, \text{element}) : \]
\[ e_2 := x^6 + c_5*x^5 + c_4*x^4 + c_3*x^3 + c_2*x^2 + c_1*x + c_0 : \]
\[ e_3 := \text{subs}(x=e_1, e_2) : \]
\[ e_4 := \text{rem}(e_3, \text{poly}, x) : \]
\[ e_5 := \text{coeff}(e_4, x, 5) : \]
\[ e_6 := \text{coeff}(e_4, x, 4) : \]
\[ e_7 := \text{coeff}(e_4, x, 3) : \]
\[ e_8 := \text{coeff}(e_4, x, 2) : \]
\[ e_9 := \text{coeff}(e_4, x, 1) : \]
\[ e_{10} := \text{coeff}(e_4, x, 0) : \]
\[ e_{11} := \text{solve}([e_5, e_6, e_7, e_8, e_9, e_{10}], \{c_5, c_4, c_3, c_2, c_1, c_0\}) : \]
\[ \text{assign}(e_{11}) : \]
\[ e_{12} := e_2 : \]
\[ e_{13} := \text{factor}(\text{coeff}(e_{12}, x, 4)) : \]
\[ e_{14} := \text{numer}(e_{13}) : \text{denom}(e_{13}) : \]
\[ e_{15} := \text{msolve}(e_{14}, 2) : \]
\[ e_{16} := \text{expand}((\text{subs}(b=1, e_{14})) \mod 2) : \]
\[ e_{17} := \text{subs}(b=2*m, e_{12}) : \]
\[ e_{18} := \text{factor}(\text{coeff}(e_{17}, x, 4)) : \]
\[ e_{19} := \text{numer}(e_{18}) \mod 2 : \]
\[ e_{20} := \text{numer}(e_{18}) \mod 4 : \]
\[ e_{21} := \text{subs}(a=0, e_{20}) : \text{subs}(a=1, e_{20}) \mod 4 : \text{subs}(a=2, e_{20}) \mod 4 : \]

206
We see two cases.

```
> e22 := subs(a = 4*u, m = 2*v + 1, e17):
> e23 := factor(coeff(e22, x, 4)):
> e24 := factor(coeff(e22, x, 3)):
> e25 := factor(coeff(e22, x, 2)):

Cannot be in Z. Next.

> e26 := subs(a = 4*u + 2, m = 2*v, e17):
> e27 := factor(coeff(e26, x, 1)):

Cannot be in Z. End of case.
```

```
Case01101-

> restart:
> element := (a0 + a1*x + a2*x^2 + a3*x^3 + a4*x^4 + x^5)/2:
> poly := x^6 + a*x^4 + b*x^2 - 1:
> e1 := subs(a0 = 0, a1 = 1, a2 = 1, a3 = 0, a4 = 1, element):
> e2 := x^6 + c5*x^5 + c4*x^4 + c3*x^3 + c2*x^2 + c1*x + c0:
> e3 := subs(x = e1, e2):
> e4 := rem(e3, poly, x):
> e5 := coeff(e4, x, 5):
> e6 := coeff(e4, x, 4):
> e7 := coeff(e4, x, 3):
> e8 := coeff(e4, x, 2):
> e9 := coeff(e4, x, 1):
> e10 := coeff(e4, x, 0):
> e11 := solve({e5, e6, e7, e8, e9, e10}, {c5, c4, c3, c2, c1, c0}):
> assign(e11):
> e12 := e2:
> e13 := factor(coeff(e12, x, 4)):
> e14 := numer(e13):denom(e13):
```
\[ e_{15} = e_{14} \mod 2: \]
\[ e_{16} = \text{subs}(a=0, e_{15}) \mod 2: \text{subs}(a=1, e_{15}) \mod 2: \]

We have two cases.

\[ e_{17} = \text{subs}(a=2m, b=2n, e_{12}): \]
\[ e_{18} = \text{factor} \left( \text{coeff} \left( e_{17}, x, 4 \right) \right): \]
\[ e_{19} = \text{factor} \left( \text{subs} \left( n=m+2u, e_{17} \right) \right): \]
\[ e_{20} = \text{factor} \left( \text{coeff} \left( e_{19}, x, 4 \right) \right): \]
\[ e_{21} = \text{factor} \left( \text{coeff} \left( e_{19}, x, 3 \right) \right): \]
\[ e_{22} = \text{factor} \left( \text{subs} \left( m=2v, e_{19} \right) \right): \]

We have a new condition. It is \( a=b=0 \mod 4 \). Last we try \( a, b \) both odd.

\[ e_{28} = \text{subs} \left( a=2m+1, b=2n+1, e_{12} \right): \]
\[ e_{29} = \text{factor} \left( \text{coeff} \left( e_{28}, x, 4 \right) \right): \]
\[ e_{30} = \text{factor} \left( \text{coeff} \left( e_{28}, x, 3 \right) \right): \]
\[ e_{31} = \text{factor} \left( \text{subs} \left( n=m+1+2u, e_{28} \right) \right): \]
\[ e_{32} = \text{factor} \left( \text{coeff} \left( e_{31}, x, 3 \right) \right): \]
\[ e_{33} = \text{factor} \left( \text{coeff} \left( e_{31}, x, 2 \right) \right): \]
\[ e_{34} = \text{factor} \left( \text{subs} \left( m=2v, e_{31} \right) \right): \]
\[ e_{35} = \text{factor} \left( \text{coeff} \left( e_{34}, x, 2 \right) \right): \]
\[ e_{36} = \text{factor} \left( \text{coeff} \left( e_{34}, x, 1 \right) \right): \]
\[ e_{37} = \text{factor} \left( \text{coeff} \left( e_{34}, x, 0 \right) \right): \]
\[ e_{38} = \text{factor} \left( \text{subs} \left( u=2v-1+2w, e_{37} \right) \right): \]

We have another new condition. It is \( (a,b) = (1,7), (5,3) \mod 8 \).
Case01110-

\[ \text{element} := \frac{a_0 + a_1 x + a_2 x^2 + a_3 x^3 + a_4 x^4 + x^5}{2} \]

\[ \text{poly} := x^6 + a x^4 + b x^2 - 1 \]

\[ \text{element} := \text{subs}(a_0=0, a_1=1, a_2=1, a_3=1, a_4=0, \text{element}) \]

\[ \text{element} := \text{subs}(x=x^6 + c_5 x^5 + c_4 x^4 + c_3 x^3 + c_2 x^2 + c_1 x + c_0) \]

\[ \text{element} := \text{subs}(x=x^6 + c_5 x^5 + c_4 x^4 + c_3 x^3 + c_2 x^2 + c_1 x + c_0) \]

\[ \text{assign}(\text{e11}) \]

\[ \text{e12} := \text{e2} \]

\[ \text{factor}(\text{coeff}(\text{e12}, x, 4)) \]

\[ \text{numer}(\text{e13}) : \text{denom}(\text{e13}) \]

\[ \text{subs}(a=0, \text{e14}) \mod 2 : \text{subs}(a=1, \text{e14}) \mod 2 \]

We have two cases.

\[ \text{expand}(\text{subs}(a=2*m, b=2*n+1, \text{e13})) \]

\[ \text{subs}(a=2*m, b=2*n+1, n=m+1+2*u, \text{e12}) \]

\[ \text{factor}(\text{coeff}(\text{e17}, x, 4)) \]

\[ \text{factor}(\text{coeff}(\text{e17}, x, 3)) \]

\[ \text{subs}(m=2*u+1, \text{e17}) \]

\[ \text{factor}(\text{coeff}(\text{e20}, x, 3)) \]

\[ \text{factor}(\text{coeff}(\text{e20}, x, 2)) \]

Cannot be in Z, next subcase
\( e_{23} := \text{subs}(a = 2m + 1, e_{12}) : \)
\( e_{24} := \text{factor}(\text{coeff}(e_{23}, x, 4)) : \)
\( e_{25} := \text{numer}(e_{24}) : \text{denom}(e_{24}) : \)
\( e_{26} := \text{subs}(b = 0, e_{25}) \mod 4 : \text{subs}(b = 1, e_{25}) \mod 4 : \text{subs}(b = 2, e_{25}) \mod 4 : \text{subs}(b = 3, e_{25}) \mod 4 : \)

We have three cases to consider.
\( e_{27} := \text{subs}(b = 4u, m = 2v, e_{23}) : \)
\( e_{28} := \text{factor}(\text{coeff}(e_{27}, x, 2)) : \)
Clearly not in \( \mathbb{Z} \), next subcase.
\( e_{29} := \text{subs}(b = 4u + 2, m = 2v + 1, e_{23}) : \)
\( e_{30} := \text{denom}(e_{29}) : \)
We have a new case. It is \( a = 3 \mod 4 \) and \( b = 2 \mod 4 \). Now for the last subcase.
\( e_{31} := \text{subs}(b = 4u + 3, e_{23}) : \)
\( e_{32} := \text{factor}(\text{coeff}(e_{31}, x, 2)) : \)
\( e_{33} := \text{numer}(e_{32}) \mod 4 : \text{denom}(e_{32}) : \)
\( e_{34} := \text{msolve}(e_{33}, 2) : \)
\( e_{35} := \text{expand}(\text{subs}(u = 2c + 1, e_{33})) \mod 2 : \)
\( e_{36} := \text{subs}(u = 2c, e_{31}) : \)
\( e_{37} := \text{factor}(\text{coeff}(e_{36}, x, 1)) : \)
\( e_{38} := \text{subs}(m = 2v, e_{36}) : \)
\( e_{39} := \text{factor}(\text{coeff}(e_{38}, x, 2)) : \)
\( e_{40} := \text{subs}(c = v + 1 + 2w, e_{38}) : \)
\( e_{41} := \text{factor}(\text{coeff}(e_{40}, x, 1)) : \)
\( e_{42} := \text{factor}(\text{subs}(v = 4y + 3, e_{40})) : \)
\( e_{43} := \text{factor}(\text{coeff}(e_{42}, x, 0)) : \)
\( e_{44} := \text{factor}(\text{subs}(w = y + 1 + 2z, e_{42})) : \)
\( e_{45} := \text{factor}(\text{coeff}(e_{44}, x, 0)) : \)
\( e_{46} := \text{factor}(\text{subs}(z = 2d, e_{44})) : \)
We have a new case. It is \((a,b) = (13,51), (29,35), (45,19), (61,3) \mod 64\).

Case01111-

\[\text{restart: element:=}(a_0+a_1x+a_2x^2+a_3x^3+a_4x^4+x^5)/2:\]
\[\text{poly:=}x^6+a*x^4+b*x^2-1:\]
\[\text{e1:=subs(a0=0,a1=1,a2=1,a3=1,a4=1,element):}\]
\[\text{e2:=}x^6+c5*x^5+c4*x^4+c3*x^3+c2*x^2+c1*x+c0:\]
\[\text{e3:=subs(x=e1,e2):}\]
\[\text{e4:=rem(e3,poly,x):}\]
\[\text{e5:=coeff(e4,x,5):}\]
\[\text{e6:=coeff(e4,x,4):}\]
\[\text{e7:=coeff(e4,x,3):}\]
\[\text{e8:=coeff(e4,x,2):}\]
\[\text{e9:=coeff(e4,x,1):}\]
\[\text{e10:=coeff(e4,x,0):}\]
\[\text{e11:=solve({e5,e6,e7,e8,e9,e10},{c5,c4,c3,c2,c1,c0}):}\]
\[\text{assign(e11):}\]
\[\text{e12:=e2:}\]
\[\text{e13:=factor(coeff(e12,x,4)):}\]
\[\text{e14:=numer(e13):denom(e13):}\]
\[\text{e15:=subs(a=0,e14) mod 2:subs(a=1,e14) mod 2:}\]

We see one case to consider namely a even and b odd.

\[\text{e16:=subs(a=2*m,b=2*n+1,e12):}\]
\[\text{e17:=factor(coeff(e16,x,4)):}\]
\[\text{e18:=subs(m=n+1+2*u,e16):}\]
\[\text{e19:=factor(coeff(e18,x,3)):}\]

Cannot be in \(\mathbb{Z}\). Done this case.

Case10000-
We see three cases to consider.

Cannot be in $\mathbb{Z}$. Next subcase.
We have a new case \((a,b) = (29,3), (13, 19) \mod 32\). Now for the last subcase.

We have a new case \((a,b) = (29,3), (13, 19) \mod 32\). Now for the last subcase.

Case10001-

```plaintext
>restart:
>element := (a0+a1*x+a2*x^2+a3*x^3+a4*x^4+x^5)/2:
>poly := x^6+a*x^4+b*x^2-1:
>e1 := subs(a0=1,a1=0,a2=0,a3=0,a4=1,element):
>e2 := x^6+c5*x^5+c4*x^4+c3*x^3+c2*x^2+c1*x+c0:
>e3 := subs(x=e1,e2):
>e4 := rem(e3,poly,x):
>e5 := coeff(e4,x,5):
>e6 := coeff(e4,x,4):
```
> e7 := coeff(e4, x, 3):
> e8 := coeff(e4, x, 2):
> e9 := coeff(e4, x, 1):
> e10 := coeff(e4, x, 0):
> e11 := solve({e5, e6, e7, e8, e9, e10}, {c5, c4, c3, c2, c1, c0}):
> assign(e11):
> e12 := e2:
> e13 := factor(coeff(e12, x, 4)):
> e14 := numer(e13) mod 2:
> subs(a = 0, e14): subs(a = 1, e14) mod 2:
We see two cases.
> e15 := subs(a = 2*m, b = 2*n + 1, e12):
> e16 := factor(coeff(e15, x, 4)):
> e17 := subs(n = 2*u + 1 + m, e15):
> e18 := factor(coeff(e17, x, 2)):
> e19 := subs(m = 2*v + 1, e17):
> e20 := denom(e19):
We have a new condition. a = 2 mod 4 and b = 1 mod 4. Next subcase.
> e21 := subs(a = 2*m + 1, b = 2*n, e12):
> e22 := factor(coeff(e21, x, 4)):
> e23 := subs(m = 2*u + 1, e21):
> e24 := factor(coeff(e23, x, 3)):
Cannot be in Z. end of case.

Case10010-

> restart: element := (a0 + a1*x + a2*x^2 + a3*x^3 + a4*x^4 + x^5)/2:
> poly := x^6 + a*x^4 + b*x^2 - 1:
> e1 := subs(a0 = 1, a1 = 0, a2 = 0, a3 = 1, a4 = 0, element):
> e2 := x^6 + c5*x^5 + c4*x^4 + c3*x^3 + c2*x^2 + c1*x + c0:
> e3 := subs(x = e1, e2):
> e4 := rem(e3, poly, x):
> e5 := coeff(e4, x, 5):
> e6 := coeff(e4, x, 4):
> e7 := coeff(e4, x, 3):
> e8 := coeff(e4, x, 2):
> e9 := coeff(e4, x, 1):
> e10 := coeff(e4, x, 0):
> e11 := solve({e5, e6, e7, e8, e9, e10}, {c5, c4, c3, c2, c1, c0}):
> assign(e11):
> e12 := e2:
> e13 := factor(coeff(e12, x, 4)):
> e14 := numer(e13):
> e15 := subs(a = 0, e14) mod 2: subs(a = 1, e14) mod 2:

We follow one case.

> e16 := subs(a = 2*m, b = 2*n, e12):
> e17 := factor(coeff(e16, x, 0)):

Can't be in Z. end of case.

Case10011-

> restart:
element := (a0 + a1*x + a2*x^2 + a3*x^3 + a4*x^4 + x^5)/2:

> poly := x^6 + a*x^4 + b*x^2 - 1:
> e1 := subs(a0=1, a1=0, a2=0, a3=1, a4=1, element):
> e2 := x^6 + c5*x^5 + c4*x^4 + c3*x^3 + c2*x^2 + c1*x + c0:
> e3 := subs(x = e1, e2):
> e4 := rem(e3, poly, x):
> e5 := coeff(e4, x, 5):
> e6 := coeff(e4, x, 4):
> e7 := coeff(e4, x, 3):
\begin{verbatim}
> e8 := coeff(e4, x, 2):
> e9 := coeff(e4, x, 1):
> e10 := coeff(e4, x, 0):
> e11 := solve({e5, e6, e7, e8, e9, e10}, {c5, c4, c3, c2, c1, c0}):
> assign(e11):
> e12 := e2:
> e13 := factor(coeff(e12, x, 4)):
> e14 := numer(e13) mod 4:
> e15 := subs(a = 0, e14) mod 2: subs(a = 1, e14) mod 2:

We have two cases.

> e16 := subs(a = 2*m, b = 2*n, e12):
> e17 := factor(coeff(e16, x, 4)):
> e18 := subs(n = 2*u, e16):
> e19 := factor(coeff(e18, x, 3)):

Cannot be in \( \mathbb{Z} \), next subcase.

> e20 := subs(a = 2*m + 1, e12):
> e21 := factor(coeff(e20, x, 4)):
> e22 := numer(e21) mod 4:
> e23 := subs(b = 0, e22) mod 4: subs(b = 1, e22) mod 4: subs(b = 2, e22) mod 4:
> subs(b = 3, e22) mod 4:

There are three cases to consider.

> e24 := subs(b = 4*n + 1, m = 2*u + 1, e20):
> e25 := factor(coeff(e24, x, 2)):

Cannot be in \( \mathbb{Z} \). Next subcase.

> e26 := subs(b = 4*n + 2, e20):
> e27 := factor(coeff(e26, x, 3)):
> e28 := factor(subs(m = 2*u + 1, e26)):
> e29 := denom(e28):
\end{verbatim}
We have a new condition. It is $a = 3 \mod 4$ and $b = 2 \mod 4$. Next subcase.

```plaintext
>e30:=subs(b=4*n+3,m=2*u,e20):
e31:=factor(coeff(e30,x,0)):
e32:=(numer(e31) mod 4):
e33:=subs(n=u+1+2*v,e30):
denom(e33):
```

We have a new condition $(a,b) = (1,7)$ or $(5,3) \mod 8$.

Case10100-

```plaintext
>restart:element:=(a0+a1*x+a2*x^2+a3*x^3+a4*x^4+x^5)/2:
poly:=x^6+a*x^4+b*x^2-1:
e1:=subs(a0=1,a1=0,a2=1,a3=0,a4=0,element):
e2:=x^6+c5*x^5+c4*x^4+c3*x^3+c2*x^2+c1*x+c0:
e3:=subs(x=e1,e2):
e4:=rem(e3,poly,x):
e5:=coeff(e4,x,5):
e6:=coeff(e4,x,4):
e7:=coeff(e4,x,3):
e8:=coeff(e4,x,2):
e9:=coeff(e4,x,1):
e10:=coeff(e4,x,0):
e11:=solve({e5,e6,e7,e8,e9,e10},{c5,c4,c3,c2,c1,c0}):
assign(e11):
e12:=e2:
e13:=coeff(e12,x,4):
e14:=numer(e13):denom(e13):
e15:=subs(a=0,e14) mod 2:
e16:=subs(a=1,e14) mod 2:
e17:=subs(b=a+1+2*m,e12):
```
\begin{verbatim}
> e18 := factor(coeff(e17, x, 4));
> e19 := numer(e18) mod 2;
> e20 := factor(coeff(e17, x, 3));
> e21 := numer(e20) : denom(e20);
> e22 := subs(a = 0, e21) mod 4 : subs(a = 1, e21) mod 4 : subs(a = 2, e21) mod 4 : subs(a = 3, e21) mod 4:

    Cannot be in \( \mathbb{Z} \). End of case.

Case 10101-

> restart: element := (a0 + a1*x + a2*x^2 + a3*x^3 + a4*x^4 + x^5)/2:
> poly := x^6 + a*x^4 + b*x^2 - 1:
> e1 := subs(a0 = 1, a1 = 0, a2 = 1, a3 = 0, a4 = 1, element):
> e2 := x^6 + c5*x^5 + c4*x^4 + c3*x^3 + c2*x^2 + c1*x + c0:
> e3 := subs(x = e1, e2):
> e4 := rem(e3, poly, x):
> e5 := coeff(e4, x, 5):
> e6 := coeff(e4, x, 4):
> e7 := coeff(e4, x, 3):
> e8 := coeff(e4, x, 2):
> e9 := coeff(e4, x, 1):
> e10 := coeff(e4, x, 0):
> e11 := solve({e5, e6, e7, e8, e9, e10}, {c5, c4, c3, c2, c1, c0}):
> assign(e11):
> e12 := e2:
> e13 := factor(coeff(e12, x, 4)):
> e14 := numer(e13) : denom(e13):
> e15 := subs(a = 0, e14) mod 2 : subs(a = 1, e14) mod 2:
> e16 := subs(b = 2*m + 1, e12):
> e17 := factor(coeff(e16, x, 4)):
\end{verbatim}
We have three subcases to consider.

We have three subcases to consider.

Cannot be in \(\mathbb{Z}\). Next subcase.

Cannot be in \(\mathbb{Z}\). End of subcase. Final subcase.

Case 10110-

Cannot be in \(\mathbb{Z}\). End of subcase. Final subcase.
> e7 := coeff(e4, x, 3):
> e8 := coeff(e4, x, 2):
> e9 := coeff(e4, x, 1):
> e10 := coeff(e4, x, 0):
> e11 := solve({e5, e6, e7, e8, e9, e10}, {c5, c4, c3, c2, c1, c0}):
> assign(e11):
> e12 := e2:
> e13 := factor(coeff(e12, x, 4)):
> e14 := numer(e13): denom(e13):
> e15 := subs(a = 0, e14) mod 2: subs(a = 1, e14) mod 2:

We have two subcases.
> e16 := subs(a = 2*m, b = 2*n, e12):
> e17 := factor(coeff(e16, x, 4)):
> e17a := subs(n = 2*u, e16):
> e17b := factor(coeff(e17a, x, 3)):
> e17c := subs(m = 2*v, e17a):
> e17d := factor(coeff(e17c, x, 0)):

We have a condition a = 0 mod 4 and b = 0 mod 4. Next subcase
> e18 := subs(a = 2*m + 1, e12):
> e19 := factor(coeff(e18, x, 4)):
> e20 := numer(e19):
> e21 := subs(b = 0, e20) mod 4: subs(b = 1, e20) mod 4: subs(b = 2, e20) mod 4: subs(b = 3, e20) mod 4:

We consider three cases.
> e22 := factor(subs(b = 4*n + 1, m = 2*u + 1, e18)):
> e23 := factor(coeff(e22, x, 2)):

Cannot be in Z. Next subcase.
> e24 := factor(subs(b = 4*n + 2, e18)):
\texttt{\textgreater{}e25:=factor(coeff(e24,x,3)):\nCannot be in Z. Next subcase.\n\texttt{\textgreater{}e26:=factor(subs(b=4*n+3,m=2*u,e18)):\n\texttt{\textgreater{}e27:=denom(e26):\nWe have a new case. (a,b) = (1,3) mod 4.\nCase10111-\n\texttt{\textgreater{}restart:element:=(a0+a1*x+a2*x^2+a3*x^3+a4*x^4+x^5)/2:\n\texttt{poly:=x^6+a*x^4+b*x^2-1:\n\texttt{e1:=subs(a0=1,a1=0,a2=1,a3=1,a4=1,element):\n\texttt{e2:=x^6+c5*x^5+c4*x^4+c3*x^3+c2*x^2+c1*x+c0:\n\texttt{e3:=subs(x=e1,e2):\n\texttt{e4:=rem(e3,poly,x):\n\texttt{e5:=coeff(e4,x,5):\n\texttt{e6:=coeff(e4,x,4):\n\texttt{e7:=coeff(e4,x,3):\n\texttt{e8:=coeff(e4,x,2):\n\texttt{e9:=coeff(e4,x,1):\n\texttt{e10:=coeff(e4,x,0):\n\texttt{e11:=solve({e5,e6,e7,e8,e9,e10},{c5,c4,c3,c2,c1,c0}):\n\texttt{assign(e11):\n\texttt{e12:=e2:}\n\texttt{e13:=factor(coeff(e12,x,4)):\n\texttt{e14:=numer(e13):denom(e13):\n\texttt{e15:=subs(a=0,e14) mod 2:subs(a=1,e14) mod 2:\n\texttt{e16:=subs(a=2*m,b=2*n,e12):\n\texttt{e17:=factor(coeff(e16,x,4)):\n\texttt{e18:=subs(n=2*u+1,e16):\n\texttt{e19:=factor(coeff(e18,x,3)):}
Cannot be in Z. End of case.

Case 11000-

\[ \text{restart: element:} = \frac{(a_0 + a_1 x + a_2 x^2 + a_3 x^3 + a_4 x^4 + x^5)}{2} : \]
\[ \text{poly:} = x^6 + a x^4 + b x^2 - 1 : \]
\[ e_1 := \text{subs}(a_0 = 1, a_1 = 1, a_2 = 0, a_3 = 0, a_4 = 0, \text{element}) : \]
\[ e_2 := x^6 + c_5 x^5 + c_4 x^4 + c_3 x^3 + c_2 x^2 + c_1 x + c_0 : \]
\[ e_3 := \text{subs}(x = e_1, e_2) : \]
\[ e_4 := \text{rem}(e_3, \text{poly}, x) : \]
\[ e_5 := \text{coeff}(e_4, x, 5) : \]
\[ e_6 := \text{coeff}(e_4, x, 4) : \]
\[ e_7 := \text{coeff}(e_4, x, 3) : \]
\[ e_8 := \text{coeff}(e_4, x, 2) : \]
\[ e_9 := \text{coeff}(e_4, x, 1) : \]
\[ e_{10} := \text{coeff}(e_4, x, 0) : \]
\[ e_{11} := \text{solve}\left\{ e_5, e_6, e_7, e_8, e_9, e_{10}\right\}, \{c_5, c_4, c_3, c_2, c_1, c_0\} : \]
\[ \text{assign}(e_{11}) : \]
\[ e_{12} := e_2 : \]
\[ e_{13} := \text{factor}(\text{coeff}(e_{12}, x, 4)) : \]
\[ e_{14} := \text{numer}(e_{13}) : \text{denom}(e_{13}) : \]
\[ e_{15} := \text{subs}(a = 0, e_{14}) \mod 2 : \text{subs}(a = 1, e_{14}) \mod 2 : \]

We have two cases.

\[ e_{16} := \text{subs}(a = 2m, b = 2n + 1, e_{12}) : \]
\[ e_{17} := \text{factor}(\text{coeff}(e_{16}, x, 2)) : \]

Cannot be in Z. Next subcase.

\[ e_{18} := \text{subs}(a = 2m + 1, b = 2n, e_{12}) : \]
\[ e_{19} := \text{factor}(\text{coeff}(e_{18}, x, 2)) : \]
\[ e_{20} := \text{numer}(e_{19}) : \text{denom}(e_{19}) : \]
\[ e_{21} := \text{subs}(m = 0, e_{20}) \mod 2 : \text{subs}(m = 1, e_{20}) \mod 2 : \]
We have a new condition. \(a = 3 \text{ mod 4}\) and \(b = 2 \text{ mod 4}\).

We can see two cases.
\( e_{20} := \text{factor}(\text{coeff}(e_{19}, x, 3)) \):

Cannot be in \( \mathbb{Z} \). Next subcase.

\( e_{21} := \text{subs}(a=2n+1, e_{15}) \):

\( e_{22} := \text{factor}(\text{coeff}(e_{21}, x, 0)) \):

\( e_{23} := \text{subs}(n=m+1+2k, e_{21}) \):

\( e_{24} := \text{denom}(e_{23}) \):

We have a new condition \((a, b) = (3, 1) \text{ or } (1, 3) \mod 4\). End of case.

Case 11010-

\( \text{restart}: \text{element} := (a0+a1*x+a2*x^2+a3*x^3+a4*x^4+x^5)/2: \)

\( \text{poly} := x^6+a*x^4+b*x^2-1:\)

\( e1 := \text{subs}(a0=1, a1=1, a2=0, a3=1, a4=0, \text{element}): \)

\( e2 := x^6+c5*x^5+c4*x^4+c3*x^3+c2*x^2+c1*x+c0: \)

\( e3 := \text{subs}(x=e1, e2): \)

\( e4 := \text{rem}(e3, \text{poly}, x): \)

\( e5 := \text{coeff}(e4, x, 5): \)

\( e6 := \text{coeff}(e4, x, 4): \)

\( e7 := \text{coeff}(e4, x, 3): \)

\( e8 := \text{coeff}(e4, x, 2): \)

\( e9 := \text{coeff}(e4, x, 1): \)

\( e10 := \text{coeff}(e4, x, 0): \)

\( e11 := \text{solve}\{e5, e6, e7, e8, e9, e10\},\{c5, c4, c3, c2, c1, c0\} ): \)

\( \text{assign}(e11): \)

\( e12 := e2: \)

\( e13 := \text{factor}(\text{coeff}(e12, x, 4)): \)

\( e14 := \text{numer}(e13): \text{denom}(e13): \)

\( e15 := \text{subs}(a=0, e14) \mod 2: \text{subs}(a=1, e14) \mod 2: \)

We see two cases.

\( e16 := \text{subs}(a=2m, b=2n, e12): \)
\[ e_{17} := \text{factor}(\text{coeff}(e_{16}, x, 2)) : \]
Cannot be in \( \mathbb{Z} \). end of subcase. Next...
\[ e_{18} := \text{subs}(a = 2m + 1, e_{12}) : \]
\[ e_{19} := \text{factor}(\text{coeff}(e_{18}, x, 4)) : \]
\[ e_{20} := \text{numer}(e_{19}) : \]
\[ \text{subs}(b = 0, e_{20}) \mod 4 : \text{subs}(b = 1, e_{20}) \mod 4 : \text{subs}(b = 2, e_{20}) \mod 4 : \]
\[ \text{subs}(b = 3, e_{20}) \mod 4 : \]

There are 3 subcases here.
\[ e_{21} := \text{subs}(b = 4n, m = 2u + 1, e_{18}) : \]
\[ e_{22} := \text{factor}(\text{coeff}(e_{21}, x, 1)) : \]
Cannot be in \( \mathbb{Z} \). Next subcase.
\[ e_{23} := \text{subs}(b = 4n + 2, m = 2u, e_{18}) : \]
\[ e_{24} := \text{factor}(\text{coeff}(e_{23}, x, 2)) : \]
Cannot be in \( \mathbb{Z} \). Last subcase.
\[ e_{25} := \text{subs}(b = 4n + 3, e_{18}) : \]
\[ e_{26} := \text{factor}(\text{coeff}(e_{25}, x, 2)) : \]

For \( \text{numer}(e_{26}) \) to be even the first thing we need is \( m \) even.
\[ e_{27} := \text{subs}(m = 2u, e_{25}) : \]
\[ e_{28} := \text{factor}(\text{coeff}(e_{27}, x, 2)) : \]
\[ e_{29} := \text{numer}(e_{28}) \mod 4 : \text{denom}(e_{28}) : \]
\[ e_{30} := \text{subs}(u = 3 + 2n + 4v, e_{27}) : \]
\[ e_{31} := \text{factor}(\text{coeff}(e_{30}, x, 0)) : \]
\[ e_{32} := \text{subs}(n = 4w, e_{31}) : \]
\[ e_{33} := \text{numer}(e_{32}) \mod 4 : \]
\[ e_{34} := \text{factor}(\text{subs}(v = w + 3 + 4z, e_{32})) : \]

We have a new condition. \((a,b) = (61,3) (45,19), (29,35), (13,51) \mod 64.\)

Case11011-
\[ \text{restart: element:} = (a_0 + a_1 x + a_2 x^2 + a_3 x^3 + a_4 x^4 + x^5) / 2 : \]

225
\[ \text{poly} := x^6 + a x^4 + b x^2 - 1: \]
\[ \text{e1} := \text{subs}(a0=1, a1=1, a2=0, a3=1, a4=1, \text{element}): \]
\[ \text{e2} := x^6 + c5 x^5 + c4 x^4 + c3 x^3 + c2 x^2 + c1 x + c0: \]
\[ \text{e3} := \text{subs}(x=e1, e2): \]
\[ \text{e4} := \text{rem}(e3, \text{poly}, x): \]
\[ \text{e5} := \text{coeff}(e4, x, 5): \]
\[ \text{e6} := \text{coeff}(e4, x, 4): \]
\[ \text{e7} := \text{coeff}(e4, x, 3): \]
\[ \text{e8} := \text{coeff}(e4, x, 2): \]
\[ \text{e9} := \text{coeff}(e4, x, 1): \]
\[ \text{e10} := \text{coeff}(e4, x, 0): \]
\[ \text{e11} := \text{solve}\{\text{e5, e6, e7, e8, e9, e10}\}, \{c5, c4, c3, c2, c1, c0\}): \]
\[ \text{assign}(\text{e11}): \]
\[ \text{e12} := \text{e2}: \]
\[ \text{e13} := \text{factor}(\text{coeff}(\text{e12}, x, 4)): \]
\[ \text{e14} := \text{numer}(\text{e13}): \]
\[ \text{e15} := \text{subs}(a=0, \text{e14}) \text{ mod } 2: \text{subs}(a=1, \text{e14}) \text{ mod } 2: \]
\[ \text{e16} := \text{subs}(a=2 * m, \text{e12}): \]
\[ \text{e17} := \text{factor}(\text{coeff}(\text{e16}, x, 4)): \]
\[ \text{e18} := \text{subs}(b=2 * n, \text{e16}): \]
\[ \text{e19} := \text{factor}(\text{coeff}(\text{e18}, x, 1)): \]

\text{Cannot be in } \mathbb{Z}. \text{ end of case.}

\text{Case11100-}

\[ \text{restart: element := (a0+a1*x+a2*x^2+a3*x^3+a4*x^4+x^5)/2:} \]
\[ \text{poly := x^6 + a x^4 + b x^2 - 1:} \]
\[ \text{e1 := subs(a0=1, a1=1, a2=1, a3=0, a4=0, element):} \]
\[ \text{e2 := x^6 + c5 x^5 + c4 x^4 + c3 x^3 + c2 x^2 + c1 x + c0:} \]
\[ \text{e3 := subs(x=e1, e2):} \]
\[ e_4 := \text{rem}(e_3, \text{poly}, x) \]
\[ e_5 := \text{coeff}(e_4, x, 5) \]
\[ e_6 := \text{coeff}(e_4, x, 4) \]
\[ e_7 := \text{coeff}(e_4, x, 3) \]
\[ e_8 := \text{coeff}(e_4, x, 2) \]
\[ e_9 := \text{coeff}(e_4, x, 1) \]
\[ e_{10} := \text{coeff}(e_4, x, 0) \]
\[ e_{11} := \text{solve} \{ e_5, e_6, e_7, e_8, e_9, e_{10}, \{ c_5, c_4, c_3, c_2, c_1, c_0 \} \} \]
\[ \text{assign}(e_{11}) \]
\[ e_{12} := e_2 \]
\[ e_{13} := \text{factor}(\text{coeff}(e_{12}, x, 4)) \]
\[ e_{14} := \text{numer}(e_{13}) \]
\[ e_{15} := \text{subs}(a = 0, e_{14}) \mod 2 \]
\[ e_{16} := \text{subs}(a = 1, e_{14}) \mod 2 \]
\[ e_{17} := \text{factor}(\text{coeff}(e_{16}, x, 4)) \]
\[ e_{18} := \text{numer}(e_{17}) \]
\[ e_{19} := \text{subs}(a = 0, e_{18}) \mod 4 \]
\[ e_{20} := \text{subs}(a = 2 \cdot n, m = 2 \cdot v, e_{16}) \]
\[ e_{21} := \text{factor}(\text{coeff}(e_{20}, x, 2)) \]
\[ e_{21a} := \text{subs}(n = 2 \cdot w + 1, e_{20}) \]
\[ e_{21b} := \text{denom}(e_{21a}) \]

We see two cases. Subcase 1.
\[ e_{22} := \text{subs}(a = 2 \cdot n + 1, e_{16}) \]
\[ e_{23} := \text{factor}(\text{coeff}(e_{22}, x, 3)) \]
\[ e_{24} := \text{subs}(n = m + 1 + 2 \cdot k, e_{22}) \]
\[ e_{25} := \text{factor}(\text{coeff}(e_{24}, x, 2)) \]
\[
e^{26} := \text{numer}(e^{25}) \mod 4:
\]
\[
e^{27} := \text{subs}(m = 2u + 1, e^{24}):
\]
\[
e^{28} := \text{factor}(\text{coeff}(e^{27}, x, 0)):
\]
\[
e^{29} := \text{numer}(e^{28}) \cdot \text{denom}(e^{28}):
\]
\[
e^{30} := e^{29} \mod 4:
\]
\[
e^{31} := \text{subs}(k = 2 + 2u + 2w, e^{27}):
\]
\[
\text{denom}(e^{31}):
\]

We have a new condition. It is \((a, b) = (5, 3)\) or \((1, 7)\) mod 8.

Case 11101-
\[
\text{restart: element:} = (a0 + a1x + a2x^2 + a3x^3 + a4x^4 + x^5)/2:
\]
\[
\text{poly:} = x^6 + a \cdot x^4 + b \cdot x^2 - 1:
\]
\[
e^{1} := \text{subs}(a0 = 1, a1 = 1, a2 = 1, a3 = 0, a4 = 1, \text{element}):
\]
\[
e^{2} = x^6 + c5x^5 + c4x^4 + c3x^3 + c2x^2 + c1x + c0:
\]
\[
e^{3} := \text{subs}(x = e^{1}, e^{2}):
\]
\[
e^{4} := \text{rem}(e^{3}, \text{poly}, x):
\]
\[
e^{5} := \text{coeff}(e^{4}, x, 5):
\]
\[
e^{6} := \text{coeff}(e^{4}, x, 4):
\]
\[
e^{7} := \text{coeff}(e^{4}, x, 3):
\]
\[
e^{8} := \text{coeff}(e^{4}, x, 2):
\]
\[
e^{9} := \text{coeff}(e^{4}, x, 1):
\]
\[
e^{10} := \text{coeff}(e^{4}, x, 0):
\]
\[
e^{11} := \text{solve} \{e^{5}, \text{e6}, \text{e7}, \text{e8}, \text{e9}, \text{e10}\}, \{c5, c4, c3, c2, c1, c0\}):
\]
\[
\text{assign}(e^{11}):
\]
\[
e^{12} := e^{2}:
\]
\[
e^{13} := \text{factor}(\text{coeff}(e^{12}, x, 4)):
\]
\[
e^{14} := \text{numer}(e^{13}):
\]
\[
e^{15} := \text{subs}(a = 0, e^{14}) \mod 2:
\]
\[
e^{16} := \text{subs}(a = 1, e^{14}) \mod 2:
\]
We have two cases.

\[ e_{17} := \text{subs}(a=2m, b=2n+1, e_{12}) : \]
\[ e_{18} := \text{factor}(\text{coeff}(e_{17}, x, 4)) : \]
\[ e_{19} := \text{subs}(n=2u, e_{17}) : \]
\[ e_{20} := \text{factor}(\text{coeff}(e_{19}, x, 2)) : \]

Cannot be in $\mathbb{Z}$. Next subcase.

\[ e_{21} := \text{subs}(a=2m+1, b=2n, e_{12}) : \]
\[ e_{22} := \text{factor}(\text{coeff}(e_{21}, x, 4)) : \]

Cannot be in $\mathbb{Z}$. End of case.

Case 11110-

\[ \text{restart}: \text{element} := \frac{(a_0+a_1x+a_2x^2+a_3x^3+a_4x^4+x^5)}{2} : \]
\[ \text{poly} := x^6+ax^4+bx^2-1 : \]
\[ e_1 := \text{subs}(a_0=1, a_1=1, a_2=1, a_3=1, a_4=0, \text{element}) : \]
\[ e_2 := x^6+c_5x^5+c_4x^4+c_3x^3+c_2x^2+c_1x+c_0 : \]
\[ e_3 := \text{subs}(x=e_1, e_2) : \]
\[ e_4 := \text{rem}(e_3, \text{poly}, x) : \]
\[ e_5 := \text{coeff}(e_4, x, 5) : \]
\[ e_6 := \text{coeff}(e_4, x, 4) : \]
\[ e_7 := \text{coeff}(e_4, x, 3) : \]
\[ e_8 := \text{coeff}(e_4, x, 2) : \]
\[ e_9 := \text{coeff}(e_4, x, 1) : \]
\[ e_{10} := \text{coeff}(e_4, x, 0) : \]
\[ e_{11} := \text{solve} \{e_5, e_6, e_7, e_8, e_9, e_{10}\}, \{c_5, c_4, c_3, c_2, c_1, c_0\} : \]
\[ \text{assign}(e_{11}) : \]
\[ e_{12} := e_2 : \]
\[ e_{13} := \text{factor}(\text{coeff}(e_{12}, x, 4)) : \]
\[ e_{14} := \text{numer}(e_{13}) : \]
\[ e_{15} := \text{subs}(a=0, e_{14}) \mod 2 : \]
\[ e_{16} := \text{subs}(a=1, e_{14}) \mod 2: \]
\[ e_{17} := \text{subs}(a=2m, b=2n, e_{12}): \]
\[ e_{18} := \text{factor}(\text{coeff}(e_{17}, x, 4)): \]
\[ e_{19} := \text{subs}(n=m+1+2k, e_{17}): \]
\[ e_{20} := \text{factor}(\text{coeff}(e_{19}, x, 3)): \]
\[ e_{21} := \text{subs}(m=2u+1, e_{19}): \]
\[ e_{22} := \text{factor}(\text{coeff}(e_{21}, x, 1)): \]

Cannot be in \( Z \). End of case.

Case11111-

\[ \text{restart: element} := (a0+a1*x+a2*x^2+a3*x^3+a4*x^4+x^5)/2: \]
\[ \text{poly} := x^6+a*x^4+b*x^2-1: \]
\[ e1 := \text{subs}(a0=1, a1=1, a2=1, a3=1, a4=1, \text{element}): \]
\[ e2 := x^6+c5*x^5+c4*x^4+c3*x^3+c2*x^2+c1*x+c0: \]
\[ e3 := \text{subs}(x=e1, e2): \]
\[ e4 := \text{rem}(e3, \text{poly}, x): \]
\[ e5 := \text{coeff}(e4, x, 5): \]
\[ e6 := \text{coeff}(e4, x, 4): \]
\[ e7 := \text{coeff}(e4, x, 3): \]
\[ e8 := \text{coeff}(e4, x, 2): \]
\[ e9 := \text{coeff}(e4, x, 1): \]
\[ e10 := \text{coeff}(e4, x, 0): \]
\[ e11 := \text{solve}\{e5, e6, e7, e8, e9, e10\}, \{c5, c4, c3, c2, c1, c0\}: \]
\[ \text{assign}(e11): \]
\[ e12 := e2: \]
\[ e13 := \text{factor}(\text{coeff}(e12, x, 4)): \]
\[ e14 := \text{numer}(e13): \]
\[ e15 := \text{subs}(a=0, e14) \mod 2: \text{subs}(a=1, e14) \mod 2: \]

We have two cases.
\[ e_{16} := \text{subs}(a=2*m, b=2*n, e_{12}) : \]
\[ e_{17} := \text{factor} \left( \text{coeff} (e_{16}, x, 4) \right) : \]
\[ e_{18} := \text{subs} (n=m+2*u, e_{16}) : \]
\[ e_{19} := \text{factor} \left( \text{coeff} (e_{18}, x, 0) \right) : \]
\[ \text{denom} (e_{18}) : \]

We have two new conditions. \(a=0 \text{ mod } 4\) and \(b = 0 \text{ mod } 4\) or \(a=2 \text{ mod } 4\) and \(b = 2 \text{ mod } 4\). Last subcase.

\[ e_{20} := \text{subs} (a=2*m+1, e_{12}) : \]
\[ e_{21} := \text{factor} \left( \text{coeff} (e_{20}, x, 4) \right) : \]
\[ e_{22} := \text{numer} (e_{21}) \mod 4 : \]
\[ e_{23} := \text{subs} (b=0, e_{22}) \mod 4 : \text{subs} (b=1, e_{22}) \mod 4 : \text{subs} (b=2, e_{22}) \mod 4 : \]
\[ \text{subs} (b=3, e_{22}) \mod 4 : \]

We have 3 more subcases.

\[ e_{24} := \text{subs} (b=4*n, m=2*u, e_{20}) : \]
\[ e_{25} := \text{factor} \left( \text{coeff} (e_{24}, x, 3) \right) : \]

Cannot be in \(Z\), next subcase.

\[ e_{26} := \text{subs} (b=4*n+2, m=2*u+1, e_{20}) : \]
\[ e_{27} := \text{factor} \left( \text{coeff} (e_{26}, x, 2) \right) : \]

Cannot be in \(Z\), last subcase.

\[ e_{28} := \text{subs} (b=4*n+3, e_{20}) : \]
\[ e_{29} := \text{factor} \left( \text{coeff} (e_{28}, x, 3) \right) : \]
\[ e_{30} := \text{subs} (m=2*v, e_{28}) : \]
\[ e_{31} := \text{factor} \left( \text{coeff} (e_{30}, x, 2) \right) : \]
\[ e_{32} := \text{subs} (n=4*w, e_{30}) : \]
\[ e_{33} := \text{factor} \left( \text{coeff} (e_{32}, x, 1) \right) : \]
\[ e_{34} := \text{numer} (e_{33}) \mod 4 : \]
\[ e_{35} := \text{subs} (v=3+4*z, e_{32}) : \]
\[ e_{36} := \text{factor} \left( \text{coeff} (e_{35}, x, 0) \right) : \]
\begin{verbatim}
> e37:=numer(e36):denom(e36):
> e38:=subs(w=0,e37) mod 4:subs(w=1,e37) mod 4:subs(w=2,e37) mod 4:
> subs(w=3,e37) mod 4:
> e39:=subs(z=3*w+3+4*y,e35):
> denom(e39):

We have one last condition, \((a,b) = (61,3)\), \((45,19)\), \((29,35)\), \((13,51)\) mod 64.
\end{verbatim}