On the Galois Groups of Sextic Trinomials

by

Stephen Christopher Brown

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

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

MASTER OF SCIENCE

in

The College of Graduate Studies

(Mathematics)

THE UNIVERSITY OF BRITISH COLUMBIA

(Okanagan)

August 2011

Abstract

It is well known that the general polynomial

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

cannot be solved algebraically for $n \geq 5$; that is, it cannot be solved in terms of a finite number of arithmetic operations and radicals. We can, however, associate every irreducible sextic polynomial with a Galois group. The Galois group of a given polynomial can give us a great deal of information about the nature of the roots of a polynomial and it can also tell us if the polynomial itself is algebraically solvable. This leads to the typical problem in Galois theory: finding the Galois group of a given polynomial.

In this thesis, we investigate the inverse problem: for a specific Galois group, what irreducible polynomials occur. More specifically, we look at monic trinomials – polynomials with only three terms, having 1 as the leading coefficient. The first unresolved case of trinomials are of degree six and we will look specifically at trinomials of the form

$$x^6 + ax + b.$$

We begin by investigating families of these trinomials that will result in Galois groups having a particular structure. From these families of trinomials, we can then make a final determination of individual Galois groups after eliminating any reducible possibilities.

In the main calculations of this thesis, we investigate two parametric families of trinomials, one of which is given in [1]. From these families we completely characterize five of the possible sixteen Galois groups that

can occur for sextic polynomials. In the notation of Butler and Mckay [2], these groups are 6T1, 6T2, 6T4, 6T5, and 6T6. In the final determination of these polynomials, rational points are found on genus 2 curves using a method known as elliptic Chabauty.

We give an introduction to Galois theory followed by a brief explanation of the methods used to attain our results. We then discuss our results and proceed to prove them through the use of powerful software such as MAPLE$^{\mathrm{TM}}$and the Magma algebra system [3].

Preface

The main results discussed in Chapter 5 and Chapter 6 are from collaborative research done with Dr. Blair Spearman and Dr. Qiduan Yang. The results discussed in Chapter 5 are from the paper [4] and all authors listed contributed to this paper as well as the results discussed in Chapter 6, which are intended to be published in a subsequent paper. In both of these chapters I have been responsible for finding rational solutions to genus 2 curves using software such as MAPLE$^{\mathrm{TM}}$and the Magma algebra system [3]. I have also contributed to the editing of these papers.

Table of Contents

Appendices

List of Tables

Acknowledgements

I am very grateful for all the encouragement I have received from my family and from a network of friends. I thank these amazing people for all the support they have given me.

I would also like to thank my wonderful committee of professors: Dr. Blair Spearman, Dr. Qiduan Yang, Dr. Shawn Wang, and Dr. Rebecca Tyson. They have contributed to the completion of this thesis through their guidance and exceptional teaching, which have helped me get through my education this far.

I would especially like to recognize my supervisor, Dr. Blair Spearman, who has always given me encouragement and confidence in myself. You have played an integral role in my decision to continue my education and you inspire me for what I could achieve in the future.

Chapter 1

Algebraic Preliminaries

1.1 Homomorphisms, Quotient Rings, and Ideals

We begin with some basic definitions regarding rings and maps.

Definition 1.1. *A ring is a triple $\langle R, +, \cdot \rangle$, where R is a set with two binary operations $+$ and $\cdot$ defined on R such that*

i. $\langle R, + \rangle$ *is an abelian group;*

ii. $\cdot$ *is associative; and*

iii. for all $a, b, c, \in R$, the left distributive law

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c)$$

and the right distributive law

$$(a + b) \cdot c = (a \cdot c) + (b \cdot c)$$

hold. We call $+$ addition and $\cdot$ multiplication. We shall write ab instead of $a \cdot b$.

Definition 1.2 (Homomorphism)**.** *For rings R and S, a map $\phi : R \to S$ is a homomorphism if the following two conditions are satisfied for all $a, b \in R$:*

i. $\phi(a + b) = \phi(a) + \phi(b)$

ii. $\phi(ab) = \phi(a)\phi(b)$.

Definition 1.3 (Isomorphism)**.** *An isomorphism $\phi : R \to S$ from a ring R to a ring S is a homomorphism that is one to one and onto S.*

If an isomorphism exists from a ring R to a ring S, then R is said to be isomorphic to S and we write $R \cong S$.

Definition 1.4 (Subring)**.** *A subring of a ring R is a subset S of R which is itself a ring under the operations it inherits from R.*

Definition 1.5 (Ideal)**.** *A subset I of a ring R is an ideal of R if*

i. $\langle I, + \rangle$ *is a group under the addition operation defined in R and*

ii. for all $x \in I$ and for all $r \in R$, $xr \in R$.

With the idea of ideals, we can now define a quotient ring. First we must understand the concept of cosets.

Definition 1.6 (Cosets)**.** *Let H be a subgroup of G. The subset $aH = \{ah \mid h \in H\}$ is called the left coset of H containing a, whereas the subset $Ha = \{ha \mid h \in H\}$ is called the right coset of H containing a.*

In the case where addition is the group operation, we write $a + H = \{a + h \mid h \in H\}$ and $H + a = \{h + a \mid h \in H\}$ as the left and right cosets of H containing a, respectively.

Remark 1.1. *In the case where G is an abelian group, the left and right cosets of H containing a are equal.*

Definition 1.7 (Quotient ring)**.** *If I is an ideal of a ring R, we can form the quotient ring R/I, consisting of the cosets of I in R considered as a group under addition, having the properties*

i. $(I + r) + (I + s) = I + (r + s)$

ii. $(I + r)(I + s) = I + (rs)$.

Definition 1.8 (Kernel of a homomorphism)**.** *Let a map $\phi : R \to S$ be a ring homomorphism. The subring*

$$\phi^{-1}(0_s) = \{r \in R \mid \phi(r) = 0_s\}$$

is the kernal of ϕ where 0_s is the zero element in S. We denote the kernel of ϕ by $Ker(\phi)$.

It should also be noted that the kernel $Ker(\phi)$ of a ring homomorphism $\phi : R \to S$ is an ideal of R. The concept of an integral domain and a field will also be useful for later definitions. An integral domain is a ring D with an additional three properties.

Definition 1.9 (Integral Domain)**.** *An integral domain is a ring $\langle D, +, \cdot \rangle$ such that*

i. $\cdot$ is commutative;

ii. there exists an element $1 \in D$ such that $a1 = 1a = a$ for all $a \in D$; and

iii. if $ab = 0$ for $a, b, \in D$ then either $a = 0$ or $b = 0$.

Finally, we can build onto this concept one step further to define a field.

Definition 1.10 (Field)**.** *A field is a ring $\langle F, +, \cdot \rangle$ such that $F \backslash \{0\}$ is an abelian group under multiplcation.*

In this definition, $f \backslash \{0\}$ means "all non-zero elements of F". Since $\langle f \backslash \{0\}, \cdot \rangle$ is an abelian group, for every $a \in F$, we use $a^{-1} \in F$ to denote the multiplicative inverse of a.

1.2 The Ring of Polynomials

We can express a polynomial in x (called an indeterminate) with coefficients in a ring R as a finite sum

$$\sum_{i=0}^{n} a_i x^i = a_0 + a_1 x + \cdots + a_n x^n,$$

where $a_i \in R$ and n is the degree of the polynomial. We say that two polynomials are equal if and only if the corresponding coefficients are equal (where any omitted powers of x can be taken to have a coefficient of zero). We define the addition and multiplication operations on polynomials as follows: If

$$f = \sum_{i=0}^{n} a_i x^i$$

and

$$g = \sum_{i=0}^{n} b_i x^i,$$

then we define

$$f + g = \sum_{i=0}^{n} (a_i + b_i) x^i$$

$$fg = \sum_{i=0}^{n} c_i x^i$$

where

$$c_i = \sum_{j+k=i}^{n} a_j b_k.$$

Under these operations, the set of all polynomials with coefficients in R and an indeterminate x forms a ring, which we denote by $R[x]$.

Lemma 1.1. *If D is an integral domain and x is an indeterminate, then $D[x]$ is an integral domain.*

Proof. Let

$$f = a_0 + a_1 x + \cdots + a_n x^n$$

and

$$g = b_0 + b_1 x + \cdots + b_m x^m$$

where $a_n \neq 0$ and $b_m \neq 0$ and all the coefficients are in D. The coefficient of t^{m+n} in fg is $a_n b_m$, which is non-zero since D is an integral domain. Therefore if f, g are non-zero, then fg is also non zero. Thus, $D[x]$ is an integral domain. □

In particular, if F is a field, then $F[x]$ is an integral domain.

Remark 1.2. *$F[x]$ is not a field, as x is does not have a multiplicative inverse. That is, there is no polynomial $f(x) \in F[x]$ such that $xf(x) = 1$.*

1.3 Factorization of Polynomials

Not all polynomials can be factored over a given integral domain or field, so let us first define what what it means for a polynomial to be reducible.

Definition 1.11 (Reducible Polynomial)**.** *A non-constant polynomial $f(x)$ is said to be reducible over a ring R if it can be expressed as the product of two or more non-constant polynomials of lesser degree in $R[x]$. That is,*

$$f(x) = g(x)h(x) \quad f(x), g(x), h(x) \in R[x].$$

If no such factorization is possible, then $f(x)$ is said to be irreducible.

All polynomials of degree 0 or 1 are irreducible, because they cannot be expressed as a product of polynomials of lesser degree.

Definition 1.12 (Roots of a function)**.** *Given a function $f(x)$, a root of $f(x)$ is any value r that gives $f(x) = 0$ when $x = r$.*

Corollary 1.1 (Factor theorem)**.** *Let $f(x)$ be a polynomial in $\mathbb{Q}[x]$. $f(x)$ has a root $a \in \mathbb{Q}$ if and only if $x - a$ is a factor of $f(x)$ in $\mathbb{Q}[x]$.*

Proof. Suppose that $f(a) = 0$ for some $a \in \mathbb{Q}$. By the division algorithm,

$$f(x) = (x - a)q(x) + r(x)$$

for some $q(x), r(x) \in \mathbb{Q}[x]$ with either $r(x) = 0$ or $r(x)$ having degree less than 1. In either case we have $r(x) = c$ for some $c \in F$. Thus,

$$f(x) = (x - a)q(x) + c.$$

Evaluating at $x = a$,

$$\begin{aligned} f(x) &= (a - a)q(a) + c \\ 0 &= 0q(a) + c \\ 0 &= c \end{aligned}$$

Then $f(x) = (x - a)q(x)$ and $x - a$ is a factor of $f(x)$.
Conversely, if $x - a$ is a factor of $f(x) \in F[x]$ where $a \in \mathbb{Q}$, it is obvious that evaluating at $x = a$ will give $f(a) = 0$ and therefore a is a root of $f(x)$. □

We can now establish some criterion that will help determine whether a specific polynomial is reducible over $\mathbb{Q}$. The Rational Root Test or Rational Root Theorem gives candidates for the roots of a polynomial (pg 214–215, [5]).

Theorem 1.1 (Rational Root Test)**.** *Let $f(x)$ be a polynomial*

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

with integer coefficients. Let a_n and a_0 be nonzero. Then any root of $f(x)$ in the rational numbers $\mathbb{Q}$ can be expressed as $x = \frac{p}{q}$ for $p, q \in \mathbb{Z}$, $q \neq 0$, where p and q satisfy the following two properties:

i. p divides the constant term a_0

ii. q divides the leading coefficient a_n.

We now state Gauss' Lemma (Proposition 2.4, pg. 19, [6]).

Theorem 1.2. *Let $f(x)$ be a polynomial in $\mathbb{Z}[x]$ be irreducible over $\mathbb{Z}$. Then $f(x)$ is also irreducible over $\mathbb{Q}$.*

Proof. By way of contradiction, we assume that $f(x) \in \mathbb{Z}[x]$ is irreducible over $\mathbb{Z}$, but reducible over $\mathbb{Q}$. That is, $f(x) = g(x)h(x)$ where $g(x), h(x)$ are polynomials in $\mathbb{Q}[x]$ of smaller degree. By multiplying by the product of denominators of the coefficients of g and h, we can rewrite this equation as

$$nf = g'h'$$

where $n \in \mathbb{Z}$ and g', h' are polynomials in $\mathbb{Z}[x]$. We will now cancel out the prime factors of n one by one, while staying within $\mathbb{Z}[x]$.

Suppose that p is a prime factor of n. If we define

$$g' = g_0 + g_1 x + \cdots + g_r x^r$$
$$h' = h_0 + h_1 x + \cdots + h_s x^s$$

then we claim that either p divides all of the coefficients g_i or p divides all the coefficients h_j. Otherwise, there must exist smallest values i and j such that $p \nmid g_i$ and $p \nmid h_j$. However, p does divide the coefficient of x^{i+j} in the polynomial $g'h'$, which is

$$h_0 g_{i+j} + h_1 g_{i+j-1} + \cdots + h_j g_i + \cdots + h_{i+j} g_0.$$

By the choice of i and j, the prime p divides every term of this expression, perhaps with the exception of $h_j g_i$. However, we know that p divides the whole expression, so $p|h_j g_i$. But $p \nmid h_j$ and $p \nmid g_i$, which gives a contradiction. This establishes our claim.

Without loss of generality, we may now assume that p divides every coefficient g_i. Then $g' = pg''$ where g'' is a polynomial in $\mathbb{Z}[x]$ of the same degree as g' or g. Let $n = pn_1$. Then

$$pn_1 f = pg''h'$$

so that

$$n_1 f = g''h'.$$

Repeating this process, we can remove all of the prime factors of n and we arrive at an equation

$$f = \bar{g}\bar{h}$$

where $\bar{g}$ and $\bar{h}$ are polynomials in $\mathbb{Z}[x]$ that are rational multiples of the original g and h. But, this contradicts the irreducibility of $f(x)$ over $\mathbb{Z}$.

Hence our assumption that $f(x)$ is reducible over $\mathbb{Q}$ is false, and $f(x)$ must be irreducible over $\mathbb{Q}$. □

Another important test for irreducibility is Eisenstein's Criterion (Theorem 2.5, pg. 20, [6])

Theorem 1.3 (Eisenstein's Criterion)**.** *Let $f(x)$ be a polynomial*

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

with integer coefficients. Suppose that there exists a prime $p \in \mathbb{Z}$ such that

i. p divides each a_i for $i \neq n$,

ii. p does not divide a_n, and

iii. p^2 does not divide a_0.

If such a p exists, then $f(x)$ is irreducible over $\mathbb{Q}$.

Proof. Suppose that such a polynomial $f(x)$ exists, which satisfies the above conditions. By way of contradiction, assume that f is reducible over $\mathbb{Q}$. Then

$$f(x) = g(x)h(x)$$

for some non-constant polynomials $g(x), h(x) \in \mathbb{Q}[x]$. The reduction map mod p given by

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

is a homomorphism and thus,

$$\phi_p\left(f(x)\right) = \phi_p\left(g(x)\right)\phi_p\left(h(x)\right).$$

But

$$\begin{aligned}\phi_p\left(f(x)\right) &= \phi_p\left(a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0\right)\\ &= \alpha x^n\end{aligned}$$

where $a_n \equiv \alpha \mod p$ because $p \mid a_i$ for $i \neq n$. So

$$\phi_p\left(g(x)\right)\phi_p\left(h(x)\right) = \alpha x^n$$

and

$$\phi_p\left(g(x)\right) = \beta x^k, \quad \phi_p\left(h(x)\right) = \gamma x^{n-k}$$

for some $0 < k < n$ and β, γ such that $\beta\gamma \equiv \alpha \mod p$. Since $\mathbb{Z}_p[x]$ is a unique factorization domain, then p must divide each of the non-leading

coefficients of $g(x)$ and $h(x)$. Looking at the constant terms b_0 and c_0 of $g(x)$ and $h(x)$ respectively,

$$b_0 = pr$$

$$c_0 = ps$$

for some $r, x \in \mathbb{Z}$. Then the constant term of $f(x)$ must be

$$\begin{aligned} a_0 &= b_0 c_0 \\ &= (pr)(ps) \\ &= p^2(rs), \end{aligned}$$

which is a contradiction because $p^2 \nmid a_0$. □

A brief definition and Theorem are also provided in this section that will serve as tools when looking at polynomials later in this thesis.

Definition 1.13 (Discriminant of a polynomial)**.** *Let $f(x)$ be a polynomial with roots $r_1, \ldots, r_n \in \mathbb{C}$ (not necessarily distinct). The discriminant of $f(x)$ is defined by*

$$\prod_{1 \le i < j \le n} (r_i - r_j)^2.$$

In other words, the discriminant of a polynomial is equal to the product of the squares of the differences of the polynomial's roots. Frequently we denote a polynomial's discriminant by D.

Theorem 1.4 (Rolle)**.** *(pg. 290 [7]) Let $f(x)$ be a real-valued function that is continuous on $[a, b]$ and differentiable on (a, b). Then if $f(a) = f(b)$ there must exist some $c \in (a, b)$ such that*

$$f'(c) = 0.$$

1.4 Algebraic Numbers

We will be using algebraic numbers to define extensions of common fields such as $\mathbb{Q}$. We begin with the idea of an extension field.

Definition 1.14 (Extension field)**.** *A field E is an extension field of a field F if F is a subfield of E.*

To understand how polynomials define extension fields, we begin with a theorem of Kronecker (Theorem 29.3, pg. 266, [8]).

Theorem 1.5 (Kronecker)**.** *Let F be a field and let $f(x) \in F[x]$ be a non-constant polynomial. Then there exists an extension field E of F and some $\alpha \in E$ such that $f(\alpha) = 0$.*

We can now define an algebraic number and begin to construct algebraic number fields.

Definition 1.15 (Algebraic number)**.** *Let E be an extension field of F. An element $\alpha \in E$ is algebraic over F if $f(\alpha) = 0$ for some nonzero $f(x) \in F[x]$.*

If α is not algebraic over F, then α is transcendental over F. Note that since any field F is an extension field of itself, any element $\alpha \in F$ is algebraic over F.

Definition 1.16 (Minimal polynomial)**.** *Let E be an extension field of F and let $\alpha \in E$ be algebraic over F. The minimal polynomial is the unique monic polynomial $f(x) \in F[x]$ of smallest degree such that $f(\alpha) = 0$.*

In this last definition, the term "monic" means that the leading coefficient is equal to 1.

Definition 1.17 (Algebraic number field)**.** *An algebraic number field is a subfield of* $\mathbb{C}$ *of the form* $\mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_n)$ *where* $\alpha_1, \alpha_2, \ldots, \alpha_n$ *are algebraic numbers.*

In other words, an algebraic number field is an extension of the field of rational numbers $\mathbb{Q}$ by adjoining finitely many algebraic numbers $\alpha_1, \alpha_2, \ldots, \alpha_n$. This is the smallest field that contains $\mathbb{Q}$ and $\alpha_1, \alpha_2, \ldots, \alpha_n$. If we construct an algebraic number field from a single algebraic number, $\mathbb{Q}(\alpha)$, we call this a simple extension. A useful Theorem regarding simple extensions is taken from (Theorem 51.15, pg. 441, [8])

Theorem 1.6 (Primitive Element Theorem)**.** *If* $K = \mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_n)$ *is an algebraic number field, then there exists an algebraic number* α *such that* $K = \mathbb{Q}(\alpha)$*.*

Example 1.1. *Let* α *be a root of the polynomial*

$$x^2 - 2$$

and let β *be a root of the polynomial*

$$x^2 - 3.$$

We create an algebraic number field $K = \mathbb{Q}(\alpha, \beta)$ *and wish to show that there exists a primitive element* $\gamma = \alpha + \beta$ *such that* $K = \mathbb{Q}(\gamma)$*. Obviously* $\mathbb{Q}(\gamma) \subseteq \mathbb{Q}(\alpha, \beta)$*. It remains to show that* $\mathbb{Q}(\alpha, \beta) \subseteq \mathbb{Q}(\gamma)$*. Looking at powers of* γ*,*

$$\gamma^2 = (\alpha + \beta)(\alpha + \beta) = \alpha^2 + 2\alpha\beta + \beta^2 = 2\alpha\beta + 5$$
$$\gamma^3 = (2\alpha\beta + 5)(\alpha + \beta) = 2\alpha^2\beta + 2\alpha\beta^2 + 5\alpha + 5\beta = 11\alpha + 9\beta$$

we can see that

$$\alpha = \frac{\gamma^3 - 9\gamma}{2} \in \mathbb{Q}(\gamma)$$

and

$$\beta = \frac{-(\gamma^3 - 11\gamma)}{2} \in \mathbb{Q}(\gamma).$$

Therefore we have $\mathbb{Q}(\alpha, \beta) \subseteq \mathbb{Q}(\gamma)$. *Thus,*

$$\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\gamma).$$

We can also think of an algebraic number field as a vector space to define important properties such as degree.

Definition 1.18 (Degree of an algebraic number field)**.** *Let* $K = \mathbb{Q}(\alpha)$ *be an algebraic number field. Then* K *is an* n*-dimensional vector space over* $\mathbb{Q}$ *with basis* $\{1, \alpha, \ldots, \alpha^{n-1}\}$ *and the degree of* K *over* $\mathbb{Q}$ *is* n*. We denote the degree of* K *over* $\mathbb{Q}$ *as* $[K : \mathbb{Q}] = n$*.*

Any extension field with a finite degree n is called a finite extension field. It should also be noted that all finite extension fields of a field F are algebraic extensions of F.

Example 1.2. *Let* $\theta = \sqrt{\sqrt{7} - 2}$ *and* $K = \mathbb{Q}(\theta)$ *. We wish to find the degree* $[K : \mathbb{Q}]$*. We start by finding the minimum polynomial of* θ *over* $\mathbb{Q}$*. Squaring* θ*,*

$$\theta^2 = \sqrt{7} - 2$$

we obtain

$$\theta^2 + 2 = \sqrt{7}.$$

Squaring both sides,

$$\theta^4 + 4\theta^2 + 4 = 7.$$

Therefore θ is a root of the polynomial

$$f(x) = x^4 + 4x^2 - 3,$$

which is monic. This shows that θ is an algebraic number and that $[K : \mathbb{Q}] \leq 4$ since $f(x)$ over $\mathbb{Q}$ has degree 4. It remains to determine whether $f(x)$ is irreducible. Assuming that $f(x)$ is reducible, then $f(x-1)$ must also be reducible. However,

$$f(x-1) = x^4 - 4x^3 + 10x^2 - 12x + 2$$

meets Eisenstein's criterion for $p = 2$ and is therefore irreducible. By Gauss' Lemma, since $f(x)$ is irreducible over $\mathbb{Z}$, then $f(x)$ is also be irreducible over $\mathbb{Q}$. Thus, $f(x)$ is monic and irreducible and $f(x)$ is the minimum polynomial for θ. Since $f(x)$ has degree 4, then

$$[K : \mathbb{Q}] = 4.$$

Algebraic number fields are typically classified by their degree. If the degree of K over $\mathbb{Q}$ is $n = 2$, we say that K is a quadratic field. Similarly, K is a cubic subfield for $n = 3$, a quartic field for $n = 4$, and so on. We will make reference to sextic fields ($n = 6$) throughout later chapters.

We can now better understand what the elements of an algebraic number field look like. For example, the field $\mathbb{Q}(\alpha)$ with $[\mathbb{Q}(\alpha) : \mathbb{Q}] = n$ contains all elements of the form

$$a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{n-1}\alpha^{n-1}$$

with $a_0, \ldots, a_{n-1} \in \mathbb{Q}$. The elements of the field $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ can then be constructed by looking at a series of individual extensions:

$$\mathbb{Q}(\alpha_1, \ldots, \alpha_n) = \mathbb{Q}(\alpha_1, \ldots, \alpha_{n-1})(\alpha_n) = \ldots = \mathbb{Q}(\alpha_1) \cdots (\alpha_n).$$

Another useful principle regarding the degree of an extension is sometimes referred to as The Tower Law (Theorem 31.4, pg. 283 [8]).

Theorem 1.7. *If K, E, and F are fields where E is a finite extension of F and K is a finite extension of E, then*

$$[K : F] = [K : E][E : F].$$

Having explained much of the background theory in algebra, we can now explain the concepts of Galois theory and the types of problems investigated by mathematicians studying in Galois theory.

Chapter 2

Galois Theory

2.1 Introduction to Galois Theory

When analyzing a polynomial, we are often concerned with finding its roots, or zeros. In the case of the general quadratic polynomial, $f(x) = ax^2 + bx + c$ with $a \neq 0$, we are familiar with the formula for the roots,

$$\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

We commonly refer to this equation as the quadratic formula. For polynomials of higher degree, we wish to find similar expressions of the roots in terms of the coefficients of the polynomial. If it is possible to express the roots in terms of the coefficients of the polynomial using only algebraic operations (addition, subtraction, multiplication, and division) and radicals, we say that the polynomial is solvable. In fact, the roots of polynomials of degree 3 and 4 are also able to be expressed in terms of radicals. However, mathematicians had tried for years to find the radical formula for polynomials of degree 5 until Niels Henrik Abel proved that the general quintic polynomial was not solvable (see Historical Note, pg. 56, [8]).

Through Galois theory, we are able to determine whether a given polynomial is solvable by radicals. Each polynomial has a Galois group that is defined to be solvable or not solvable, and this corresponds to whether the roots of that polynomial can be expressed in terms of its coefficients using algebraic operations and radicals.

In the case of quadratic polynomials, every polynomial is solvable. This is because there is only one possible Galois group of a quadratic polynomial,

which is a solvable group. We will see examples of various Galois groups in Chapter 3. Before being able to calculate the Galois group of a given polynomial, we will need a basic understanding of the underlying theory.

2.2 The Idea Behind Galois Theory

Throughout this chapter, several references will be made to a particular type of isomorphism, called an automorphism.

Definition 2.1 (Automorphism)**.** *An isomorphism of a field onto itself is an automorphism of the field.*

Definition 2.2 (K-Automorphism)**.** *Let K be a subfield of L. An automorphism ϕ of L is a K-automorphism of L if*

$$\phi(k) = k \quad \forall k \in K.$$

The main importance of these K-automorphisms is their group structure.

Theorem 2.1. *If K is a field extension of L, then the set of all K-automorphisms of L forms a group under composition of maps.*

Proof. Let ϕ and ψ be K-automorphisms of L. Then $\phi\psi$ is also a K automorphism, as $\phi\psi(k) = \phi(k) = k$. The identity map on L is obviously a K-automorphism and finally, ϕ^{-1} is also a K-automorphism, as $k = \phi^{-1}\phi(k) = \phi^{-1}(k)$. Composition of maps is associative, and so the set of all K-automorphisms of L is a group. □

It should also be noted that the identity map from L onto itself is automatically a K-automorphism and therefore the set of all K-automorphisms of L is non-empty.

Definition 2.3 ($Aut_{\mathbb{Q}}(K)$)**.** *Let K be an algebraic number field. We define $Aut_{\mathbb{Q}}(K)$ to be the group of automorphisms of K that fix $\mathbb{Q}$ under composition of maps.*

We will now introduce two more important properties of certain algebraic number fields: the idea of normal and separable fields.

Definition 2.4 (Separable)**.** *An algebraic number field K is separable if for each algebraic number $\alpha \in K$, the minimal polynomial of α over K has no repeated roots.*

Definition 2.5 (Splits)**.** *Let K be a field and let $f(x) \in K[x]$. If $f(x)$ can be expressed as a product of linear factors*

$$f(x) = a(x - r_1) \cdots (x - r_n)$$

where $a, r_1, \ldots, r_n \in K$, then we say that $f(x)$ splits over K.

Definition 2.6 (Normal)**.** *An algebraic number field K is normal if for each algebraic number $\alpha \in K$, the minimal polynomial of α splits over K.*

We can now define the Galois group of an algebraic number field.

Definition 2.7 (Galois group)**.** *An algebraic number field K is Galois if it is both separable and normal. In this case, $Aut_{\mathbb{Q}}(K)$ is called the Galois group of K and is denoted as $Gal(K : \mathbb{Q})$.*

Using these same concepts, we can now define the Galois group of a polynomial.

2.3 The Galois Group of a Polynomial

Now that we understand the concept of a polynomial splitting over a given field, we can define the splitting field of a specific polynomial.

Definition 2.8 (Splitting field)**.** *The field E is the splitting field of a polynomial $f(x)$ over F if $F \subseteq E$ and*

i. $f(x)$ splits over E and

ii. if $F \subseteq E' \subseteq E$ and $f(x)$ splits over E' then $E' = E$.

Remark 2.1. *The second condition of this last definition is equivalent to*

$$ii^*. \quad E = F(\alpha_1, \ldots, \alpha_n),$$

where $\alpha_1, \ldots, \alpha_n$ are the roots of $f(x)$ in E.

Just as we defined a separable algebraic number field in the previous section, we can also say that a polynomial is separable.

Definition 2.9 (Separable polynomial)**.** *A polynomial $f(x)$ is called separable if it has no repeated roots in a splitting field.*

We can also obtain a normal algebraic number field for a specific polynomial through the following theorem.

Theorem 2.2. *An field extension E of F is normal and finite if and only if E is a splitting field for some polynomial over F.*

From the definitions and theorems given, we can now see that, given a separable polynomial $f(x)$, we can construct a splitting field E which is normal and finite. Since $f(x)$ is a separable polynomial, E contains all the distinct roots of $f(x)$ and E is separable. If $f(x) \in \mathbb{Q}[x]$, then E is an algebraic number field. We can now give a formal definition of the Galois group of a polynomial.

Definition 2.10 (Galois group of a polynomial)**.** *If $f(x)$ is a separable polynomial over $\mathbb{Q}$, then the Galois group of $f(x)$ over $\mathbb{Q}$ is the Galois group of the splitting field of $f(x)$ over $\mathbb{Q}$. We denote this group as $Gal\,(f(x))$.*

Every polynomial over $\mathbb{Q}$ has a unique Galois group. This is because we can construct the splitting field of any polynomial over $\mathbb{Q}$ by considering only its irreducible factors. Once we remove any multiple factors, we are left with a separable polynomial with the same splitting field as the original polynomial. This leaves us with the splitting field of a separable polynomial over $\mathbb{Q}$, which is Galois.

Throughout the remainder of this thesis, Galois groups of polynomials will frequently be referred to as "being isomorphic to" a common group structure. These groups have notations such as A_4, S_5, D_4, etc. For a list of common group names and structures, see Appendix A.

2.4 Determining the Galois Group of a Given Polynomial

Knowing the theory behind Galois groups is necessary, but not always sufficient to be able to formally determine the Galois group of a given polynomial. As mentioned, the Galois group of a separable polynomial $f(x)$ over $\mathbb{Q}$ with splitting field K is the group of all $\mathbb{Q}$-automorphisms of K. In practice, we can describe the Galois group $Gal\,(f(x))$ another way.

Firstly, it is useful to define an algebraic equation.

Definition 2.11 (Algebraic equation)**.** *An algebraic equation is an equation of the form $P = 0$ where P is a (possibly multivariate) polynomial with rational coefficients.*

We can now consider a separable polynomial $f(x) \in \mathbb{Q}[x]$ with roots $x_1, \ldots, x_n$. We are interested in permutations of these roots such that any algebraic equation satisfied by the roots will still be satisfied once the roots have been permuted. Of the possible $n!$ permutations, many will be eliminated by this required property. The remaining permutations form a group and this group is $Gal\,(f(x))$.

Remark 2.2. *Since $Gal\,(f(x))$ is a subgroup of the permutations of the n distinct roots of a separable polynomial $f(x)$, then*

$$|Gal\,(f(x))\,| \,\Big|\, |S_n|,$$

where S_n is the group of all permutations of n distinct elements.

With this alternate description of the Galois group of a polynomial, we can now proceed to determine the Galois group of a given polynomial. We will denote a permutation of the roots in cycle notation in order to help determine the group structure. An example of cycle notation for the permutation $\sigma(1) = 2, \sigma(2) = 1, \sigma(3) = 4, \sigma(4) = 3$ would be

$$(1\ 2)(3\ 4).$$

In this example we can clearly see two cycles of length 2. We use this notation in the following example.

Example 2.1. *Consider the polynomial*

$$f(x) = x^4 - x^2 - 2 = (x^2 + 1)(x^2 - 2).$$

We wish to determine $Gal\,(f(x))$, the Galois group of $f(x)$ over $\mathbb{Q}$. The four

roots of $f(x)$ *are*

$$x_1 = i$$
$$x_2 = -i$$
$$x_3 = \sqrt{2}$$
$$x_4 = -\sqrt{2}$$

There are a total of $4! = 24$ *ways of permuting these roots, but we must eliminate any permutations that do not preserve algebraic equations in terms of these four roots. For example, one algebraic equation would be*

$$x_1 + x_2 = 0.$$

This would allow us to eliminate the permutation

$$(x_1\ x_2\ x_3\ x_4)$$

because the same equation after permutation would become

$$x_2 + x_3 = -i + \sqrt{2}$$
$$\neq 0.$$

Similarly, the algebraic equation $(x_1 + x_2)^2 + (x_3 + x_4)^2$ *would not permit the permutation* $(1\ 3)(2)(4)$*. If we repeat this process, there are only four permutations which satisfy both equations. These four permutations are:*

i. $(x_1)(x_2)(x_3)(x_4)$ *(the trivial permutation)*

ii. $(x_1\ x_2)(x_3)(x_4)$

iii. $(x_1)(x_2)(x_3\ x_4)$

iv. $(x_1\ x_2)(x_3\ x_4)$

If we then denote the trivial permutation as 1 and define the permutations $\sigma = (x_1\ x_2)(x_3)(x_4)$, $\tau = (x_1)(x_2)(x_3\ x_4)$, *we can see that the fourth permutation is simply* $\sigma\tau$. *From this we can see a clear group structure. We can then say that*

$$\begin{aligned} Gal\,(f(x)) &= \{1, \sigma, \tau, \sigma\tau\} \\ &\cong \mathbb{Z}_2 \times \mathbb{Z}_2 \end{aligned}$$

With the help of this trivial example, we can better understand the potential group structures of the Galois groups of polynomials for varying degree n. We will investigate these groups in the following chapter.

Chapter 3

Polynomials and their Known Galois Groups

For a polynomial of degree n, the possible Galois groups of that polynomial are the symmetrical group of order n, S_n and all transitive subgroups of S_n. By determining this Galois group, we are then able to determine whether the polynomial is solvable algebraically. We will begin by looking at a few known examples, particularly monic trinomials of degree n. A monic trinomial is a polynomial with only three terms and a coefficient of the highest degree term equal to 1. Finding criteria for the coefficients of trinomial is easier than working with the general form of a polynomial, but is still non- trivial.

Since there are no non-trivial subgroups of S_2, we will begin by looking polynomials of degree 3.

3.1 Cubic Polynomials

The first example of nontrivial Galois groups occurs for polynomials of degree 3. A polynomial of degree 3 is referred to as a cubic polynomial and has the form

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

where $a \neq 0$. There are two possible Galois groups for cubics, S_3 and A_3, the alternating group on three elements, as shown in Cohen [9]. It should be noted that A_3 is isomorphic to the C_3, the cyclic group of order three. Since

S_3 is the most common case, we want to determine criteria for obtaining C_3 as a Galois group.

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

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

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

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

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

The main distinction of cubics with a Galois group of C_3 is that the polynomial discriminant is equal to a square in $\mathbb{Q}$. In [10], Seidelmann uses this fact to give a form for the coefficients of a monic cubic trinomial with a Galois group of C_3. For $p, q \in \mathbb{Q}$, the equation

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

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

3.2 Quartic Polynomials

When looking at polynomials of degree 4, there are a total of five possible Galois groups, which are listed in [9]. Again, S_4 is the most common case, followed by A_4. In more rare cases, quartic polynomials may have a Galois

group of D_4, the dihedral group of order 8; V_4, the Klein-4 group; or C_4, the cyclic group of order 4.

In [10], Seidelmann once again gives forms for a quartic polynomial with each of the four less common Galois groups. Perhaps the most interesting component of his results is the manner in which he categorizes each group. His method for finding these forms starts with knowing how the roots of the polynomial appear in each case. This is particularly significant because by looking at the forms of these roots it is possible to get an idea of the actual permutations between the roots. Knowing the forms of the four roots x_0, x_1, x_2, x_3, we can expand a product of linear factors

$$(x - x_0)(x - x_1)(x - x_2)(x - x_3)$$

to understand what the polynomial itself looks like. From this general form of the polynomial, we can then impose further conditions if we wish to look specifically at trinomials.

3.2.1 The Klein-4 Group V_4

In the case of quartic polynomials with a Galois group of V_4, Seidelmann recognizes that the general form of the roots is

$$\begin{aligned} x_0 &= \sqrt{e} + \sqrt{f} + g\sqrt{ef} \\ x_1 &= \sqrt{e} - \sqrt{f} - g\sqrt{ef} \\ x_2 &= -\sqrt{e} + \sqrt{f} + -\sqrt{ef} \\ x_3 &= -\sqrt{e} - \sqrt{f} + g\sqrt{ef} \end{aligned}$$

for some $e, f, g \in \mathbb{Q}$. Through expansion of linear factors, the quartic polynomial must be of the form

$$f(x) = x^4 - 2x^3(e + f + efg^3) - 8efgx + (e - f - efg^3)^3 - 4eg^2f^2.$$

3.2.2 The Dihedral Group D_4

In the case of quartics with a Galois group of D_4, Seidelmann gives the roots in the form

$$\begin{aligned} x_0 &= e\sqrt{f} + \sqrt{g + \sqrt{f}} \\ x_1 &= e\sqrt{f} - \sqrt{g + \sqrt{f}} \\ x_2 &= -e\sqrt{f} + \sqrt{g - \sqrt{f}} \\ x_3 &= -e\sqrt{f} - \sqrt{g - \sqrt{f}} \end{aligned}$$

for some $e, f, g \in \mathbb{Q}$. After expanding the product of linear factors, we find that the quartic polynomial must be of the form

$$f(x) = x^4 - 2(e^2 f + g)x^2 - 4efx + \left[(e^2 f - g)^2 - f\right].$$

3.2.3 The Cyclic Group C_4

Seidelmann goes on to explicitly give the form of the roots of quartics with a Galois group of C_6, as

$$\begin{aligned} x_0 &= f\sqrt{1+e^2} + \sqrt{g\left[1 + e^2 + \sqrt{1+e^2}\right]} \\ x_1 &= f\sqrt{1+e^2} - \sqrt{g\left[1 + e^2 + \sqrt{1+e^2}\right]} \\ x_2 &= -f\sqrt{1+e^2} + \sqrt{g\left[1 + e^2 - \sqrt{1+e^2}\right]} \\ x_3 &= -f\sqrt{1+e^2} - \sqrt{g\left[1 + e^2 - \sqrt{1+e^2}\right]} \end{aligned}$$

for some $e, f, g \in \mathbb{Q}$. In the case of this family of quadratics, the polynomial must be of the form

$$f(x) = x^4 - 2(1+e^2)(f^2+g)x^2 - 4fg(1+e^2)x + (1+e^2)\left[(1+e^2)(f^2-g)^2 - g^2\right].$$

It becomes more evident by looking at the more complicated restrictions of the polynomial that the cyclic group of order 4 is the most rarely occurring Galois group of quartics.

3.2.4 The Alternating Group A_4 and Symmetric Group S_4

Finally, Seidelmann gives an expression for quartics with a Galois group of A_4 as

$$f(x) = x^4\left[e^3 - (f^2+3g^2)(3e+2f)\right] - 6x^2e - 8x \\ - 3\frac{e^2 - 4f^2 - 12g^2}{e^2 - (f^2+3g^2)(3e+2f)}$$

with $e, f, g \in \mathbb{Q}$. In the remaining cases where a quartic polynomial $f(x)$ does not have any of the above forms, then the Galois group of $f(x)$ is the symmetric group S_4.

3.3 Quintic Trinomials

In the case of polynomials of degree 5, there are five possible Galois groups that may occur, listed once again in [9]. These groups are the symmetric group S_5, A_5 the alternating group on 5 letters, the Frobenius group F_{20}, the dihedral group D_5, and the cyclic group C_5. Of these five possible groups, only three of the groups are solvable and therefore only their associated polynomials are solvable. These solvable groups are F_{20} and its subgroups D_5 and C_5. It is also known that the discriminant of a solvable quintic must be positive, as demonstrated by Dummit [11].

In [11], Dummit gives criteria for the solvability of a quintic in the form of the existence of a rational root of an associated resolvent sextic polynomial. This resolvent sextic is given in terms of the coefficients of the original

quintic polynomial. Though it may seem odd to determine the solvability of a quintic by means of solving a sextic, the existence of a rational root allows us to use many properties associated with integers. Dummit defines this resolvent sextic $f_{20}(x)$ using elementary symmetric polynomials. For a given quintic

$$f(x) = x^5 + px^3 + qx^2 + rx + s,$$

where the x^4 term has been eliminated after making a translation to the general quintic, he gives an expression for $f_{20}(x)$:

$$\begin{aligned}
f_{20}(x) = {} & x^6 + 8rx^5 + (2pq^2 - 6p^2r + 40r^2 - 50qs)x^4 \\
& + (-2q^4 + 21pq^2r - 40p^2r^2 + 160r^3 - 15p^2qs - 400qrs + 125ps^2)x^3 \\
& + (p^2q^4 - 6p^3q^2r - 8q^4r + 9p^4r^2 + 76pq^2r^2 - 136p^2r^3 \\
& + 400r^4 - 50pq^3s + 90p^2qrs - 1400qr^2s + 625q^2s^2 + 500prs^2)x^2 \\
& + (-2pq^6 + 19p^2q^4r - 51p^3q^2r^2 + 3q^4r^2 + 32p^4r^3 + 76pq^2r^3 \\
& - 256p^2r^4 + 512r^5 - 31p^3q^3s - 58q^5s + 117p^4qrs + 105pq^3rs \\
& + 260p^2qr^2s - 2400qr^3s - 108p^5s^2 - 325p^2q^2s^2 + 525p^3rs^2 \\
& + 2750q^2rs^2 - 500pr^2s^2 + 625pqs^3 - 3125s^4)x \\
& + (q^8 - 13pq^6r + p^5q^2r^2 + 65p^2q^4r^2 - 4p^6r^3 - 128p^3q^2r^3 + 17q^4r^3 \\
& + 48p^4r^4 - 16pq^2r^4 - 192p^2r^5 + 256r^6 - 4p^5q^3s - 12p^2q^5s \\
& + 18p^6qrs + 12p^3q^3rs - 124q^5rs + 196p^4qr^2s + 590pq^3r^2s \\
& - 160p^2qr^3s - 1600qr^4s - 27p^7s^2 - 150p^4q^2s^2 - 125pq^4s^2 \\
& - 99p^5rs^2 - 725p^2q^2rs^2 + 1200p^3r^2s^2 + 3250q^2r^2s^2 - 2000pr^3s^2 \\
& - 1250pqrs^3 + 3125p^2s^4 - 9375rs^4).
\end{aligned}$$

The main benefit of working with trinomials rather than with the general

form of polynomials becomes immediately apparent when we look at the particular case when $f(x) = x^5 + Ax + B$. In this case f_{20} is simply

$$f_{20}(x) = x^6 + 8Ax^5 + 40A^2x^4 + 160A^3x^3 + 400A^4x^2 + (512A^5 - 3125B^4)x + (256A^6 - 9375AB^4).$$

Many of the calculations involved in working with the Galois groups of polynomials are simplified when we restrict the polynomial to only three terms. Trinomials provide a great opportunity to explore concepts in Galois theory without being trivial and many of the results obtained from trinomials can be applied to polynomials with more terms.

In the case of quintic trinomials, Spearman and Williams [12] showed that there are an infinite number of essentially different, irreducible, solvable trinomials of the form $x^5 + ax + b$. They gave a parametrization for a and b in [13] to generate these trinomials, namely

$$a = \frac{5e^4(3 - 4\epsilon c)}{c^2 + 1} \text{ and } b = \frac{-4e^5(11\epsilon + 2c)}{c^2 + 1},$$

with $\epsilon = \pm 1$ and rational numbers c and e such that $c \geq 0$, and $e \neq 0$. Remarkably, there are only five essentially different, irreducible, solvable trinomials of the form $x^5 + ax^2 + b$. These five are also given in [12]:

x^5+5x^2+3, x^5+5x^2-15, x^5+25x^2+300, x^5+100x^2+1000, x^5+250x^2+625.

We do not consider possible trinomials here of the forms $x^5 + ax^3 + b$ or $x^5 + ax^4 + b$, as we can use fairly simple transforms on x to obtain one of the previous trinomials. For example, replacing $x = 1/X$ in $x^5 + ax^3 + b$ and clearing denominators, we obtain

$$1 + aX^2 + bX^5.$$

Then, making this polynomial monic by dividing by b, we have

$$\frac{1}{b} + \frac{a}{b}X^2 + X^5.$$

Now we must only define $B = 1/b$ and $A = a/b$ to obtain

$$B + AX^2 + X^5,$$

which is one of the forms already discussed. Since these transformations preserve solvability, we need only consider solvable trinomials of the form $x^5 + ax^m + b$ with $m = 1, 2$.

3.4 Sextic Trinomials

As expected, increasing the degree of a polynomial will increase its complexity. In the case of quartics or quintics, there were a total of five possible Galois groups. In the case of sextics, however, the number of possible Galois groups jumps up to sixteen. We can once again find a list of these groups in Cohen [9] and we expect S_6 to be the most frequently occuring group. This fact can be easily demonstrated through software such as MAPLE$^{\text{TM}}$by calculating the Galois group for randomly chosen sextic polynomials. However, the frequency of the subgroups of S_6 as a Galois group is not known.

Using the experience of working with quintics, it is much more preferable to work with sextic trinomials rather than general sextics. Again, we can reduce the possible unique forms of these trinomials to only $x^6 + ax + b$, $x^6 + ax^2 + b$, and $x^6 + ax^3 + b$. However, it should be noted that the last of these three forms can be simplified to a quadratic in x^3.

Very little work has been done regarding the categorization of sextic trinomials with a given Galois group when compared to polynomials of lesser

degree. Because of the complexity of sextic polynomials and the number of possible Galois groups, it is a wise plan to analyze families of sextic polynomials having a common trait. The sixteen possible subgroups of S_6 that can occur as Galois groups are well known and luckily some subsets of these groups share common group structures. These structural similarities make excellent candidates for families of polynomials, so long as we can develop restrictions on a and b such that trinomials belong to a particular family. More importantly, if we can express these restrictions in terms of common variables, we can parametrize the possible values of a and b that exist in this family. We investigate such parametric families in later chapters.

Chapter 4

Elliptic Curves, Genus 2 Curves, and Elliptic Chabauty

A curve is an equation of the form

$$f(x, y) = 0$$

where $f \in K[x, y]$ for some field K. To classify curves, we define the notion of its genus.

Definition 4.1 (Genus of a curve)**.** *Let $f(x, y) = 0$ be an algebraic curve with $f(x, y) \in \mathbb{Q}[x, y]$, and let P be the set of all singular points on $f(x, y) = 0$. We define the genus of $f(x, y) = 0$ with $f(x, y)$ of degree d to be*

$$g = \frac{(d-1)(d-2)}{2} - \sum_{P} \delta_P,$$

where δ_P is the delta-invariant at each singular point.

The genus of a curve and the delta-invariant of each singular point on a curve can easily be calculated using MAPLE$^{\text{TM}}$. Without software, this definition is helpful as it allows us to determine an upper bound on the genus of a curve, since the delta-invariant is always a non negative integer measuring the number of double points at each singular point. We do this by finding the singular points on a curve by solving the equation

$$\frac{\partial}{\partial x} f(x, y) = \frac{\partial}{\partial y} f(x, y) = 0$$

and then setting $\delta_P \geq 1$ for each singular point P.

Remark 4.1. *In the case of a nonsingular curve, then the curve $f(x, y) = 0$ has a genus of exactly*

$$g = \frac{(d-1)(d-2)}{2}$$

where d is the degree of $f(x, y)$.

The genus of a given curve gives us an idea of how complicated the curve is. For example, all conics (such as parabolas, ellipses, hyperbolas, etc.) have genus 0 whereas all elliptic curves have genus 1. This can easily shown in the case of non singular curves in standard form, where conics have degree $d = 1$ or $d = 2$ and elliptic curves have degree $d = 3$. Even stronger than this though, we can say that any curve of genus 0 is birationally equivalent to a conic and similarly all curves of genus 1 with at least one rational point are birationally equivalent to an elliptic curve. This birational equivalence means that there is a bidirectional rational transformation of variables between a given curve and a curve in a more desirable form. We will see such transformations in Chapters 5 and 6.

4.1 Elliptic Curves

As mentioned above, an elliptic curve is a special case of an algebraic curve $f(x, y) = 0$ having genus 1. We can write any elliptic curve in Weierstrass form

$$y^2 = x^3 + ax + b,$$

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

In this section, we discuss some of the important properties of elliptic curves, as several of these concepts are used directly in calculation or are

able to translate into similar ideas for more complex curves.

Typically when studying an elliptic curve, we are primarily concerned with rational points (x, y) that lie on the curve. The most important property of these points is that they form a group. To understand this group structure, we must first define an addition function which operates on two rational points.

Given two rational points P and Q on an elliptic curve E, we can use method known as "chord-and-tangent" addition to calculate $P+Q$. Firstly, we must define the negation of $P = (x, y)$ as

$$-P = -(x, y) = (x, -y).$$

We then form a line intersecting P and Q. If $P \neq Q$, this line is a chord and it intersects E at a third point, say R. If $P = Q$, we chose a line through P which is tangent to the curve E and this line once again intersects the E at a point R. We can then define "chord-and-tangent" addition as

$$P + Q = -R.$$

To properly form a group structure, we must also define an identity element. For such an element, we use a "point at infinity". For example, to add

$$P + (-P) = (x, y) + (x, -y),$$

we must form a line intersecting $P = (x, y)$ and $-P = (x, -y)$. This line of intersection is vertical and thus intersects E at a third point $\mathcal{O}$, the point at infinity. Therefore $P + (-P) = (O)$ and $\mathcal{O}$ is the additive identity.

Remark 4.2. *In the case of elliptic curves, we define a single point at infinity, notated here as $\mathcal{O}$. For other types of curves, such as the ones*

discussed in later chapters, we may need to define two points at infinity, which we can denote by ∞^+ *and* ∞^-.

Quite often we transform an equation for an algebraic curve into homogeneous form by making a substitution

$$x = \frac{X}{Z}, \quad y = \frac{Y}{Z}$$

with $Z \neq 0$. This also gives rise to a new projective coordinate system consisting of equivalence classes of triples $[X : Y : Z]$ with X, Y, Z not all zero. Two triples $[X_1 : Y_1 : Z_1], [X_2 : Y_2 : Z_2]$ are equivalent if there exists a constant $\lambda \in \mathbb{R}, \lambda \neq 0$ such that $[X_2 : Y_2 : Z_2] = [\lambda X_1 : \lambda Y_1 : \lambda Z_1]$. We can then transform a triple $[X : Y : Z]$ to Cartesian coordinates by scaling

$$[X : Y : Z] = \left(\frac{X}{Z}, \frac{Y}{Z}\right)$$

with $Z \neq 0$ and we define

$$[X : Y : 0]$$

to be a point at infinity.

Definition 4.2 (Group of rational points)**.** *Let* E *be an elliptic curve* $y^2 = x^3 + ax + b$ *with* $a, b \in \mathbb{Q}$. *We define* Γ *to be the group of rational points* (x, y) *on* E *under chord-and-tangent addition.*

It is easy to see that this addition operation in Γ is commutative and so the group defined above is abelian. The following theorem gives a much more detailed description of the group structure of Γ and it is detailed in [14].

Theorem 4.1 (Mordell-Weil)**.** *Let* E *be the elliptic curve defined by*

$$y^2 = x^3 + ax + b = f(x),$$

with $a, b, c \in \mathbb{Z}$ and the discriminant of $f(x)$ not equal to zero. Then the group of rational points (x, y) on E, Γ, is a finitely generated abelian group.

From this theorem, we know that Γ has the structure

$$\begin{aligned}\Gamma &\cong \mathbb{Z}_{p_1^{a_1}} \oplus \cdots \oplus \mathbb{Z}_{p_n^{a_n}} \oplus \mathbb{Z} \oplus \cdots \oplus \mathbb{Z} \\ &\cong T \oplus \mathbb{Z}^r\end{aligned}$$

where $p_1, \ldots, p_n$ are prime integers (not necessarily distinct) and $a_1, \ldots, a_n$ are positive integers. We define T to be the torsion subgroup of Γ and r to be the rank of Γ. The structure of the torsion subgroup describes points of finite order, whereas the rank tells us if there are points of infinite order and therefore if there are infinitely many rational points on a given elliptic curve.

Some of the calculations done in this thesis will require finding rational points on elliptic curves. Finding the group Γ can typically be done through software such as Magma [3], which will tell us the structure of the torsion subgroup as well as the rank of Γ in many cases. While the concept of Γ applies specifically to elliptic curves, we can construct a similar group structure for genus 2 curves.

4.2 Genus 2 Curves and Elliptic Chabauty

Most of the difficult calculations in this paper will be related to genus 2 curves and require a method known as elliptic Chabauty, which derives from [15]. In the study of genus 2 curves, we are typically concerned with the determination of the rational points on the curve. In the case of genus 0 curves, we have the ability to parametrize all the rational points in terms of rational functions of a single variable. With genus 1 curves, we have

the chord-and- tangent method of adding two rational points to obtain a third, creating a useful group structure of rational points. Unfortunately with genus 2 (and greater) curves, processes that can determine the rational points are much more difficult and are not guaranteed to work. Luckily we have one very useful theorem regarding the number of rational points on curves of genus greater than 1, given in [16].

Theorem 4.2 (Faltings)**.** *Let K be a number field and let C be a non-singular curve defined over K of genus $g \geq 2$. Then there are finitely many K-rational points on C.*

We frequently denote the set of $K-$rational points on a curve C as $C(K)$ and in the case where $K = \mathbb{Q}$, we say that $C(\mathbb{Q})$ is simply the set of rational points on C. $\#C(K)$ can also be used to denote the number of $K-$rational points on C.

While helpful, Faltings' Theorem does not help us to determine the rational points on a curve, as it does not give an actual numerical bound on the number of rational points. A more effective bound, given by Coleman in [17], can be found through the reduction of a curve C modulo p for a prime p. We reduce a curve C modulo p by reducing each coefficient in $f(x, y)$ modulo p, provided that p does not divide appear in the denominator of any coefficient. We then obtain a new curve

$$\bar{C} : \bar{f}(x, y),$$

the reduction of C modulo p, where $(\bar{f}) \in \mathbb{Z}_p[x, y]$. If the genus of this curve $\bar{C}$ over $\mathbb{Z}_p$ is also equal to 2, then we say that p is a prime of good reduction for C. Typically primes that are not of good reduction are referred to as "bad primes". (As a helpful property, for any curve of the form $y^2 = f(x)$,

where $f(x) \in \mathbb{Z}[x]$, a "bad prime" p has the property that $p \mid 2disc(f)$, where $disc(f)$ is the discriminant of f.) We can then use a theorem proven by Coleman in [17]:

Theorem 4.3. *Let C be a curve of genus 2 defined over $\mathbb{Q}$ and let $p \geq 5$ be a prime of good reduction for C. If C has rank at most 1 and $\bar{C}$ is the reduction of C modulo p, then*

$$\#C(\mathbb{Q}) \leq \#C(\mathbb{Z}_p) + 2.$$

Actually determining the finitely many rational points on a genus 2 curve typically involves studying the Jacobian of the curve. We will give a few definitions to better understand the Jacobian of a given curve. The following definitions are taken from [18] and will help to define the Jacobian and show its complexity, but will not be explicitly used in this thesis. For a complete understanding of the Jacobian, other literature such as [18] and [19] is recommended.

Definition 4.3 (Divisor of a curve)**.** *Let C be a curve defined over an algebraically closed field K. A divisor on C is an element of the group of points on C defined over K and is equal to a finite linear combination of points on C defined over K. For notation, we write*

$$\mathfrak{A} = \sum_P n_P P$$

where $\mathfrak{A}$ is a divisor and each P is a point on C defined over K. The coefficient n_P is referred to as the multiplicity of the point P and is equal to 0 for all except finitely many P.

Divisors are frequently denoted in a germanic Fraktur font $\mathfrak{A}, \mathfrak{B}$, etc. The set of divisors on a curve forms a free abelian group. We can also define the degree of a divisor.

Definition 4.4 (Degree of a divisor)**.** *The degree of a divisor*

$$\mathfrak{A} = \sum_P n_P P$$

is defined to be the sum of the multiplicities of the points within the divisor

$$\sum_P n_P.$$

Definition 4.5 (Principal divisors)**.** *Let f be a nonzero function on a curve C. A principal divisor, denoted $[f]$ is determined as follows. The multiplicity n_P of each point P in $[f]$ is the order to which f vanishes at P in terms of a local uniformizer.*

The set of principle divisors forms a subgroup of the group of divisors and two divisors differing by principal divisor are in the same divisor class.

We can now give a formal definition of the Jacobian so that we can briefly look at a couple of its properties.

Definition 4.6 (Jacobian)**.** *Given an algebraic curve, the Jacobian is defined to be the group of divisors of degree 0 modulo principle divisors.*

An important property of the Jacobian is that it is a finitely generated abelian group, much like the group of rational points on a elliptic curve as described earlier. The Jacobian is a very useful structure to look at for genus 2 curves, as it helps us in the determination of rational points through Chabauty methods, named after Claude Chabauty [15]. In fact, arithmetic of higher genus curves is actually arithmetic of their Jacobians and when we refer to the rank of a higher genus curve, we are referring to the rank its Jacobian. Unfortunately, Chabauty's method only works in cases where the Jacobian's rank is less than its dimension.

In the case of a genus 2 curve where the rank of the Jacobian is > 1, we have to use alternate methods. This is why we use elliptic Chabauty. Elliptic Chabauty methods work even if the rank is greater than 1 and theoretically applies to any rank of the Jacobian. Another major advantage of elliptic Chabauty methods is that we do not need to use the Jacobian in calculations.

Before using the method of elliptic Chabauty in the following two chapters, we will give a brief description of the method. We start with a hyperelliptic curve

$$y^2 = f(x)$$

of genus 2 where $f(x) \in \mathbb{Q}(x)$ is a monic polynomial of degree six with rational coefficients. We then factor $f(x)$ over a number field K to obtain

$$y^2 = F_1(x)F_2(x),$$

where $F_1(x)$ is a quadratic in $K[x]$ and $F_2(x)$ is a quartic in $K[x]$. Looking at these two polynomial factors, we find the greatest common divisor of $F_1(x)$ and $F_2(x)$ in $K[x]$ modulo squares. If this gcd is equal to 1 modulo squares, then both

$$F_1(x) = gU^2$$

and

$$F_2(x) = gV^2$$

for some polynomials U and V, since each of the factors must then be equal to a square. In these equations,

$$g = (-1)^{i_0}\epsilon_1^{i_1} \cdots \epsilon_n^{i_n}, i_0, \ldots, i_n = 0, 1,$$

where each ϵ is a fundamental unit of K. This gives a list of paired equations where possible rational solutions can be found. Each of these equations is a

simpler curve than the original problem and many of the possible values of g can be ruled out through local solvability of the associated two curves. This test for local solvability can be done through the Magma algebra system [3] for each of the curve's "bad primes". The *IsLocallySolvable* routine in Magma then looks for a possible solution through p-adic analysis.

After local solvability, there will likely be only very few remaining possible values for g that result in equations which are locally solvable. Of these resulting equations we then pick one for each value of g that gives the equation of an elliptic curve. If we are fortunate enough at this point to have the rank of the Mordell-Weil group of this elliptic curve less than the degree $[K : \mathbb{Q}]$, we can then apply elliptic Chabauty to the curve. Once again, Magma provides routines *PseudoMordellWeilGroup* and *Chabauty* for the calculations. If Magma is successful, we find only finitely many rational points on these elliptic curves.

These rational points from Magma give us finitely many candidates for x at which rational points on the original hyperelliptic curve $y^2 = f(x)$ may occur. We must then see if any of these candidates actually translate to rational points on the original curve. This completes our method.

Chapter 5

Sextic Trinomials $x^6 + Ax + B$ Defining Sextic Fields with a Cyclic Cubic Subfield

5.1 Main Theorem

Let $f(x)$ be a polynomial with rational coefficients which is irreducible over the rational numbers $\mathbb{Q}$. Let $Gal(f)$ denote the Galois group of $f(x)$. In this chapter, we characterize irreducible trinomials of the form $f(x) = x^6 + Ax + B$, having a Galois group isomorphic to either A_4 the alternating group on four letters, or $A_4 \times C_2$ where C_2 is the cyclic group of order 2. These polynomials define sextic fields (as discussed in chapter 1) having a cyclic cubic subfield and they occur in a parametric family, which enables an analysis of their Galois groups. While there are 16 possible Galois groups for irreducible sextic polynomials in $\mathbb{Q}[x]$, [9, pp. 323-325], basic group theory shows that only these three can occur if $f(x)$ defines a sextic field with a cyclic cubic subfield. These groups are C_6 the cyclic group of order 6, A_4 or $A_4 \times C_2$. In the notation of Butler and Mckay [2], these three groups are 6T1, 6T4, and 6T6 respectively. It has already been shown in [20] that up to scaling, there exists a single, unique sextic trinomial with Galois group isomorphic to C_6, which was given as

$$x^6 + 133x + 209.$$

For the trinomials discussed in this chapter, we show that only $A_4 \times C_2$ occurs. Our main theorem is the following, which appears in [4].

Theorem 5.1. *Let A and B denote nonzero rational numbers and set $f(x) = x^6 + Ax + B$*

i. $f(x)$ is irreducible over $\mathbb{Q}$ and $Gal(f) \simeq A_4 \times C_2 \Leftrightarrow$

$$A = 4u(u^2+3)(3u^2+1)(3u^2+25)^2v^5,$$
$$B = (u^2-5)(3u^2+1)(u^4+10u^2+5)(3u^2+25)^2v^6,$$

for rational numbers u and v with $u \neq 0, \pm 5$ and $v \neq 0$.

ii. If $f(x)$ is irreducible over $\mathbb{Q}$ then $Gal(f) \simeq A_4$ does not occur.

In the following section, we describe the parametric family of sextic trinomials $x^6 + Ax + B$ that define sextic fields with cyclic cubic subfields and assess the irreducibility of these trinomials. In section 3, we will prove our theorem characterizing the Galois groups of these polynomials.

5.2 A Parametric Family

We begin with the family of sextic trinomials which appears in [1].

Proposition 5.1. *Let A and B denote nonzero rational numbers such that $f(x) = x^6 + Ax + B$ is irreducible over $\mathbb{Q}$. 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*

$$A = 4u(u^2+3)(3u^2+1)(3u^2+25)^2v^5,$$
$$B = (u^2-5)(3u^2+1)(u^4+10u^2+5)(3u^2+25)^2v^6.$$

These restrictions on A and B have been carefully expressed in this way so as to parametrize A and B in terms of a single variable u with scaling factor.

In order to completely determine the Galois groups of the polynomials in this family, we will first need to investigate which of these polynomials, if any, are irreducible. Such a study frequently requires an analysis of an algebraic curve as for example in [21]. For our determination, we will require the study of a genus 2 curve and an application of elliptic Chabauty as discussed in Chapter 4. We begin with a Lemma establishing a condition for reducibility.

Lemma 5.1. *Let A and B denote rational numbers such that*

$$A = 4u(u^2+3)(3u^2+1)(3u^2+25)^2v^5,$$
$$B = (u^2-5)(3u^2+1)(u^4+10u^2+5)(3u^2+25)^2v^6.$$

for rational numbers u and v. Let $f(x) = x^6 + Ax + B$. If $f(x)$ is reducible over $\mathbb{Q}$, then the cubic polynomial

$$g(x) = x^3 - (3u^2+25)(3u^2+1)x - 4u(3u^2+25)(3u^2+1)$$

has a rational root.

Proof. Let θ denote a root of $f(x)$ and set $K = \mathbb{Q}(\theta)$. It was shown in the proof of the main theorem in [1] that K contains a subfield E defined by

$$g(x) = x^3 - (3u^2+25)(3u^2+1)x - 4u(3u^2+25)(3u^2+1).$$

Suppose that $f(x)$ is reducible over $\mathbb{Q}$, yet $g(x)$ is irreducible over $\mathbb{Q}$. Since the discriminant of $g(x)$ is equal to

$$4(3u^2+1)^2(3u^2-5)^2(3u^2+25)^2,$$

a perfect square in $\mathbb{Q}$, we see that E is a cyclic cubic field and hence $E \subseteq \mathbb{R}$. The degree of K over $\mathbb{Q}$ is divisible by 3 by Theorem 1.7 and less than 6. It follows that $[K : \mathbb{Q}] = 3$ and so $K = E$, which implies $\theta \in \mathbb{R}$ for any root θ of $f(x)$. However, the trinomial $f(x)$ clearly has complex roots, which can be deduced from Rolle's Theorem (Theorem 1.4). This contradiction shows that $g(x)$ must be reducible over $\mathbb{Q}$. □

Lemma 5.2. *The projective curve* $y^2 = x^6 - 3x^4 + 51x^2 + 15$ *has the six points* $\infty^+, \infty^-, (1, 8), (-1, 8), (1, -8), (-1, -8)$.

Proof. The method of elliptic Chabauty as discussed in chapter 5 is used for this determination. We work in the number field defined by a root of $x^3 - 3x^2 + 51x + 15$. This field is $K = \mathbb{Q}(t)$, where $t^3 + 3t + 1 = 0$. The maximal order $O_K = \mathbb{Z}[t]$, and there is one fundamental unit, $\epsilon = t$, which has norm -1. The class number of O_K is 1. We have the following prime ideal factorizations in O_K, which are confirmed by MAPLE$^{\text{TM}}$:

$$\langle 2 \rangle = \wp_2, \qquad \langle 3 \rangle = \wp_3^3, \qquad \langle 5 \rangle = \wp_{51}^2 \wp_{52}$$

where $\wp_2 = \langle 2 \rangle$, $\wp_3 = \langle t + 1 \rangle$, $\wp_{51} = \langle 1 - t \rangle$, and $\wp_{52} = \langle t^2 - t + 3 \rangle$. A scripted $\wp$ notation is used to distinguish prime ideals from a prime integer p.

In the equation specified in this Lemma, we make the substitution $(x, y) = (X/Z, Y/Z^3)$, where $X, Y, Z \in \mathbb{Z}$ and $\gcd(X, Z) = 1$, to obtain

$$Y^2 = X^6 - 3X^4Z^2 + 51X^2Z^4 + 15Z^6. \tag{5.1}$$

This substitution now allows us to use many useful properties of integers.

Next we show that X must be odd, for if X were even, then Z would be odd and equation (5.1) would reduce to

$$Y^2 \equiv 3 (\text{mod} 4),$$

which is impossible. Furthermore, we can see that X is not divisible by 3, for otherwise Z would not be divisible by 3 and equation (5.1) would reduce to

$$Y^2 \equiv 6(\mathrm{mod}9),$$

which is impossible. Finally we can see that $X \not\equiv \pm 2Z(\mathrm{mod}5)$ or else (5.1) reduces to

$$Y^2 \equiv \pm 10(\mathrm{mod}25),$$

which is impossible.

We now factor the right hand side of (5.1) over K to obtain

$$Y^2 = \left(X^2 - (4t+1)Z^2\right)\left(X^4 + 2(2t-1)X^2Z^2 + (16t^2 - 4t + 49)Z^4\right). \quad (5.2)$$

We will now calculate the ideal gcd of the two factors on the right of (5.2) modulo squares. For notation, we use F_2 for the quadratic factor and F_4 for the quartic factor. We begin with 2 identities

$$F_4 - (X^2 + (8t-1)Z^2)F_2 = 48Z^4(1+t^2)$$

and

$$(1+4t)^2F_4 - ((-32t^2 + 8t - 47)X^2 + 15Z^2)F_2 = 48X^4(1+t^2),$$

which can be obtained through the division algorithm for polynomials. Since $\gcd(X, Z) = 1$ and as ideals we have

$$\wp_{51} = \left\langle 1 + t^2 \right\rangle,$$

we see that the ideal gcd of F_2 and F_4 divides

$$\langle 48 \rangle \, \wp_{51}$$

and therefore consists of some powers of (2), $\wp_3$, and $\wp_{51}$. We will consider these cases of ideals to determine the power of each ideal in the gcd modulo squares.

Case i. The power of $\langle 2 \rangle$ in the gcd. We expand F_2 to get

$$F_2 = X^2 - Z^2 - 4tZ^2.$$

We already know that X is odd. Therefore $\langle 2 \rangle$ divides F_2 if and only if Z is odd, in which case we have $8 \mid (X^2 - Z^2)$ so that $\langle 2 \rangle^2 \parallel F_2$. Turning to F_4, we note that since

$$F_2 F_4 = Y^2,$$

then $\langle 2 \rangle^{0 \text{ or } 2} \parallel F_2$ and we conclude that $\langle 2 \rangle^{even} \parallel F_4$. This eliminates the presence of $\langle 2 \rangle$ in the gcd modulo squares.

Case ii. The power of $\wp_3$ in the gcd. Since

$$\wp_3 = \langle t + 1 \rangle,$$

we have

$$t \equiv -1 (\mathrm{mod} \wp_3).$$

Hence

$$F_2 = X^2 - (4t + 1)Z^2 \equiv X^2 + 3Z^2 (\mathrm{mod} \wp_3)$$

and so $\wp_3 \mid F_2$ if and only if $3 \mid X$ which was ruled out earlier. Therefore

$$\wp_3 \nmid \gcd(F_2, F_4)$$

and is also eliminated from the gcd modulo squares.

Case iii. The power of $\wp_{51}$ in the gcd. Since we know that

$$1 + t^2 \equiv 0 (\mathrm{mod} \wp_{51}),$$

we must have either $t \equiv 2(\mathrm{mod}\wp_{51})$ or $t \equiv 3(\mathrm{mod}\wp_{51})$. From

$$t^3 + 3t + 1 \equiv 0(\mathrm{mod}\wp_{51}),$$

we are left only with the possibility that

$$t \equiv 2(\mathrm{mod}\wp_{51}).$$

Using this congruence and recalling our expressions for F_2 and F_4, we deduce that

$$\begin{aligned} F_2 &\equiv X^2 + Z^2(\mathrm{mod}\wp_{51}) \\ &\equiv (X + 3Z)(X + 2Z)(\mathrm{mod}\wp_{51}) \end{aligned}$$

and

$$\begin{aligned} F_4 &\equiv X^4 + X^2Z^2(\mathrm{mod}\wp_{51}) \\ &\equiv X^2(X + 3Z)(X + 2Z)(\mathrm{mod}\wp_{51}). \end{aligned}$$

These two identities show that

$$\wp_{51} \mid \gcd(F_2, F_4) \Leftrightarrow X \equiv \pm 2Z(\mathrm{mod}5),$$

but these possibilities were already ruled out earlier. Therefore, $\wp_{51} \nmid \gcd(F_2, F_4)$ and $\wp_{51}$ is not a factor in the gcd modulo squares.

Through these three cases, we can see that the ideal gcd of the factors F_2 and F_4 is equal to 1 modulo squares. Therefore we can deduce that F_2 and F_4 must each be equal to a square multiplied by some product of fundamental units. This gives rise to four pairs of element equations

$$F_2 = gU^2, \quad F_4 = gV^2$$

Table 5.1: Local Solvability of the Quadratic

(i_0, i_1)	locally insolvable at
$(0,1)$	$\wp_3$
$(1,0)$	$\wp_3$

with $Y = gUV$ and

$$g = (-1)^{i_0}(t)^{i_1}, \quad i_0, i_1 = 0, 1.$$

Next we turn to local solvability. We can rule out two of the above pairs by testing the quadratic. The results are given in a table.

This leaves only the possibilities

$$(i_0, i_1) = (0,0), (1,1).$$

Case 1. $(i_0, i_1) = (0,0)$ In this case, the quartic

$$Y^2 = X^4 + 2(2t-1)X^2 + (16t^2 - 4t + 49)$$

defines an elliptic curve of rank 1 over K, confirmed by the *PseudoMordell-WeilGroup* command in Magma [3]. Using the elliptic Chabauty routines in Magma with $p = 17$, we find two points at infinity as well as $X = 0$. This value $X = 0$ does not yield a point on the original sextic

$$y^2 = x^6 - 3x^4 + 51x^2 + 15.$$

Case 2. $(i_0, i_1) = (1,1)$. In this case, the quartic

$$Y^2 = -t(X^4 + 2(2t-1)X^2 + (16t^2 - 4t + 49))$$

also defines an elliptic curve of rank 1 over K, once again using *PseudoMordellWeilGroup* in Magma. Using the elliptic Chabauty routines in

Magma again with $p = 17$, we find two choices for X, namely $X = \pm 1$. These lead to the points

$$(x, y) = (\pm 1, \pm 8)$$

Together Case 1 and Case 2 yield all 6 points in the statement of the Lemma. □

We can now use this lemma to assess the reducibility of our family of trinomials.

Lemma 5.3. *Let $f(x) = x^6 + Ax + B$ where the nonzero rational numbers A and B are given by*

$$A = 4u(u^2 + 3)(3u^2 + 1)(3u^2 + 25)^2 v^5$$
$$B = (u^2 - 5)(3u^2 + 1)(u^4 + 10u^2 + 5)(3u^2 + 25)^2 v^6$$

for nonzero rational numbers u and v. Then $f(x)$ is irreducible over $\mathbb{Q}$.

Proof. Suppose that $f(x)$ is reducible over $\mathbb{Q}$ for some nonzero value of u. Since v is a nonzero scaling factor, we may assume that $v = 1$. By Lemma 5.1, $g(x)$ must also be reducible over $\mathbb{Q}$ where $g(x)$ is given by

$$g(x) = x^3 - (3u^2 + 25)(3u^2 + 1)x - 4u(3u^2 + 25)(3u^2 + 1).$$

Reducibility of $g(x)$ implies the existence of linear factor in $\mathbb{Q}[x]$ and therefore a rational root. Thus, there exists a rational number r such that

$$r^3 - (3u^2 + 25)(3u^2 + 1)r - 4u(3u^2 + 25)(3u^2 + 1) = 0. \tag{5.3}$$

Viewed as an algebraic curve, (5.3) has genus 2 and is birationally equivalent to

$$y^2 = x^6 - 3x^4 + 51x^2 + 15$$

via the transformations:

$$x = \frac{3u^2 - 5}{r + 6u},$$
$$y = -\frac{-75r^2 + 3r^4 - 2000 - 12ur^3 - 234r^2u^2 - 6240u^2 - 27u^4r^2 - 720u^4}{2r^3},$$
$$r = \frac{8x^5 - 48x^3 - 216x - (24 + 8x^2)y}{2(-3x^4 - 3 + 6x^2)},$$
$$u = \frac{-x^3 + 9x + y}{-3x^2 + 3}.$$

These transformations can easily be found using MAPLE$^{\text{TM}}$and confirmed by substitution. Since $u \neq 0$, a simple calculation using (5.3) confirms that we must have $r \neq 0, r \neq -6u$ so that any point on the first curve contributes a point on the second curve. By Lemma 5.2, the only finite rational points on the second curve are $(\pm 1, \pm 8)$. None of these points transfers back to the first curve as the denominators in the transformations for r and u are equal to 0 for $x = \pm 1$. Hence $g(x)$ has no rational root and therefore $f(x)$ is irreducible over $\mathbb{Q}$. □

Having eliminated the possibility of reducible trinomials in our parametric family, we can introduce a Lemma which will assist in our determination of specific Galois groups.

Lemma 5.4. *Let u denote a nonzero rational number. Then the quantity*

$$-(3u^2 + 1)(u^6 - 15u^4 - 225u^2 - 225)$$

is not equal to a square in $\mathbb{Q}$.

Proof. Suppose by way of contradiction that for some nonzero rational number u, the given quantity is equal to a square in $\mathbb{Q}$. We may assume that u is positive. In this expression we make a substitution $u = a/b$ where a, b

are nonzero integers with $\gcd(a, b) = 1$. By clearing the denominator b^6, we have

$$-G_1G_2 = \text{ a square in } \mathbb{Q}$$

where

$$G_1 = (3a^2 + b^2),$$
$$G_2 = (a^6 - 15a^4b^2 - 225a^2b^4 - 225b^6).$$

Using division of polynomials we obtain the identities

$$-27G_2 + (9a^4 - 138a^2b^2 - 1979b^4)G_1 = 2^{12}b^6$$

and

$$G_2 - (-1365a^4 + 450a^2b^2 - 225b^4)G_1 = 2^{12}a^6.$$

Using these identities and recalling that $\gcd(a, b) = 1$, we see that if we define $d = \gcd(G_1, G_2)$, then $d = 2^k$ for some nonnegative integer k. If $k > 0$, then $2 \mid G_1$ so we must have a and b odd and

$$a \equiv b \equiv 1 (\mathrm{mod} 2),$$

in which case a calculation shows that

$$2^2 \parallel G_1 \text{ and } 2^4 \parallel G_2.$$

Therefore,

$$\gcd(G_1, G_2) = 1 \text{ or } 2^2$$

and in either case is equal to a square. It follows that since $G_1 > 0$, both of G_1 and $-G_2$ are squares in $\mathbb{Q}$. Continuing, since $a \neq 0$, we have

$$\frac{1}{a^6}G_2 = \text{ a square in } \mathbb{Q}.$$

In this last equation we set $x = \dfrac{b^2}{a^2}$. We can now conclude that

$$y^2 = 225x^3 + 225x^2 + 15x - 1$$

with $y \in \mathbb{Q}$. This last equation can be viewed as an elliptic curve over $\mathbb{Q}$ and using MAPLE$^{\text{TM}}$, we find that it is birationally equivalent to

$$Y^2 = X^3 - 13500X + 540000$$

via the transformations:

$$\begin{aligned} X &= 225x + 75, \\ Y &= 225y, \\ x &= \frac{X}{225} - \frac{1}{3}, \\ y &= \frac{Y}{225}. \end{aligned}$$

Using Magma we find that the rank of this curve is equal to zero and it has no finite rational points. Therefore we conclude that $-G_1G_2$ cannot equal a square in $\mathbb{Q}$, completing the proof of the Lemma. □

5.3 Proof of Theorem

We give the proof of Theorem 5.1.

Proof. As noted at the beginning of the chapter, irreducible trinomials $x^6 + Ax + B \in \mathbb{Q}[x]$ with Galois group isomorphic to either A_4 or $A_4 \times C_2$ over $\mathbb{Q}$ define sextic fields with a cyclic cubic subfield. By Lemma 5.1, A and B are given by

$$\begin{aligned} A &= 4u(u^2+3)(3u^2+1)(3u^2+25)^2v^5, \\ B &= (u^2-5)(3u^2+1)(u^4+10u^2+5)(3u^2+25)^2v^6, \end{aligned}$$

for rational numbers u and v with $u \neq 0$ and $v \neq 0$. It was shown in [20] that the Galois group of $f(x)$ is C_6 if and only if $u = \pm 5$. These values of u yield the unique cyclic sextic trinomial up to scaling which was given in the introduction of this chapter as

$$x^6 + 133x + 209.$$

The remaining choices of u and v, namely $u \neq 0, u \neq \pm 5, v \neq 0$, will produce a trinomial with Galois group isomorphic to either A_4 or $A_4 \times C_2$. Fortunately, we can distinguish between these possibilities with a useful fact regarding the the polynomial discriminant of $f(x)$, as given by [9, p. 327]. Cohen states that the Galois group of $f(x)$ is isomorphic to A_4 if and only if its discriminant is equal to a square in $\mathbb{Q}$. The discriminant of $f(x)$ given by MAPLE$^{\text{TM}}$, is equal to

$$-2^6(3u^2+1)^5(u^6-15u^4-225u^2-225)(3u^2+25)^{10}\times$$
$$(27u^{12}+540u^{10}+6075u^8+29600u^6+20625u^4+22500u^2+5625)^2.$$

The squarefree part of this discriminant is equal to

$$-(3u^2+1)(u^6-15u^4-225u^2-225).$$

It was shown in Lemma 5.4 that for $u \neq 0$, this quantity is not equal to a square in $\mathbb{Q}$. Hence the Galois group of $x^6 + Ax + B$ cannot be isomorphic to A_4. The only remaining possibility for the Galois group is $A_4 \times C_2$. This completes the proof of our theorem. □

Chapter 6

Sextic Trinomials $x^6 + Ax + B$ Defining Normal Sextic Extensions of Number Fields

6.1 Main Theorem and Corollaries

Let $f(x)$ be a polynomial with coefficients in an algebraic number field K. Assume that $f(x)$ is irreducible over K. Let $Gal(f)$ denote the Galois group of $f(x)$. We are interested in determining those irreducible trinomials $f(x) = x^6 + Ax + B$, with A, B nonzero elements of K, which define normal sextic extensions of K. A discussion of the Galois group of a sextic polynomial and the theory of resolvents used to calculate them is available in Cohen, [9, p. 323], or Jensen, Ledet and Yui [22]. Irreducible polynomials, $f(x) \in K[x]$ defining normal extensions of K can only have two possible Galois groups, namely C_6 the cyclic group of order 6 or S_3 the symmetric group on three letters. These Galois groups are denoted by 6T1 or 6T2, respectively in the notation of Butler and Mckay [2]. Our determination will establish a correspondence between these trinomials and the $K-$ rational points on a genus two curve. As a consequence of Faltings' theorem [16], there are finitely many $K-$ rational points on this curve hence finitely many normal extensions of the type we are interested in. As a bonus, our method will determine trinomial sextic extensions with Galois group $C_3 \times D_3$, or 6T5 again referring to [2]. We apply our method to find all trinomials x^6+Ax+B

with one of these three Galois groups over $\mathbb{Q}$. Using the method of elliptic Chabauty, we determine the rational points on our genus 2 curve in the case $K = \mathbb{Q}$ and find that there is a unique normal trinomial sextic extension and no occurrence of the Galois groups S_3 or $C_3 \times D_3$. The details of elliptic Chabauty are given by Bruin [23]. Our main results are the following.

Theorem 6.1. *Let K be an algebraic number field. If $f(x) = x^6 + Ax + B \in K[x]$ is irreducible over $\mathbb{Q}$ and has Galois group C_6, S_3, or $C_3 \times D_3$, then there exist elements u, v and $w \in K$ with $u \neq 0$ and $v \neq 0$, such that*

$$\begin{aligned} A &= 4u(3u+1)v^5 \\ B &= -u(1-18u+u^2)v^6 \end{aligned} \tag{6.1}$$

and

$$(3w^2+144)u^2 + (-672 + 4w^4 + 210w^2)u + 784 + 27w^2 = 0. \tag{6.2}$$

Corollary 6.1. *There is a single normal sextic extension of $\mathbb{Q}$ defined by an irreducible trinomial with rational coefficients. It is $\mathbb{Q}(\theta)$ where θ is a root of*

$$x^6 + 133x + 209.$$

Corollary 6.2. *There do not exist trinomials $x^6 + Ax + B \in \mathbb{Q}[x]$ with Galois group S_3 or G_{18}.*

Corollary 6.3. *Let K be an algebraic number field and suppose that A and B are nonzero elements of K such that $x^6 + Ax + B$ is irreducible over K. The set of trinomials $x^6 + Ax + B$ with Galois group C_6, S_3, or $C_3 \times D_3$ is finite.*

In section 2 of this chapter, some preliminary Lemmas are given to assist in our determination. In section 3 we study the rational points on a genus 2 curve. In section 4 we prove our theorem and corollaries.

6.2 Preliminary Results

We begin with a family of trinomials defining sextic fields which contain a quadratic subfield. This family would seem to be well known, but unable to find a reference for it we give a short proof.

Lemma 6.1. *Let A and B denote nonzero rational numbers such that $f(x) = x^6 + Ax + B$ is irreducible over K. Then $f(x)$ defines a sextic field containing a quadratic subfield if and only if there exist rational numbers u and v with u not equal to a square in $\mathbb{Q}$ such that*

$$\begin{aligned} A &= 4u(3u+1)v^5, \\ B &= -u(1-18u+u^2)v^6. \end{aligned} \tag{6.3}$$

The quadratic subfield is $\mathbb{Q}(\sqrt{u})$.

Proof. Let θ be a root of $f(x)$ and set $L = K(\theta)$ and suppose that L has a quadratic subfield E containing K. Since the degree $[L : E] = 3$, the minimal polynomial $g(x)$ of θ in $E[x]$ has degree 3 and hence has the form

$$g(x) = x^3 + (m + n\sqrt{t})x^2 + (p + q\sqrt{t}) + (r + s\sqrt{t})$$

for elements $m, n, p, q, r, s, t \in K$ with t not equal to a square in K. Clearly $t \neq 0$. If we define $\overline{g}(x)$ by

$$\overline{g}(x) = x^3 + (m - n\sqrt{t})x^2 + (p - q\sqrt{t}) + (r - s\sqrt{t})$$

we see that θ is a root of $h(x) = g(x)\overline{g}(x) \in K[x]$. The polynomial $h(x)$ is given explicitly by

$$\begin{aligned} h(x) = x^6 + 2mx^5 + (m^2 - n^2t + 2p)x^4 + (2mp - 2nqt + 2r)x^3 \\ + (2mr - 2nst + p^2 - q^2t)x^2 + (2pr - 2qst)x + r^2 - s^2t. \end{aligned}$$

By uniqueness of the minimal polynomial of θ over K we deduce that $f(x) = h(x)$. Thus we can equate coefficients of $f(x) - h(x)$ to zero to solve for A and B. Begin with the coefficient of x^5, which yields the equation

$$2m = 0,$$

so that $m = 0$. Substituting $m = 0$ into $f(x) - h(x)$ and examining the coefficient of x^4, we obtain the equation

$$\frac{n^2t}{2} = p.$$

Substituting both $m = 0$ and $p = \dfrac{n^2t}{2}$ into $f(x) - h(x) = 0$ and examining the coefficient of x^3 gives the equation

$$-2nqt + 2r = 0,$$

so that

$$r = nqt.$$

Substituting all of the previous equations into $f(x) - h(x) = 0$, we note that the coefficient of x^2 yields the equation

$$\frac{t(n^4t - 8ns - 4q^2)}{4} = 0.$$

Since $t \neq 0$ we deduce that

$$\frac{(n^4t - 8ns - 4q^2)}{4} = 0.$$

If $n = 0$, then it would follow from the previous equation that $q = 0$. This would imply from equating the coefficient of x to zero that

$$A = 0,$$

which contradicts the assumption that $A \neq 0$. Therefore $n \neq 0$. Hence we may solve the above equation for s giving

$$s = \frac{n^4 t - 4q^2}{8n}.$$

Substitution of this value of s into the coefficients of x and the constant term yields the equations

$$\frac{-3n^4t^2q - 4q^3t + 4An}{4n} = 0.$$

and

$$\frac{-72n^4q^2t^2 + n^8t^3 + 16n^4t + 64Bn^2}{64n^2} = 0.$$

Since n was shown to be nonzero, and $A \neq 0$ by assumption, the first equation shows that $q \neq 0$. Applying a scaling on A and B and a change of variable on q and t, specifically $q \to n^2q, t \to 4q^2u, A \to n^5q^5A, B \to n^6q^6B$ yields the equations

$$-n^5q^5(-12u^2 - 4u + A) = 0$$

and

$$-n^6q^6(-18u^2 + u^3 + u + B) = 0.$$

Cancelling the nonzero factors in each equation and solving for A and B gives the values of A and B stated in the theorem. Finally we insert a scaling factor v to get the general polynomial. Conversely, a simple calculation shows that $f(x)$ factors into a pair of conjugate cubics over $K(\sqrt{u})$, showing that L contains a quadratic subfield. □

Next we give a condition which enables us to determine when x^6+Ax+B defines a normal extension of K, which is given in Dummit and Foote [11, p.525].

Proposition 6.1 (Dummit and Foote p. 525)**.** *Let K be a field of characteristic zero and $f(x) \in K[x]$ with degree n. Then the Galois group of $f(x)$ is a subgroup of A_n if and only if the discriminant of $f(x)$ is a square in K.*

The previous proposition is now specialized to trinomials $x^6 + Ax + B$.

Lemma 6.2. *Let A and B denote nonzero rational numbers such that $f(x) = x^6 + Ax + B$ is irreducible over K. If $f(x)$ defines a relative normal cubic extension field over a quadratic extension field of K then there exist nonzero elements u, v in K with u not equal to a square in K such that*

$$A = 4u(3u+1)v^5$$
$$B = -u(1 - 18u + u^2)v^6$$

and

$$-(-112\sqrt{u} + 210u + 48u\sqrt{u} + 3u^2 + 27) = (a + b\sqrt{u})^2$$

for some elements a and b, belonging to K.

Proof. If $f(x) = x^6 + Ax + B$ defines a relative cubic extension field L over a quadratic extension field of K then by Lemma 6.1, there exist nonzero elements u, v in K such that

$$A = 4u(3u+1)v^5$$
$$B = -u(1 - 18u + u^2)v^6.$$

We may assume that $v = 1$, replacing $f(x)$ as necessary by $\frac{1}{v^6} f(vx)$. One of the factors of $f(x)$ over $K(\sqrt{u})$ is

$$x^3 + 2\sqrt{u}x^2 + (2\sqrt{u} + 2u)x + 4u + u\sqrt{u} - \sqrt{u}.$$

If in addition $L/K(\sqrt{u})$ is normal and of degree 3, we know that the Galois group of $L/K(\sqrt{u})$ must be isomorphic to A_3. Proposition 6.1 shows that

the discriminant of this cubic must be a square in $K(\sqrt{u})$. This discriminant is

$$-u(-112\sqrt{u}+210u+48u\sqrt{u}+3u^2+27).$$

Since u is obviously a square in $K(\sqrt{u})$, we deduce that there must exist elements $a, b \in K$ such that

$$-(-112\sqrt{u}+210u+48u\sqrt{u}+3u^2+27) = (a+b\sqrt{u})^2$$

thus establishing the Lemma. □

The condition given in the previous Lemma can be converted to a genus 2 curve as is shown in the following Lemma.

Lemma 6.3. *If $f(x) = x^6+Ax+B$ defines a relative normal cubic extension field over a quadratic extension field of K so that A and B are given by 6.1 with u not equal to a square in K and a, b are elements of K such that*

$$-(112\sqrt{u}+210u-48u\sqrt{u}+3u^2+27) = (a+b\sqrt{u})^2,$$

then

$$(3w^2+144)u^2+(-672+4w^4+210w^2)u+784+27w^2 = 0,$$

for some element $w \in K$.

Proof. Under the assumptions stated in the lemma, we have

$$-(-112\sqrt{u}+210u+48u\sqrt{u}+3u^2+27) = (a+b\sqrt{u})^2.$$

Equating the coefficients of 1 and$\sqrt{u}$ we deduce the pair of equations

$$48u+2ab-112 = 0$$
$$3u^2+(b^2+210)u+27+a^2 = 0.$$

If $b = 0$ then the first equation yields $u = 7/3$, which corresponds to $w = 0$ in the equation stated in this lemma. If $b \neq 0$, we use a resultant to eliminate the variable a to obtain an equation in b and u, then set $b = 2w$ and divide by 16, obtaining the result stated in this Lemma. □

The algebraic curve

$$(3w^2 + 144)u^2 + (-672 + 4w^4 + 210w^2)u + 784 + 27w^2 = 0$$

from Lemma 6.3 is birationally equivalent to

$$y^2 = x^6 + 105x^4 + 2400x^2 - 19200$$

via the transformations:

$$\begin{aligned} x &= w, \\ y &= \frac{(3w^2 + 144)u - 336 + 2w^4 + 105w^2}{2w}, \\ w &= x, \\ u &= \frac{336 - 2x^4 - 105x^2 + 2xy}{3x^2 + 144}. \end{aligned}$$

These transformations can easily be found through MAPLE$^{\text{TM}}$and can be confirmed by substitution.

Lemma 6.4. *The projective curve* $y^2 = x^6 + 105x^4 + 2400x^2 - 19200$ *has the six points* ∞^+, ∞^-, $(4, 224)$, $(-4, 224)$, $(4, -224)$, $(-4, -224)$.

Proof. This proof uses the method known as elliptic Chabauty. Computations involved are supported by Magma [3]. We work in the number field defined by a root of $x^3 + 105x^2 + 2400x - 19200$. This field is $K = \mathbb{Q}(t)$,

where $t^3 - 15t + 20 = 0$. The maximal order $O_K = \mathbb{Z}[t]$, and there are two fundamental units which we can take to be

$$\epsilon_1 = 8t^2 + 22t - 59, \quad \epsilon_2 = -13t^2 - 21t + 161,$$

both of norm 1.The class number of O_K is 1. We have the following prime ideal factorizations in O_K :

$$\langle 2 \rangle = \wp_{21}\wp_{22}^2 = \langle t-2 \rangle \langle t-3 \rangle^2, \tag{6.4}$$

$$\langle 3 \rangle = \wp_3^3 = \left\langle t^2 + 3t - 7 \right\rangle^3, \tag{6.5}$$

$$\langle 5 \rangle = \wp_5^3 = \left\langle t^2 + t - 15 \right\rangle^3. \tag{6.6}$$

Once again, a scripted notation is used to differentiate prime ideals from prime integers. Assuming a solution (x, y) to the equation specified in this Lemma, put $(x, y) = \left(X/Z, Y/Z^3\right)$, where $X, Y, Z \in \mathbb{Z}$, $\gcd(X, Z) = 1$, giving

$$Y^2 = X^6 + 105X^4Z^2 + 2400X^2Z^4 - 19200Z^6. \tag{6.7}$$

We note that X is not divisible by 3, for otherwise Z would not be divisible by 3 and equation (6.7) would reduce to

$$Y^2 \equiv 6 (\mathrm{mod} 9),$$

which is impossible.

Factoring the right hand side of (6.7) over K gives

$$Y^2 = F_2F_4 \tag{6.8}$$

where

$$F_2 = X^2 - (7t^2 + 20t - 105)Z^2$$

and

$$F_4 = X^4 + (7t^2 + 20t)X^2Z^2 + (1120t + 400t^2 - 3200)Z^4$$

We will calculate the ideal gcd of the two factors F_2 and F_4. Begin with the following two identities.

$$F_4 = (X^2 + (14t^2 + 40t - 105)Z^2)F_2 + 15(31t^2 + 84t - 225)Z^4,$$

and

$$4F_4 = (-46t^2 - 129t + 332)F_2 + (46t^2 + 129t - 328)X^4.$$

As ideals, the factorization of the remainders is

$$\wp_{22}^{12}\wp_3^3\wp_5^4 \left\langle Z^4 \right\rangle \text{and} \wp_{21}^2\wp_3 \left\langle X^4 \right\rangle .$$

Since the integers X and Z are relatively prime, the only possible prime ideal divisor of both F_2 and F_4 is $\wp_3$. From the remark at the start of this proof, we know that $3 \nmid X$ so that $\wp_3 \nmid F_2$. Hence the ideal gcd of F_2 and F_4 modulo squares is equal to 1. Thus we can deduce a pair of element equations

$$\begin{aligned} &X^2 - (7t^2 + 20t - 105)Z^2 = gU^2, \\ &X^4 + (7t^2 + 20t)X^2Z^2 + (1120t + 400t^2 - 3200)Z^4 = gV^2, \end{aligned}$$

with

$$Y = gUV \quad \text{and} \quad g = (-1)^{i_0}\epsilon_1^{i_1}\epsilon_2^{i_2},\ i_0, i_1, i_2 = 0, 1.$$

Using local solvability in Magma, we can rule out 6 of the above pairs of equations by testing the quadratic $Y = g(x^2 - (7t^2 + 20t - 105))$. We present the results in a table.

Table 6.1: Local Solvability of the Quadratic

(i_0, i_1, i_2)	locally insolvable at
$(0,0,1)$	$\wp_{22}$
$(0,1,1)$	$\wp_{22}$
$(1,0,0)$	$\wp_{21}$
$(1,0,1)$	$\wp_{21}$
$(1,1,0)$	$\wp_{21}$
$(1,1,1)$	$\wp_{21}$

For the remaining cases $(i_0, i_1, i_2) = (0,0,0)$ and $(0,1,0)$ working with the quartics

$$V^2 = X^4 + (7t^2 + 20t)X^2Z^2 + (1120t + 400t^2 - 3200)Z^4$$

and

$$(\epsilon_1 V)^2 = \epsilon_1(X^4 + (7t^2 + 20t)X^2Z^2 + (1120t + 400t^2 - 3200)Z^4),$$

A rational point X/Z satisfying either of these quartics contributes a point (x, y) with $x \in \mathbb{Q}$ on one of the elliptic curves

$$y^2 = x(x^2 + (7t^2 + 20t)x + (1120t + 400t^2 - 3200))$$

or

$$y^2 = \epsilon_1 x(x^2 + (7t^2 + 20t)x + (1120t + 400t^2 - 3200))$$

We find using the *PseudoMordellWeilGroup* routine in Magma that the ranks of these elliptic curves are both equal to 1. Using the elliptic Chabauty procedure in Magma, with prime $p = 17$ in both cases, successfully determines the points (x, y) on these curves with $x \in \mathbb{Q}$, which give all of the points on the genus 2 curve stated in this lemma. □

6.3 Proof of Theorem and Corollaries

We give the proof of Theorem 6.1, then the proofs of our corollaries.

Proof. If $f(x) = x^6 + Ax + B \in K[x]$ is irreducible over K and has Galois group C_6, S_3 or $C_3 \times D_3$ then $f(x)$ defines a normal relative cubic extension of a quadratic extension of K so that A and B are given by 6.1 by Lemma 6.1 and the quadratic extension field of K is $K(\sqrt{u})$. This statement is obvious for the Galois groups C_6 and S_3 while for $C_3 \times D_3$ the splitting field of $f(x)$ over $K(\sqrt{u})$ has degree 9, so is an abelian extension of $K(\sqrt{u})$. We may assume that the nonzero scaling factor $v = 1$. From Lemma 6.2 we see that

$$-(112\sqrt{u} + 210u - 48u\sqrt{u} + 3u^2 + 27) = (a + b\sqrt{u})^2$$

for some rational numbers a and b. Lemma 6.3 shows that

$$(3w^2 + 144)u^2 + (-672 + 4w^4 + 210w^2)u + 784 + 27w^2 = 0.$$

for some element $w \in K$, which establishes (6.2). □

Next we prove Corollary 6.1.

Proof. Suppose that $L/\mathbb{Q}$ is a normal extension defined by an irreducible trinomial $x^6 + Ax + B \in \mathbb{Q}[x]$. By Theorem 6.1 equations (6.1) and (6.2), we have

$$A = 4u(3u + 1)v^5$$
$$B = -u(1 - 18u + u^2)v^6$$

and

$$(3w^2 + 144)u^2 + (-672 + 4w^4 + 210w^2)u + 784 + 27w^2 = 0$$

for rational numbers u, v and w. From (6.2) we calculate the discriminant with respect to u and deduce that

$$16w^2(w^6 + 105w^4 + 2400w^2 - 19200)$$

is equal to a square in $\mathbb{Q}$. One possibility is $w = 0$, in which case (6.3) reduces to

$$16(3u - 7)^2 = 0$$

so that $u = 7/3$. Using (6.2) and setting the scaling factor $v = 1$, we obtain the trinomial

$$x^6 + 224/3x + 2240/27,$$

which has Galois group $D_3 \times D_3$ (or 6T9 in the notation of Butler and McKay [2]) and does not define a normal extension of $\mathbb{Q}$. If $w \neq 0$ then we must have $w^6 + 105w^4 + 2400w^2 - 19200$ equal to a square in $\mathbb{Q}$ and we can invoke Lemma 6.4, which shows that $w = \pm 4$. Appealing to (6.3), we obtain $u = -1/3$ or $u = -19$. The first value of u yields a reducible polynomial, while the second value of u gives

$$x^6 + 133x + 209$$

after scaling, which defines a normal extension with Galois group C_6 as seen in Chapter 5, completing the proof. □

Since all trinomials with Galois group C_6, S_3, or $C_3 \times D_3$ were determined in the proof of Corollary 6.1, the proof of Corollary 6.2 is immediate. For Corollary 6.3, the finitude of sextic trinomials under study is guaranteed by their correspondence with the $K-$ rational points on the genus 2 curve and the theorem of Faltings.

Chapter 7

Results and Future Work

7.1 Results

We give our findings from the theorems proved in Chapter 5 and Chapter 6 in the form of a table. Here "T-notation" refers to the notation of Butler and Mckay [2]. A total of five solvable Galois groups have been completely categorized for trinomials $x^6 + Ax + B$ with $A, B \in \mathbb{Q}$.

In the case of trinomials $x^6 + ax + b$ with $a, b \in \mathbb{Q}$ defining normal sextic extensions of $\mathbb{Q}$, the trinomial

$$x^6 + \frac{224}{3}x + \frac{2240}{27}$$

was discovered to have Galois group $G_{36} \cong D_3 \times D_3$ in Chapter 6. This did not define a normal sextic extension of $\mathbb{Q}$ and we do not claim it to be the only trinomial of this form to have a Galois group of G_{36}.

Also recall that in the case of our trinomials

$$f(x) = x^6 + Ax + B,$$

that $f(x)$ has Galois group $A_4 \times C_2$ if and only if

$$\begin{aligned} A &= 4u(u^2+3)(3u^2+1)(3u^2+25)^2v^5, \\ B &= (u^2-5)(3u^2+1)(u^4+10u^2+5)(3u^2+25)^2v^6. \end{aligned}$$

for some $u, v \in \mathbb{Q}$ with $u \neq 0, \pm 5$ and $v \neq 0$. This generates infinitely many trinomials with Galois group $A_4 \times C_2$ as given in the above table. However, it must be noted that the occurrence of such a Galois group amongst all

Table 7.1: List of Findings

T-notation	Group notation	For trinomials $x^6 + Ax + B$, $A, B \in \mathbb{Q}$
$6T1$	C_6	$x^6 + 133x + 209$ (up to scaling)
$6T2$	S_3	Does not occur
$6T4$	A_4	Does not occur
$6T5$	$G_{18} \cong C_3 \times D_3$	Does not occur
$6T6$	$A_4 \times C_2$	Infinitely many
$6T10$	$G_{36} \cong D_3 \times D_3$	At least $x^6 + 224/3x + 2240/27$ (up to scaling)

trinomials is very rare. In the case of A and B both integers we find

$$x^6 + 49x - 49$$

for $(u, v) = (1, 1/4)$,

$$x^6 + 10647x - 13013$$

for $(u, v) = (3, 1/4)$, and

$$x^6 + 996632x - 1085617$$

for $(u, v) = (2, 1)$ all have Galois group $A_4 \times C_2$, showing that an extensive search is necessary for even a few example polynomials.

As mentioned in Chapter 3, a trinomial $x^6 + ax + b$ with $a, b \in \mathbb{Q}$ chosen at random will almost certainly have a Galois group of S_6, which can be calculated in MAPLE$^{\text{TM}}$. Any case that yields a result other than S_6 (even if there are infinitely many) is an exceptional result, particularly when it implies that the polynomial itself is solvable.

7.2 Future Work

The methods and procedures used in obtaining the main results in this thesis lend themselves to many future extensions of this work. Firstly and most obviously, a complete determination of all sixteen possible Galois groups for trinomials $x^6 + Ax + B$ with $A, B \in \mathbb{Q}$ would provide a great deal of future work. In order to accomplish this, further criteria would be needed to establish parametric families of polynomials that would give a desired selection of Galois groups. From this, further investigation into these parametrizations through the use of elliptic Chabauty could yield a complete determination of each individual Galois group.

Secondly, an investigation intro trinomials of other forms, namely $x^6 + Ax^2 + B$, would require similar calculations as those used in this thesis. These results would translate directly to trinomials of the forms x^6+Ax^4+B and $x^6 + Ax^5 + B$ through a simple transformation. Trinomials of the form x^6+Ax^3+B could also be looked at, though they could easily be considered as quadratics in x^3. It would also be theoretically possible to look at sextic polynomials with an additional number of terms.

Finally, another possible extension of this work would be to analyze sextic trinomials over fields other than $\mathbb{Q}$. Much of theory used to create the restrictions on the coefficients of these trinomials can be applied to a field extension K of $\mathbb{Q}$.

Bibliography

[1] B. K. Spearman, *Trinomials $x^6 + Ax + B$ defining sextic fields with a cyclic cubic subfield*, J. Appl. Algebra Discrete Struct. **4** (2006), 149–155.

[2] G. Butler and J. McKay, *The transitive groups of degree up to eleven*, Comm. Algebra **11** (1983), 863–911.

[3] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), 235–265 (Computational algebra and number theory (London, 1993)).

[4] S. C. Brown, B. K. Spearman, and Q. Yang, *On the Galois groups of sextic trinomials*, JP J. Algebra Number Theory Appl. **18** (2010), 67–77.

[5] A. Marshall, *Precalculus: functions and graphs*, Addison-Wesley Pub., 1990.

[6] I. Stewart, *Galois theory*, Second edition, Chapman and Hall Ltd., London, 1989.

[7] J. Stewart, *Calculus: Early Transcendentals Single Variable*, Fifth edition, Brooks/Cole, 2003.

[8] J. B. Fraleigh, *A first course in abstract algebra*, Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1967.

[9] H. Cohen, *A course in computational algebraic number theory*, Vol. 138 of *Graduate Texts in Mathematics*, Springer-Verlag, Berlin, 1993.

[10] F. Seidelmann, *Die gesamtheit der kubischen und biquadratischen gleichungen mit affekt bei beliebigem rationalittsbereich*, Math. Annalen **78** (1918), 230–233.

[11] D. S. Dummit, *Solving solvable quintics*, Math. Comp. **57** (1991), 387–401.

[12] B. K. Spearman and K. S. Williams, *On solvable quintics $X^5 + aX + b$ and $X^5 + aX^2 + b$*, Rocky Mountain J. Math. **26** (1996), 753–772.

[13] ———, *Characterization of solvable quintics $x^5 + ax + b$*, Amer. Math. Monthly **101** (1994), 986–992.

[14] J. Silverman, *The arithmetic of elliptic curves*, Graduate texts in mathematics, Springer, 2009.

[15] C. Chabauty, *Sur les points rationnels des courbes algébriques de genre supérieur à l'unité*, C. R. Acad. Sci. Paris **212** (1941), 882–885.

[16] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), 349–366.

[17] R. F. Coleman, *Effective Chabauty*, Duke Math. J. **52** (1985), 765–770.

[18] J. W. S. Cassels and E. V. Flynn, *Prolegomena to a middlebrow arithmetic of curves of genus* 2, Vol. 230 of *London Mathematical Society Lecture Note Series*, Cambridge University Press, Cambridge, 1996.

[19] L. C. Washington, *Elliptic curves*, Discrete Mathematics and its Applications (Boca Raton), second edition, Chapman & Hall/CRC, Boca Raton, FL, 2008 (Number theory and cryptography).

[20] A. Bremner and B. K. Spearman, *Cyclic sextic trinomials* $x^6 + Ax + B$, Int. J. Number Theory **6** (2010), 161–167.

[21] M. J. Lavallee, B. K. Spearman, and K. S. Williams, *Reducibility and the galois group of a parametric family of quintic polynomials*, Missouri Journal of Mathematical Sciences **19** (2007), 2–10.

[22] C. U. Jensen, A. Ledet, and N. Yui, *Generic polynomials*, Vol. 45 of *Mathematical Sciences Research Institute Publications*, Cambridge University Press, Cambridge, 2002 (Constructive aspects of the inverse Galois problem).

[23] N. Bruin, *Chabauty methods using elliptic curves*, J. Reine Angew. Math. **562** (2003), 27–49.

Appendix A

Common Group Names and Structures

A.1 The Symmetry Group S_n

The symmetry group S_n is also known as the symmetric group on n letters. This group consists of all the $n!$ permutations of n elements. Any two of these permutations can then be combined together in order to form a single composite permutation.

For instance, the group S_5 consists of the $5! = 120$ permutations of the set $\{1, 2, 3, 4, 5\}$. The identity permutation would be

$$I : (1, 2, 3, 4, 5) \to (1, 2, 3, 4, 5).$$

Other permutations would include

$$\sigma : (1, 2, 3, 4, 5) \to (2, 3, 4, 5, 1),$$
$$\tau : (1, 2, 3, 4, 5) \to (2, 1, 3, 4, 5).$$

These permutations could then be combined:

$$\sigma\tau : (1, 2, 3, 4, 5) \to (1, 3, 4, 5, 2),$$
$$\sigma^3 : (1, 2, 3, 4, 5) \to (4, 5, 1, 2, 3).$$

It should be noted that the order in which the permutations should be applied is important. In the case of $\sigma\tau$, τ should be applied before σ.

A.2 The Alternating Group A_n

To understand the concept of the alternating group on n letters, consider that any permutation as described in the previous section can be expressed as a product of transpositions. A transposition is a permutation that leaves all but two elements fixed; that is, a transposition only interchanges two elements and leaves all other elements unchanged. If a permutation can be expressed as a composition of an even number of transpositions, then it is called an even permutation. A permutation that is not even is called odd; a permutation must either be called even or odd.

With this concept, we can construct a subgroup of S_n of only the even permutations. Like in the case of integers, an even permutation combined with another even permutation gives an even permutation. This subgroup of S_n is exactly the alternating group A_n.

Another interesting property of even and odd permutations is that for a given set of n unique elements, there is an equal number of even and odd permutations. Thus, the number of permutations contained in A_n is exactly $\frac{n!}{2}$.

A.3 The Dihedral Group D_n

The dihedral group D_n is also frequently known as the symmetry group of a regular $n-$sided polygon. Using this idea, we can understand the group structure of the dihedral group. We begin by visualizing two identical copies of a regular $n-$sided polygon with each vertex uniquely labeled 1, 2, etc. The second copy can then be manipulated through rotations about its centre and through mirror images over a bisecting line so that when the two copies

are placed on top of each other, every vertex is covered by another vertex.

This process creates a mapping all of the labeled vertices on the first copy of the polygon to the vertices on the second copy. In fact, these mappings are a subset of the total $n!$ permutations included in S_n and once again form a group under composition.

In the case of an equilateral triangle, a rotation could be viewed as

$$\rho : (1, 2, 3) \to (2, 3, 1)$$

and a mirror image over the line bisecting the angle at vertex 3 could be viewed as

$$\mu_3 : (1, 2, 3) \to (2, 1, 3).$$

Both of these mappings belong to the group D_3.

A.4 The Cyclic Group C_n

A cyclic group has the unique property of being generated by a single element. Following the same idea of permutations, a cyclic group can be generated by taking any permutation α on m elements other than the identity mapping and applying it until the composition results in the identity mapping. If this α requires n applications to produce the identity mapping, then there are a total of n unique permutations generated by α. The notation for a group generated by *alpha* is typically $\langle\alpha\rangle$.

In the case of the dihedral group D_3, we can visualize the group generated

by a rotation of an equilateral triangle

$$\rho : (1,2,3) \to (2,3,1)$$
$$\rho^2 : (1,2,3) \to (3,1,2)$$
$$1 = \rho^3 : (1,2,3) \to (1,2,3).$$

This produces a cyclic group C_3 consisting of $\{1, \rho, \rho^2\}$ under composition of maps.

A.4.1 The Group $\langle Z_n, + \rangle$

For positive n, the quotient ring $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$ consisting of the n cosets of $\mathbb{Z}$ under addition modulo n is in fact a cyclic group. For all n we can consider the group $\langle \bar{1} \rangle$ where $\bar{1}$ denotes the coset containing all integers with a remainder of 1 when divided by n. It is obvious to see that adding $\bar{1}$ to itself n times results in the coset $\bar{0}$, the additive identity.

There is then a one–to–one correspondence between the cyclic group C_n and Z_n and we say that $C_n \cong Z_n$.

A.5 Other Groups G_n, F_n and Direct Products

Other groups in this thesis will typically be given the notation G_n or F_n. These groups typically have a more complex structure than the specific examples given above. In these cases the n denotes the number of distinct elements in the group. For example, G_{72} has 72 elements and we write $|G_{72}| = 72$.

Some of these groups can also be written using direct product notation $G \times H$. We can define elements in this direct of groups as an ordered pair

consisting of one element from the group G and one element from the group H. The operation between two of these pairs must then be defined as

$$(g, h)(g', h') = (g \cdot g', h * h')$$

where $g, g' \in G$, $h, h' \in H$ and $\cdot$ and $*$ are the binary operations defined in G and H, respectively. It is not necessary for the operations in G and H to be distinct.

Appendix B

Magma Code Related to Chapter 5

```
print "Initialization";
print "**********************************";
_<x>:=PolynomialRing(Rationals());
PS:=ProjectiveSpace(Rationals(),1);


print "";
print "Set up the number field";
print "**********************************";
K<t>:=NumberField(x^3+3*x+1);
OK:=MaximalOrder(K);
Basis(OK, NumberField(OK));
// [ 1, t, t^2 ]
ClassNumber(OK);
// 1
U,mU:=UnitGroup(OK); U;
// Abelian Group isomorphic to Z/2 + Z
// Defined on 2 generators
// Relations:
//     2*U.1 = 0
[mU(U.2)];
// [ [0, 1, 0] ]
```

```
[mU(U.1), mU(U.2)];
// [ [-1, 0, 0], [0, 1, 0] ]
e1:=t;
[Norm(e1)];
// [ -1 ]
p2:=Factorization(2*OK); p2;
// [ <Principal Prime Ideal of OK
//   Generator:
//       [2, 0, 0], 1> ]
p21:=p2[1][1];
p3:=Factorization(3*OK); p3;
// [ <Prime Ideal of OK
//   Two element generators:
//       [3, 0, 0]
//       [1, 1, 0], 3> ]
p31:=p3[1][1];
p5:=Factorization(5*OK); p5;
// [ <Prime Ideal of OK
//   Two element generators:
//       [5, 0, 0]
//       [3, 1, 0], 2>,
//   <Prime Ideal of OK
//   Two element generators:
//       [5, 0, 0]
//       [9, 1, 0], 1> ]
p51:=p5[1][1];
p52:=p5[2][1];
```

```
print "";
print "Set up the sextic";
print "**********************************";
_<X>:=PolynomialRing(K);
Factorization(X^6-3*X^4+51*X^2+15);
// [ <X^2 - 4*t - 1, 1>,
//   <X^2 + (-2*t^2 - 4)*X + 2*t^2 + 7, 1>,
//   <X^2 + (2*t^2 + 4)*X + 2*t^2 + 7, 1> ]

print "";
print "Local Solvability";
print "**********************************";
print "";
print "Testing the Quadratic";
print "**********************";
for i0 in [0..1] do
for i1 in [0..1] do
bool:=true;
C:=HyperellipticCurve(g*(X^4+2*(2*t-1)*X^2+(16*t^2-4*t+49)))
where g is (-1)^i0*t^i1;
bp:=BadPrimes(C);
print [i0,i1];
for i in [1..4] do
bool:=bool and IsLocallySolvable(C,bp[i]);
if not IsLocallySolvable(C,bp[i]) then
print "Fails at bad prime:";
```

```
print bp[i];
end if;
end for;
print bool;
print "";
end for; end for;
// [ 0, 0 ]
// true
//
// [ 0, 1 ]
// Fails at bad prime:
// Prime Ideal of OK
// Two element generators:
//     [3, 0, 0]
//     [1, 1, 0]
// false
//
// [ 1, 0 ]
// Fails at bad prime:
// Prime Ideal of OK
// Two element generators:
//     [3, 0, 0]
//     [1, 1, 0]
// false
//
// [ 1, 1 ]
// true
```

```
print "";
print "Testing the Quartic";
print "**********************";
for i0 in [0..1] do
for i1 in [0..1] do
bool:=true;
C:=HyperellipticCurve(g*(X^4+2*(2*t-1)*X^2+(16*t^2-4*t+49)))
where g is (-1)^i0*t^i1;
bp:=BadPrimes(C);
print [i0,i1];
for i in [1..4] do
bool:=bool and IsLocallySolvable(C,bp[i]);
if not IsLocallySolvable(C,bp[i]) then
print "Fails at bad prime:";
print bp[i];
end if;
end for;
print bool;
print "";
end for; end for;
// [ 0, 0 ]
// true
//
// [ 0, 1 ]
// Fails at bad prime:
// Prime Ideal of OK
```

```
// Two element generators:
//     [3, 0, 0]
//     [1, 1, 0]
// false
//
// [ 1, 0 ]
// Fails at bad prime:
// Prime Ideal of OK
// Two element generators:
//     [3, 0, 0]
//     [1, 1, 0]
// false
//
// [ 1, 1 ]
// true


print "";
print "Case g=1";
print "**********************";
C1:=HyperellipticCurve(X^4+2*(2*t-1)*X^2+(16*t^2-4*t+49));
E1, C1toE1 := EllipticCurve(C1);
boo,G1,m1:=PseudoMordellWeilGroup(E1);
boo;
// true
G1;
// Abelian Group isomorphic to Z/2 + Z/2 + Z
// Defined on 3 generators
```

```
// Relations:
//     2*G1.1 = 0
//     2*G1.2 = 0


print "";
print "Chabauty";
print "*************";
C1toPS:=map<C1->PS|[C1.1,C1.3]>;
E1toPS:=Expand(Inverse(C1toE1)*C1toPS);
N1,V1,R1,W1:=Chabauty(m1,E1toPS,17); N1;V1;
// 4
// { 0, G1.1 + G1.2, G1.2, G1.1 }
R1;
// 4
[EvaluateByPowerSeries(E1toPS,m1(v)): v in V1];
// [ (1 : 0), (0 : 1), (1 : 0), (0 : 1) ]


print "";
print "Case g=-t";
print "**********************";
C2:=HyperellipticCurve(-t*(X^4+2*(2*t-1)*X^2+(16*t^2-4*t+49)));
print "Find rational points:";
RationalPoints(C2: Bound := 10);
// {@ (-1 : -4 : 1), (1 : -4 : 1), (2*t^2 + 7 : 8*t^2 + 28 : 1),
//  (-2*t^2 - 7 : 8*t^2 + 28 : 1) @}
pt:=C2![2*t^2+7,8*t^2+28];
E2, C2toE2 := EllipticCurve(C2,pt);
```

```
boo,G2,m2:=PseudoMordellWeilGroup(E2);
boo;
// true
G2;
// Abelian Group isomorphic to Z/2 + Z/2 + Z
// Defined on 3 generators
// Relations:
//     2*G2.1 = 0
//     2*G2.2 = 0

print "";
print "Chabauty";
print "*************";
C2toPS:=map<C2->PS|[C2.1,C2.3]>;
E2toPS:=Expand(Inverse(C2toE2)*C2toPS);
N2,V2,R2,W2:=Chabauty(m2,E2toPS,17); N2;V2;
// 4
// { G2.2 - G2.3, G2.1 + G2.2 - G2.3, G2.1 + G2.2, G2.2 }
R2;
// 32
[EvaluateByPowerSeries(E2toPS,m2(v)): v in V2];
// [ (1 : 1), (-1 : 1), (-1 : 1), (1 : 1) ]
```

Appendix C

Magma Code Related to Chapter 6

```
print "Initialization";
print "**********************************";
clear;
_<x>:=PolynomialRing(Rationals());
PS:=ProjectiveSpace(Rationals(),1);

print "";
print "Set up the number field";
print "**********************************";
print "** Number field defined by K=Q(t) where t^3-15*t+20=0";
K<t>:=NumberField(x^3 - 15*x + 20);
OK:=MaximalOrder(K);
print "** Has basis:";
Basis(OK, NumberField(OK));
// [ 1, t, t^2 ]
print "** Class number is:";
ClassNumber(OK);
// 1
print "** Find unit group:";
U,mU:=UnitGroup(OK); U;
// Abelian Group isomorphic to Z/2 + Z + Z
```

```
// Defined on 3 generators
// Relations:
//     2*U.1 = 0
[-mU(U.-3), mU(U.-2)];
// [ [-59, 22, 8], [161, -21, -13] ]
e1:=-59 + 22*t + 8*t^2; e2:=161 - 21*t - 13*t^2;
print "** Two fundamental units are";
print [e1,e2];
// [ 8*t^2 + 22*t - 59,
//   -13*t^2 - 21*t + 161 ]
print "** and have norms:";
[Norm(e1),Norm(e2)];
// [ 1, 1 ]
print "** Ideal factorization of <2> in OK:";
p2:=Factorization(2*OK); p2;
// [ <Prime Ideal of OK
//  Two element generators:
//      [2, 0, 0]
//      [2, 1, 0], 1>,
//  <Prime Ideal of OK
//  Two element generators:
//      [2, 0, 0]
//      [1, 1, 0], 2> ]
p21:=p2[1][1];
p22:=p2[2][1];
print "** Ideal factorization of <3> in OK:";
p3:=Factorization(3*OK); p3;
```

```
// [ <Prime Ideal of OK
//  Two element generators:
//      [3, 0, 0]
//      [2, 1, 0], 3> ]
print "** Ideal factorization of <5> in OK:";
p5:=Factorization(5*OK); p5;
// [ <Prime Ideal of OK
//  Two element generators:
//      [5, 0, 0]
//      [0, 1, 0], 3> ]


print "";
print "Set up the sextic";
print "**********************************";
_<X>:=PolynomialRing(K);
print "** The sextic X^6 + 105*X^4 + 2400*X^2 - 19200 factors over K as:";
Factorization(X^6 + 105*X^4 + 2400*X^2 - 19200);
// [ <X^2 - 7*t^2 - 20*t + 105, 1>,
//   <X^4 + (7*t^2 + 20*t)*X^2 + 400*t^2 + 1120*t - 3200, 1> ]


print "";
print "Local Solvability";
print "**********************************";
print "";
print "Testing the Quadratic";
print "*********************";
print "** Test hyperelliptic curve g*(X^2 - 7*t^2 - 20*t + 105)";
```

```
print "** where g is (-1)^i0*e1^i1*e2^i2";
print "** [i0,i1,i2]";
i0:=0; i1:=0; i2:=0;
for i0 in [0..1] do
for i1 in [0..1] do
for i2 in [0..1] do
bool:=true;
C:=HyperellipticCurve(g*(X^2 - 7*t^2 - 20*t + 105))
where g is (-1)^i0*e1^i1*e2^i2;
bp:=BadPrimes(C);
print [i0,i1,i2];
for i in [1..2] do
bool:=bool and IsLocallySolvable(C,bp[i]);
if not IsLocallySolvable(C,bp[i]) then
print "Fails at bad prime:";
print bp[i];
end if;
end for;
print bool;
print "";
end for; end for; end for;
// [ 0, 0, 0 ]
// true
//
// [ 0, 0, 1 ]
// Fails at bad prime:
// Prime Ideal of OK
```

```
// Two element generators:
//     [2, 0, 0]
//     [1, 1, 0]
// false
//
// [ 0, 1, 0 ]
// true
//
// [ 0, 1, 1 ]
// Fails at bad prime:
// Prime Ideal of OK
// Two element generators:
//     [2, 0, 0]
//     [1, 1, 0]
// false
//
// [ 1, 0, 0 ]
// Fails at bad prime:
// Prime Ideal of OK
// Two element generators:
//     [2, 0, 0]
//     [2, 1, 0]
// false
//
// [ 1, 0, 1 ]
// Fails at bad prime:
// Prime Ideal of OK
```

```
// Two element generators:
//     [2, 0, 0]
//     [2, 1, 0]
// Fails at bad prime:
// Prime Ideal of OK
// Two element generators:
//     [2, 0, 0]
//     [1, 1, 0]
// false
//
// [ 1, 1, 0 ]
// Fails at bad prime:
// Prime Ideal of OK
// Two element generators:
//     [2, 0, 0]
//     [2, 1, 0]
// false
//
// [ 1, 1, 1 ]
// Fails at bad prime:
// Prime Ideal of OK
// Two element generators:
//     [2, 0, 0]
//     [2, 1, 0]
// Fails at bad prime:
// Prime Ideal of OK
// Two element generators:
```

```
//     [2, 0, 0]
//     [1, 1, 0]
// false

print "** This eliminates any cases where i0=1";

print "";
print "Testing the Quartic";
print "********************";
print "** Test hyperelliptic curve g*(X^4 + (7*t^2 + 20*t)*X^2 + 400*t^2
+ 1120*t - 3200)";
print "** where g is (-1)^i0*e1^i1*e2^i2";
print "** [i0,i1,i2]";
i0:=0;i1:=0;i2:=0;
for i0 in [0..0] do
for i1 in [0..1] do
for i2 in [0..1] do
bool:=true;
C:=HyperellipticCurve(g*(X^4 + (7*t^2 + 20*t)*X^2 + 400*t^2 + 1120*t - 3200))
where g is (-1)^i0*e1^i1*e2^i2;
bp:=BadPrimes(C);
print [i0,i1,i2];
for i in [1..#bp] do
bool:=bool and IsLocallySolvable(C,bp[i]);
if not IsLocallySolvable(C,bp[i]) then
print "Fails at bad prime:";
print bp[i];
```

```
end if;
end for;
print bool;
print "";
end for; end for; end for;
// [ 0, 0, 0 ]
// true
//
// [ 0, 0, 1 ]
// true
//
// [ 0, 1, 0 ]
// true
//
// [ 0, 1, 1 ]
// true

print "** Therefore g=1 or g=e1=8*t^2 + 22*t - 59";

print "";
print "Case g=1";
print "**********************";
C1:=HyperellipticCurve(X^4 + (7*t^2 + 20*t)*X^2 + 400*t^2 + 1120*t - 3200);
print "** Find rational points:";
RationalPoints(C1: Bound := 10);
// {@ (4 : 4*t^2 + 20*t - 16 : 1), (-4 : 4*t^2 + 20*t - 16 : 1), (1 : -1 : 0) @}
E1, C1toE1 := EllipticCurve(C1);
```

```
boo,G1,m1:=PseudoMordellWeilGroup(E1);
boo;
// false

print "** Try multiplying quartic by X^2 and substituting X=sqrt(X)
to get a cubic";
C1:=HyperellipticCurve(X^3+(7*t^2+20*t)*X^2+(400*t^2+1120*t-3200)*X);
print "** Find rational points:";
RationalPoints(C1: Bound := 10);
// {@ (0 : 0 : 1), (1 : 0 : 0) @}
E1, C1toE1 := EllipticCurve(C1);
boo,G1,m1:=PseudoMordellWeilGroup(E1);
boo;
// true
G1;
// Abelian Group isomorphic to Z/2 + Z
// Defined on 2 generators
// Relations:
//     2*G1.1 = 0
C1toPS:=map<C1->PS|[C1.1,C1.3]>;
E1toPS:=Expand(Inverse(C1toE1)*C1toPS);
N1,V1,R1,W1:=Chabauty(m1,E1toPS,17); N1;V1;
// 4
// { 0, 2*G1.2, G1.1, -2*G1.2 }
R1;
// 1
[EvaluateByPowerSeries(E1toPS,m1(v)): v in V1];
```

```
// [ (1 : 0), (16 : 1), (0 : 1), (16 : 1) ]


print "";
print "Case g=8*t^2 + 22*t - 59";
print "**********************";
C2:=HyperellipticCurve(e1*(X^4 + (7*t^2 + 20*t)*X^2 + 400*t^2
+ 1120*t - 3200));
print "** Find rational points:";
RationalPoints(C2: Bound := 10);
// {@ (0 : -48*t^2 - 140*t + 320 : 1) @}
pt:=C2![0,-48*t^2-140*t+320];
E2, C2toE2 := EllipticCurve(C2,pt);
boo,G2,m2:=PseudoMordellWeilGroup(E2);
boo;
// true
G2;
// Abelian Group isomorphic to Z/2 + Z
// Defined on 2 generators
// Relations:
//     2*G2.1 = 0
C2toPS:=map<C2->PS|[C2.1,C2.3]>;
E2toPS:=Expand(Inverse(C2toE2)*C2toPS);
N2,V2,R2,W2:=Chabauty(m2,E2toPS,17); N2;V2;
// 2
// { 0, G2.1 }
R2;
// 6
```

```
[EvaluateByPowerSeries(E2toPS,m2(v)): v in V2];
// [ (0 : 1), (0 : 1) ]
```