Intersective Polynomials and Their Construction

by

Paul David Lee

B.Sc., The University of British Columbia, 2009
M.Sc., The University of British Columbia, 2011

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

DOCTOR OF PHILOSOPHY

in

THE COLLEGE OF GRADUATE STUDIES

(Mathematics)

THE UNIVERSITY OF BRITISH COLUMBIA

(Okanagan)

September 2016

The undersigned certify that they have read, and recommend to the College of Graduate Studies for acceptance, a thesis entitled: Intersective Polynomials and Their Construction submitted by Paul David Lee in partial fulfilment of the requirements of the degree of Doctor of Philosophy

Dr. Blair Spearman - Science/Mathematics
Supervisor, Professor (please print name and faculty/school above the line)

Dr. Qiduan Yang - Science/Mathematics
Supervisory Committee Member, Professor (please print name and faculty/school above the line)

Dr. Javad Tavakoli - Science/Mathematics
Supervisory Committee Member, Professor (please print name and faculty/school above the line)

Dr. Paul Shipley - Science/Chemistry
University Examiner, Professor (please print name and faculty/school above the line)

Dr. Yang Zhang - Science/Mathematics - University of Manitoba
External Examiner, Professor (please print name and faculty/school above the line)

September 20, 2016
(Date Submitted to Grad Studies)

Additional Committee Members include:

(please print name and faculty/school above the line)

(please print name and faculty/school above the line)

Abstract

A monic polynomial with integer coefficients is called intersective if it has no root in the rational numbers, but has a root modulo m for all positive integers $m > 1$. Equivalently, the polynomial has a root in each p-adic field $\mathbb{Q}_p$. Using three different methods for forming these intersective polynomials, we produce an infinite family with Galois group A_4, an infinite family with Galois group D_5, and classify intersective polynomials with holomorph Galois group $\mathbb{Z}_{2^e} \rtimes \mathbb{Z}_{2^e}^*$.

Preface

This thesis is primarily based on the following papers:

Published:

1. P. D. Lee, B. K. Spearman, and Q. Yang. *A parametric family of intersective polynomials with galois group A_4.* Communications in Algebra, 43(5), 2015, 1784-1790.

Accepted:

2. P. D. Lee, B. K. Spearman, and Q. Yang. *Covering a semi-direct product and intersective polynomials.* Manuscripta Mathematica, 2015, 10.1007/s00229-015-0811-1.

Submitted:

3. P. D. Lee, B. K. Spearman, and Q. Yang. *Intersective polynomials and dihedral quintic trinomials.*

For each of these papers with multiple authors, each author contributed equally in terms of acquisition and analysis of data and preparation of papers for publishing purposes.

Table of Contents

List of Tables

List of Symbols

$\mathbb{Z}$	Set of integers
$\mathbb{Q}$	Set of rationals
$\mathbb{R}$	Set of real numbers
$\mathbb{C}$	Set of complex numbers
$\mathbb{Q}_p$	p-adic field for prime integer $p > 1$
$\mathbb{R}^*$	Set of non-zero real numbers
$\mathbb{Q}^*$	Set of non-zero rational numbers
$\mathbb{Q}^{*^2}$	Set of square-free rational numbers
$\mathbb{Z}_n$	Set of integers modulo n
$\mathbb{Q}(\alpha)$	Field extension of $\alpha \notin \mathbb{Q}$ over $\mathbb{Q}$
$\mathbb{Z}[x]$	Set of all polynomials in x with integer coefficients
$\mathbb{Q}[x]$	Set of all polynomials in x with rational coefficients
$K[x]$	Set of all polynomials in x with coefficients in any number field K
$D(\alpha)$	Discriminant of the algebraic number α
$D(f)$	Discriminant of a polynomial $f(x)$
$deg(f), \partial f$	Degree of a polynomial $f(x)$
O_K	Ring of integers of a number field, K
$U(O_K)$	Group of units of the ring of integers of a number field, K

Acknowledgements

I would like to thank my family and friends for their support and love, especially my parents. Without them, none of this would be possible.

I would also like to express my deepest gratitude to my supervisor, Dr. Blair Spearman, for his constant support and advice. Your patience, understanding, and ability to teach is one of my core inspirations for becoming a mathematician and teacher. I would also like to thank my co-supervisor Dr. Qiduan Yang for all his support and for instilling a broad knowledge of mathematics into me throughout my undergraduate and graduate work.

I would also like to thank all of my colleagues and professors from UBC Okanagan that have been such a great source of support and encouragement.

Chapter 1

Preliminaries

While the content in this preliminary chapter is well known in algebra and number theory, it should be noted that we have followed the content and structure contained within Alaca and Williams [AW04] and Fraleigh [Fra02] quite closely with minor notation and wording changes.

1.1 Basic Algebra

In this section, we present some fundamental theory in algebra that will serve as a precursor in knowledge for the rest of the thesis.

Definition 1.1. A group $(G, *)$ is a set G, together with a binary operation $*$, such that G satisfies the following:

- Closure: G is closed under the operation $*$, that is for all $a, b \in G$, $a * b \in G$.
- Associativity: For all a, b, and c in G, $(a * b) * c = a * (b * c)$.
- Identity element: There exists an element $e \in G$ such that for every element $a \in G$, the equation $e * a = a * e = a$ holds. Such an element is unique.
- Inverse element: For each $a \in G$, there exists an element $b \in G$ such that $a * b = b * a = e$ where e is the identity element.

When $a * b = b * a$ for all $a, b \in G$, then we call G an abelian group.

Definition 1.2. A subset H of a set G is called a subgroup of G if H forms a group under the operation $*$ of G.

Definition 1.3. A subgroup H of a group G is a normal subgroup if and only if $gH = Hg$ for all g in G.

Definition 1.4. Let $(G, *)$ and $(H, \star)$ be groups with binary operations $*$ and $\star$. A map $\phi : G \to H$ such that

$$\varphi(x * y) = \varphi(x) \star \varphi(y), \quad \text{for all } x, y \in G$$

is called a homomorphism. If the group operations of G and H are not written explicitly, we just write $\varphi(xy) = \varphi(x)\varphi(y)$.

Definition 1.5. The map $\varphi : G \to H$ is called an isomorphism and G and H are said to be isomorphic if the two following hold:

1. φ is a homomorphism and
2. φ is a bijection (both onto and one-to-one).

Definition 1.6. Let G be a group. An isomorphism from G onto itself is called an automorphism of G. The set of all automorphisms of G is denoted by $\mathrm{Aut}(G)$.

Definition 1.7. Let H and K be groups and let φ be a homomorphism from K into $\mathrm{Aut}(H)$. The semidirect product of H by K via φ is the set of ordered pairs $\{(h, k) \mid h \in H, k \in K\}$, together with the binary operation defined by

$$(h_1, k_1)(h_2, k_2) = (h_1 \varphi_{k_1}(h_2), k_1 k_2).$$

We write $H \rtimes_\varphi K$ for the semidirect product of H and K.

Definition 1.8. A ring is a set R equipped with binary operations $+$ and $\cdot$ (addition and multiplication) that satisfies the following three sets of axioms:

- R is an abelian group under addition.
- Multiplication in R is associative.
- Multiplication in R is distributive with respect to addition, i.e. $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(b + c) \cdot a = b \cdot a + c \cdot a$.

If multiplication is also commutative, then R is a "commutative ring". If R has a multiplicative identity, 1, then we say that R is a "ring with 1".

If all of the above holds true, then we call R a "commutative ring with 1".

Definition 1.9. An element a of a ring R is called a zero divisor if there exists a nonzero element x such that $ax = xa = 0$.

Example 1.10. Consider the ring of elements modulo 6. The elements 2 and 3 are zero divisors since $2 \cdot 3 = 3 \cdot 2 = 0$.

Definition 1.11. An integral domain D is a commutative ring that has a multiplicative identity but no zero divisors.

Example 1.12. The set of all integers $\mathbb{Z}$ is an integral domain.

Definition 1.13. A field is an integral domain where for each $a \in D, a \neq 0$, there exists a $b \in D$ such that $ab = 1$. That is, all elements in D have a multiplicative inverse.

Definition 1.14. Let D be an integral domain. Then there exists a field F, called the field of quotients of D (or the quotient field of D) that contains an isomorphic copy D' of D. That is, the quotient field of D is the smallest field containing D as a subring.

Definition 1.15. An integral domain D is said to be integrally closed if the only elements of its quotient field that are integral over D are those of D itself.

Definition 1.16. An element a of an integral domain D is called a unit if $a \mid 1$, that is $1 = ad$ for some $d \in D$. The set of units of D is denoted by $U(D)$.

Theorem 1.17. *The set of units $U(D)$ of an integral domain D forms an Abelian group with respect to multiplication.*

Definition 1.18. A nonzero, nonunit element a of an integral domain D is called an irreducible if $a = bc$, where $b, c \in D$ implies that either b or c is a unit.

Definition 1.19. A nonzero, nonunit element p of an integral domain D is called a prime if $p \mid ab$, where $a, b \in D$, implies that either $p \mid a$ or $p \mid b$.

Theorem 1.20. *In any integral domain D a prime is irreducible.*

1.2 Ideals

Definition 1.21. An ideal I of an integral domain D is a nonempty subset D having the following two properties:

- $a \in I, b \in I \Rightarrow a + b \in I$
- $a \in I, r \in D \Rightarrow ra \in I$

The following are some properties of ideals:

- If $a_1, \ldots, a_n \in I$, then so are all r-linear combinations of these a_i. That is, for all $r_1, \ldots, r_n \in D$, $r_1a_1 + \cdots + r_na_n \in I$.
- If $a \in I$ and $b \in I$, then $-a \in I$ and $a - b \in I$.
- $0 \in I$, and if $1 \in I$ then $I = D$ for an integral domain D.

Example 1.22. If $\{a_1, \ldots, a_n\}$ is a set of elements of an integral domain D, then the set of all finite linear combinations of $a_1, \ldots, a_n$

$$\left\{ \sum_{i=1}^{n} r_i a_i \mid r_1, \ldots, r_n \in D \right\}$$

is an ideal of D, which we denote by $\langle a_1, \ldots, a_n \rangle$.

Definition 1.23. An ideal I of an integral domain D is called a principal ideal if there exists an element $a \in I$ such that $I = \langle a \rangle = \{ra \mid r \in D\}$. The element a is called a generator of the ideal I. The princpal ideal $\langle 0 \rangle$ is just the set $\{0\}$ and the ideal $\langle 1 \rangle$ is all of D.

Definition 1.24. An ideal I of an integral domain D is called a proper ideal of D if $I \neq \langle 0 \rangle, \langle 1 \rangle$.

Definition 1.25. A proper ideal P of an integral domain D is called a prime ideal if

$$a, b \in D \text{ and } ab \in P \text{ implies } a \in P \text{ or } b \in P.$$

Theorem 1.26. *Let D be an integral domain. Let $a \in D$ be such that $a \neq 0$ and $a \notin U(D)$. Then*

$$\langle a \rangle \textit{ is a prime ideal of } D \iff a \textit{ is prime in } D.$$

Definition 1.27. A proper ideal M of an integral domain D is called a maximal idea if whenever I is an ideal of D such that $M \subseteq I \subseteq D$ implies that either $I = M$ or $I = D$.

1.3 Dedekind Domains

Still building structure on top of integral domains, we will define a Dedekind domain, which has important structure for our algebraic number theory, namely with respect to the ring of integers of an algebraic number field.

Definition 1.28. An infinite sequence of ideals $\{I_n : n = 1, 2, \ldots\}$ in an integral domain D is said to be an ascending chain if

$$I_1 \subseteq I_2 \subseteq \ldots \subseteq I_n \subseteq \ldots$$

The chain is said to be a strictly ascending chain if

$$I_1 \subset I_2 \subset \ldots \subset I_n \subset \ldots$$

Definition 1.29. We say that an integral domain satisfies the ascending chain condition (ACC) if there exists a positive integer r such that $I_r = I_s$ for all $s \geq r$.

Definition 1.30. An integral domain that satisfies the ascending chain condition above is called a Noetherian domain. More generally, a Noetherian

ring is a ring R in which every ascending chain of (two-sided) ideals in R terminates.

Definition 1.31. An integral domain D that satisifies the following three properties:

- D is a Noetherian domain,
- D is integrally closed, and
- each prime ideal of D is a maximal ideal,

is called a Dedekind domain.

1.4 Field and Galois Theory

1.4.1 Field Theory

We introduce some basic field theory that will allow us to define field extensions and introduce some Galois theory. We have defined a field in the previous section, but for clarity, we will present the definition of a field with all of its core axioms:

Definition 1.32. F is a field if all of the following hold:

1. F is closed under addition.
2. Addition and multiplication are commutative and associative in F.
3. F contains an additive and multiplicative identity (usually denoted as 0 and 1) that are unique.
4. Every element a in F has an additive inverse (denoted by $-a$) and every nonzero element a in F has a multiplicative inverse (denoted by a^{-1}).
5. For every $a \in F$, $a0 = 0a = 0$.
6. Addition and multiplication are distributive, that is for every $a, b, c \in F$, $(a + b)c = ab + bc$ and $c(a + b) = ca + ba$.

Definition 1.33. The characteristic $\text{char}(F)$ of the field F is the smallest positive integer n such that $n \cdot 1 = 0 \in F$, or 0 if no such n exists.

Lemma 1.34. *Let F be a field. Then char(F) is either 0 or a prime.*

Definition 1.35. If a subset E of the elements of a field F satisfies the field axioms with the same operations of F, then E is called a subfield of F. In a finite field of order p^n, where p is a prime, there exists a subfield of order p^m for every m dividing n.

Definition 1.36. A field E is an extension of the field F if F is a subfield of E. We denote this as E/F.

Definition 1.37. Let E be a field extension of F. Then $\alpha \in E$ is algebraic over F if α is a root of some polynomial $f(x)$ that has coefficients in F.

Definition 1.38. We say that E is an algebraic extension of F (or E/F is algebraic) if every $\alpha \in E$ is algebraic over F.

Lemma 1.39. *The following are equivalent:*

1. *α is algebraic over F.*
2. *$F(\alpha)/F$ is finite.*
3. *$F(\alpha) = \{$polynomials in α with coefficients in $F\}$.*
4. *α is in B for some finite extension B of F.*

1.4.2 Field Extensions as Vector Spaces

Definition 1.40. Let L/K be a field extension, and suppose that $\alpha \in L$ is algebraic over K. Then the minimial polynomial of α over K is the unique monic polynomial f over K of smallest degree such that $f(\alpha) = 0$.

A very useful consequence of forming a field extension over a field K is that with certain operations, the extension forms a vector space over K. This allows us to associate the dimension of the vector space over the field K with the minimial polynomial of the $\alpha \in L$ of the extension.

Theorem 1.41. *If L/K is a field extension, then the operations*

$$(\lambda, u) \mapsto \lambda u \qquad (\lambda \in K, u \in L)$$
$$(u, v) \mapsto u + v \qquad (u, v \in L)$$

define on L the structure of a vector space over K.

Definition 1.42. The degree $[L : K]$ of a field extension L/K is the dimension of L considered as a vector space over K.

Theorem 1.43. *If $K_0 \subset K_1 \subset \cdots \subset K_n$ are subfields of $\mathbb{C}$ with $[K_n : K_0] < \infty$, then*

$$[K_n : K_0] = [K_n : K_{n-1}][K_{n-1} : K_{n-2}] \cdots [K_1 : K_0]$$

Proposition 1.44. *Let $K(\alpha)/K$ be a simple extension and let f be the minimal polynomial of α over K. If the extension is algebraic, then $[K(\alpha) : K] = \delta f$ where δf is the polynomial degree of f.*

1.4.3 The Group of Permutations of a Polynomial

Now that we have talked about field extensions, we introduce the concept of the group of permutations of the roots of a given polynomial. We use an example to illustrate this idea.

Consider the polynomial $f(t) = t^4 - 4t^2 - 5$ which factorizes as

$$f(t) = (t^2 + 1)(t^2 - 5).$$

From this, we can see that $f(t)$ has four roots: $t = \pm i, \pm\sqrt{5}$, where i and $-i$ are conjugates and $\sqrt{5}$ and $-\sqrt{5}$ are conjugates. We let

$$\alpha = i, \qquad \beta = -i, \qquad \gamma = \sqrt{5}, \qquad \delta = -\sqrt{5}.$$

If we now consider a set of polynomial equations that satisfy the above four roots, we can find valid algebraic equations that may either stay valid, or become invalid, depending on how we interchange the roots. A set of

equations for which the above are satisfied are stated next. Note that there are infinitely many such equations.

$$\alpha^2 + 1 = 0 \qquad \alpha + \beta = 0 \qquad \delta^2 - 5 = 0 \qquad \gamma + \delta = 0 \qquad \alpha\gamma - \beta\delta = 0$$

The next step is to decide which roots we can interchange. For example, if we interchange α and γ, we obtain the equation $\gamma^2 + 1 = 0$, which is false. We can interchange α to β only and keep γ, δ fixed, interchange γ to δ only and keep α, β fixed, interchange both at once, or don't interchange them at all. This gives us four possible permutations of the roots of $f(t)$:

$$\begin{aligned} I &= (1) \\ R &= (\alpha\beta) \\ S &= (\gamma\delta) \\ T &= (\alpha\beta)(\gamma\delta) \end{aligned}$$

These four permutations form a subgroup of S_4, namely the Klein-4 group $C_2 \times C_2$ as all non-identity elements have order 2.

1.4.4 Normality, Separability, and the Galois Correspondence

Definition 1.45. If K is a subfield of $\mathbb{C}$ and f is a polynomial over K, then f splits over K if it can be expressed as a product of linear factors

$$f(t) = k(t - \alpha_1) \cdots (t - \alpha_n)$$

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

Definition 1.46. Let $K \subseteq \mathbb{C}$ be a field. A subfield Σ of $\mathbb{C}$ is a splitting field for the polynomial f over the subfield K of $\mathbb{C}$ if $K \subset \Sigma$ and

1. f splits over Σ.
2. If $K \subset \Sigma' \subset \Sigma$ and f splits over Σ', then $\Sigma' = \Sigma$.

3. $\Sigma = K(\sigma_1, \ldots, \sigma_n)$ where $\sigma_1, \ldots \sigma_n$ are the zeros of f in Σ.

Definition 1.47. A field extension L/K is normal if every irreducible polynomial f over K that has at least one zero in L splits in L.

Definition 1.48. Let L be a finite extension of K. A normal closure of L/K is an extension N of L such that

1. N/K is normal.

2. If $L \subseteq M \subseteq N$ and M/K is normal, then $M = N$.

Thus N is the smallest extension of L that is normal over K.

Normality is important as non-normal extensions have Galois groups that don't behave in a straight-forward way. Normal extensions have a Galois correspondence that is a bijection.

Theorem 1.49. *A field extension L/K is normal and finite if and only if L is a splitting field for some polynomial over K.*

Definition 1.50. An algebraic field extension L/K that is normal and separable is called a Galois extension of L over K; or equivalently, L/K is algebraic and the field fixed by the automorphism group $Aut(L/K)$ is precisely the base field K.

Definition 1.51. An irreducible polynomial f over a subfield K of $\mathbb{C}$ is separable over K if it has simple zeros in $\mathbb{C}$, or equivalently, simple zeros in its splitting field.

Proposition 1.52. *If K is a subfield of $\mathbb{C}$, then every irreducible polynomial over K is separable.*

The connection between field theory and group theory made by Galois allows us to describe how the roots of a polynomial equation are related to each other. For a given polynomial with roots over $\mathbb{Q}$, we want to find the Galois group that contains the permutations of that root within that field. The Fundamental Theorem of Galois Theory provides the link between these two ideas.

Theorem 1.53. *Let E be a finite extension of a field F, $G = Gal(E/F)$, and $G_B = \{g \in G \mid g(b) = b \ \forall b \in B\}$.*

1. *There is a one-to-one correspondence between intermediate fields $E \supseteq B \supseteq F$ and subgroups $\{1\} \subseteq G_B \subseteq G$ given by*

$$B = Fix(G_B)$$

   where $Fix(G_B)$ is the fixed field of G_B, that is the set of all elements $x \in E$ such that x is fixed under the permutations $\alpha \in B$.

2. *B is a normal extension of F if and only if G_B is a normal subgroup of G. This is the case if and only if B is a Galois extension of F. In this case*

$$Gal(B/F) \simeq G/G_B$$

3. *For each $E \supseteq B \supseteq F$, $[B : F] = [G : G_B]$ and $[E : B] = |G_B|$*

The inverse Galois problem poses another interesting question: given a finite group G, is it possible to find a polynomial of specified degree over $\mathbb{Q}$ whose Galois group is G? Moreover, can we find an infinite family of these polynomials?

We are interested in finite groups and want to find parametric families of polynomials that have a prescribed Galois group. A partial existence result is the following theorem.

Theorem 1.54. *Every finite abelian group is the Galois group of a Galois extension E of $\mathbb{Q}$.*

The possible Galois groups of irreducible polynomials of degrees from 2 to 5 are listed in a table below:

We can approach this table two ways:

1. Given a polynomial of say degree 4, there are only five possible Galois groups that this polynomial can belong to, or

2. Given a particular Galois group, say A_4, we know that an irreducible polynomial with this Galois group must be a quartic.

Table 1.1: Possible Galois groups for polynomials from degree 2 to 5

Quadratic	**Cubic**	**Quartic**	**Quintic**
C_2	C_3	C_4	C_5
	S_3	S_4	S_5
		A_4	A_5
		D_4	D_5
		$V = C_2 \times C_2$	F_{20}

1.5 Algebraic Number Theory

In this section, we provide a brief overview of the necessary algebraic number theory used in the rest of the thesis.

Definition 1.55. An algebraic number is an element $\alpha \in \mathbb{C}$ that is a root of a monic polynomial with coefficients in $\mathbb{Q}$. That is, α is a root of a polynomial

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

where $a_i \in \mathbb{Q},\ i = 1, 2, \ldots, n-1$.

Definition 1.56. An algebraic integer is an element $\beta \in \mathbb{C}$ that is a root of a monic polynomial with coefficients in $\mathbb{Z}$. That is, β is a root of the polynomial

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

where $a_i \in \mathbb{Z},\ i = 1, 2, \ldots, n-1$.

Example 1.57. The element $\frac{\sqrt{2}}{2}$ is an algebraic number because it is a root of the monic polynomial $x^2 - \frac{1}{2} \in \mathbb{Q}[x]$.

Example 1.58. The element $\sqrt{2}$ is an algebraic integer because it is a root of the monic polynomial $x^2 - 2 \in \mathbb{Z}[x]$.

Example 1.59. The element $\sqrt{2} + \sqrt{3}$ is an algebraic integer because it is a root of the monic polynomial $x^4 - 10x^2 + 1 \in \mathbb{Z}[x]$.

In general, any algebraic number is a root of infinitely many polynomials in $\mathbb{Q}[x]$. For example, $\sqrt{2}$ is also a root of the monic polynomials $x^3 - 2x, x^3 -$

$x^2 - 2x + 2, x^5 - 2x^4 - 7x^3 + 10x^2 + 10x - 12$, etc. We want to work with the polynomial of least degree with the algebraic integer/number as a root. This leads us into the following definition:

Definition 1.60. Let K be a subfield of $\mathbb{C}$. Let $\alpha \in \mathbb{C}$ be algebraic over K. Then the monic polynomial $f(x) \in K[x]$ such that $f(\alpha) = 0$ with least degree is the minimal polynomial of α over K.

The minimal polynomial defined above is unique and also irreducible, which we will restate from Definition 1.18 in the specific case of polynomial irreducibility.

Definition 1.61. A polynomial $f(x) \in K[x]$ is called irreducible over K if $deg(f) > 0$ and it cannot be factored into the product of two non-constant polynomials over $K[x]$. That is, if $f(x) = g(x)h(x)$ for polynomials $g(x), h(x) \in K[x]$ then either $g(x)$ or $h(x)$ is a unit in $K[x]$. Otherwise, $f(x)$ is reducible over $K[x]$.

Definition 1.62. Let K be a subfield of $\mathbb{C}$. Let $\alpha \in \mathbb{C}$ be algebraic over K. Then the degree of α over K, written $\deg_K(\alpha)$, is defined by

$$\deg_K(\alpha) = \deg(\mathrm{irr}_K(\alpha)),$$

where $\mathrm{irr}_K(\alpha)$ is the irreducible, minimal polynomial of α over K. If $K = \mathbb{Q}$, we drop the subscript K and write $deg_{\mathbb{Q}}(\alpha) = deg(\alpha)$.

1.5.1 Field Extensions and Algebraic Number Fields

Definition 1.63. Let $\alpha \in \mathbb{C}$ be algebraic over K. We define $K(\alpha)$ to be the intersection of the subfields of $\mathbb{C}$ containing K and α. We say that $K(\alpha)$ is formed from K by adjoining α.

Definition 1.64. A subfield L of $\mathbb{C}$ for which there exists $\alpha \in \mathbb{C}$ such that $L = K(\alpha)$ is called a simple extension of K.

Theorem 1.65. *Let K be a subfield of $\mathbb{C}$. Let $\alpha \in \mathbb{C}$ be algebraic over K. Let $n = \deg(\mathrm{irr}_K(\alpha))$. Then*

$$K(\alpha) = \{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \mid a_0, \ldots, a_{n-1} \in K\}.$$

This allows us to view $K(\alpha)$ as an n-dimensional vector space over K with basis $\{1, \alpha, \ldots, \alpha^{n-1}\}$.

Definition 1.66. Let K be a subfield of $\mathbb{C}$. Let $\alpha \in \mathbb{C}$ be algebraic over K of degree n (so that $n = \deg_K(\alpha) = \deg(\mathrm{irr}_K(\alpha))$). The degree of the extension $K(\alpha)$ over K, written $[K(\alpha) : K]$, is defined by

$$[K(\alpha) : K] = n.$$

In the same fashion, let $\alpha_1, \ldots, \alpha_k \in \mathbb{C}$ be algebraic over K and define $K(\alpha_1, \ldots, \alpha_k)$ to be the smallest field containing K and the $\alpha_1, \ldots, \alpha_k$. Remarkably, fields constructed in this fashion are always simple extensions as the next theorem illustrates:

Theorem 1.67 (Primitive Element Theorem)**.** *Let K be a subfield of $\mathbb{C}$. Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be algebraic over K. Then there exists $\alpha \in \mathbb{C}$ that is algebraic over K such that*

$$K(\alpha_1, \alpha_2, \ldots, \alpha_n) = K(\alpha).$$

We now look at algebraic number fields, which are formed by adjoining field elements onto a base field, usually $\mathbb{Q}$.

Definition 1.68. An algebraic number field is a subfield of $\mathbb{C}$ of the form $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ where $\alpha_1, \ldots, \alpha_n$ are algebraic numbers.

By Theorem 1.67, an algebraic number field can always be obtained by adjoining a single algebraic number θ to $\mathbb{Q}$. The following theorem gives the representation of the elements of an algebraic number field $\mathbb{Q}(\theta)$.

Theorem 1.69. *Let $K = \mathbb{Q}(\theta)$ be an algebraic number field, where θ is an algebraic number. Let the degree of the polynomial* $\mathrm{irr}_{\mathbb{Q}}(\theta)$ *be n. Then every*

element of K is expressible uniquely in the form

$$c_0 + c_1\theta + \cdots + c_{n-1}\theta^{n-1},$$

where $c_0, \ldots, c_{n-1} \in \mathbb{Q}$, and every such quantity $c_0 + c_1\theta + \cdots + c_{n-1}\theta^{n-1}$ ($c_0, \ldots, c_{n-1} \in \mathbb{Q}$) belongs to K.

We now formally introduce a concept touched upon in the last section, the integers that lie inside a number field K. This set will be very important in the theory of algebraic numbers.

Definition 1.70. Let Ω be the set of all algebraic integers. The set of all algebraic integers that lie in the algebraic number field K is denoted by O_K; that is,

$$O_K = \Omega \cap K.$$

We call O_K the ring of integers of the algebraic number field K.

Theorem 1.71. *Let K be an algebraic number field. Then O_K is an integral domain.*

1.5.2 Conjugates and Conjugate Fields of an Algebraic Number Field

In this section, we will discuss conjugates of a number field K that will be necessary for our later chapters.

Consider the element $\alpha \in K$ and let $f(x) \in \mathbb{Q}[x]$ be the minimal polynomial of α of degree n where $\alpha_1, \alpha_2, \ldots \alpha_n$ are the complex roots of f. For each $k = 1, \ldots, n$, the map $\sigma_k : \alpha \mapsto \alpha_k$ induces a field homomorphism

$$\sigma_k : \mathbb{Q}(\alpha) \longrightarrow \mathbb{Q}(\alpha_k) \subset \mathbb{C}.$$

This map above is well-defined and we call the maps $\sigma_1, \ldots \sigma_n$ the distinct field embeddings $K \to \mathbb{C}$.

Definition 1.72. Let $\alpha \in \mathbb{C}$ be algebraic over a subfield K of $\mathbb{C}$. The conjugates of α over K are the roots in $\mathbb{C}$ of $\mathrm{irr}_K(\alpha)$.

Example 1.73. Consider the element $\alpha = \dfrac{1+i}{\sqrt{2}}$. The minimal polynomial of α is $f(x) = x^4 + 1$.

Since

$$x^4+1 = \left(x - \left(\frac{1+i}{\sqrt{2}}\right)\right)\left(x - \left(\frac{1-i}{\sqrt{2}}\right)\right)\left(x + \left(\frac{1+i}{\sqrt{2}}\right)\right)\left(x + \left(\frac{1-i}{\sqrt{2}}\right)\right),$$

the conjugates of $(1+i)/\sqrt{2}$ over $\mathbb{Q}$ are

$$\frac{1+i}{\sqrt{2}}, \frac{1-i}{\sqrt{2}}, \frac{-1-i}{\sqrt{2}}, \frac{-1+i}{\sqrt{2}}.$$

Theorem 1.74. *If α is an algebraic integer then its conjugates over $\mathbb{Q}$ are also algebraic integers.*

Theorem 1.75. *If α is an algebraic integer then* $\mathrm{irr}_{\mathbb{Q}}(\alpha) \in \mathbb{Z}[x]$.

Theorem 1.76. *Let K be an algebraic number field of degree n over $\mathbb{Q}$. Then there are exactly n distinct field monomorphisms $\sigma_k : K \to \mathbb{C}$ $(k = 1, \ldots, n)$.*

Definition 1.77 (**Conjugate fields of an algebraic number field**)**.** Let K be an algebraic number field. Let θ be an algebraic number such that $K = \mathbb{Q}(\theta)$. Let

$$\theta_1 = \theta, \theta_2, \ldots, \theta_n$$

be the conjugates of θ over $\mathbb{Q}$. Then the fields

$$\mathbb{Q}(\theta_1) = \mathbb{Q}(\theta) = K, \mathbb{Q}(\theta_2), \ldots, \mathbb{Q}(\theta_n)$$

are called the conjugate fields of K.

Let K be an algebraic number field of degree n over $\mathbb{Q}$. Let $\theta \in K$ be such that $K = \mathbb{Q}(\theta)$ and let $\theta_1 = \theta, \theta_2, \ldots, \theta_n$ be the conjugates of θ over $\mathbb{Q}$. Recall Theorem 1.69 that states for α in K there exist unique rational numbers $c_0, c_1, \ldots, c_{n-1}$ such that

$$\alpha = c_0 + c_1\theta + \cdots + c_{n-1}\theta^{n-1}.$$

For $k = 1, 2, \ldots, n$ set

$$\alpha_k = c_0 + c_1\theta_k + \cdots + c_{n-1}\theta_k^{n-1} \in \mathbb{Q}(\theta_k).$$

Definition 1.78. The K-conjugates of α, or the complete set of conjugates of α relative to K, are the set of algebraic numbers $\{\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_n\}$.

The K-conjugates of the algebraic number α are actually the roots of $irr(\alpha)$, the minimal polynomial of α over K.

Definition 1.79. Let K be an algebraic number field of degree n. Let $\alpha \in K$. Let $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_n$ be the K-conjugates of α. Then the field polynomial of α over K is the polynomial

$$\mathrm{fld}_K(\alpha) = \prod_{k=1}^{n}(x - \alpha_k).$$

Theorem 1.80. *Let K be an algebraic number field of degree n. Let $\alpha \in K$. Then*

$$\mathrm{fld}_K(\alpha) \in \mathbb{Q}[x].$$

Definition 1.81. Let $K = \mathbb{Q}(\theta)$ be an algebraic number field of degree n. Let $\theta_1 = \theta, \theta_2, \ldots, \theta_n$ be the conjugates of θ over $\mathbb{Q}$. If $\mathbb{Q}(\theta_1) = \mathbb{Q}(\theta_2) = \cdots = \mathbb{Q}(\theta_n) = K$, the field K is said to be a normal or Galois extension of $\mathbb{Q}$.

If all the roots of the minimal polynomial of θ are in K, then K is a normal extension over $\mathbb{Q}$.

Example 1.82. Let $K = \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$. The conjugates of $\sqrt{2} + \sqrt{3}$ are $\pm\sqrt{2} \pm \sqrt{3}$ and the conjugate fields of K all coincide with K as

$$\mathbb{Q}(\pm\sqrt{2} \pm \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3}) = K.$$

Thus K is a normal extension.

Example 1.83. Let $K = \mathbb{Q}(\sqrt[3]{2})$ so that $K \subseteq \mathbb{R}$. The conjugates of $\sqrt[3]{2}$ are

$$\sqrt[3]{2},\ \omega\sqrt[3]{2},\ \omega^2\sqrt[3]{2},$$

where $\omega = exp(2\pi i/3)$ and $\omega^2 = exp(4\pi i/3)$ are the two complex cube roots of unity, since

$$\mathrm{irr}_{\mathbb{Q}}(\sqrt[3]{2}) = x^3 - 2 = (x - \sqrt[3]{2})(x - \omega\sqrt[3]{2})(x - \omega^2\sqrt[3]{2}).$$

The conjugate fields of K are

$$K_1 = \mathbb{Q}(\sqrt[3]{2}) = K,\ K_2 = \mathbb{Q}(\omega\sqrt[3]{2}),\ K_3 = \mathbb{Q}(\omega^2\sqrt[3]{2}).$$

We want to show that the conjugate fields are distinct, showing that $\mathbb{Q}(\sqrt[3]{2})$ is not a normal extension. Clearly as K_1 is a real field and K_2 and K_3 are not, we have $K_1 \neq K_2$ and $K_1 \neq K_3$. Therefore it remains to show that $K_2 \neq K_3$.

By way of contradiction, assume $K_2 = K_3$. Then $\omega^2\sqrt[3]{2} \in K_2$. This implies that there exist $a, b, c \in \mathbb{Q}$ such that

$$\omega^2\sqrt[3]{2} = a + b\omega\sqrt[3]{2} + c(\omega\sqrt[3]{2})^2.$$

Taking complex conjugates we obtain

$$\omega\sqrt[3]{2} = a + b\omega^2\sqrt[3]{2} + c\omega(\sqrt[3]{2})^2$$

since $\bar{\omega} = \omega^2$. Subtracting the second equation from the first equation above,

$$(\omega^2 - \omega)\sqrt[3]{2} = -b(\omega^2 - \omega)\sqrt[3]{2} + c(\omega^2 - \omega)(\sqrt[3]{2})^2,$$

so that

$$\sqrt[3]{2} = -b\sqrt[3]{2} + c(\sqrt[3]{2})^2.$$

Cancelling $\sqrt[3]{2}$ from this equation, we get

$$1 + b = c\sqrt[3]{2}.$$

But since $\sqrt[3]{2} \notin \mathbb{Q}$, we must have $1 + b = c = 0$ so

$$\omega^2 \sqrt[3]{2} = a - \omega \sqrt[3]{2}.$$

Thus

$$(\omega^2 + \omega) \sqrt[3]{2} = a$$

and since $\omega^2 + \omega = -1$,

$$\sqrt[3]{2} = -a \in \mathbb{Q},$$

which is a contradiction. Therefore all the conjugate fields of $\mathbb{Q}(\sqrt[3]{2})$ are distinct, and $\mathbb{Q}(\sqrt[3]{2})$ is not a normal field.

1.5.3 Discriminants

Definition 1.84. Let K be an algebraic number field of degree n. Let $\omega_1, \ldots, \omega_n$ be n elements of the field K. Let σ_k $(k = 1, 2, \ldots, n)$ denote the n distinct monomorphisms: $K \to \mathbb{C}$. For $i = 1, 2, \ldots, n$ let

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

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

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

In a similar fashion, we define the discriminant of a single element α of K as follows:

Definition 1.85. Let K be an algebraic number field of degree n. Let $\alpha \in K$. Then we define the discriminant of α by

$$D(\alpha) = D(1, \alpha, \alpha^2, \ldots, \alpha^{n-1}).$$

Theorem 1.86. *Let K be an algebraic number field of degree n. Let $\alpha \in K$.*

Then

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

where $\alpha^{(1)} = \alpha, \alpha^{(2)}, \ldots, \alpha^{(n)}$ *are the conjugates of* α *with respect to* K*. The discriminant above is actually the determinant of a Vandermonde matrix.*

We now give some theory that links the discriminant of a polynomial with the discriminant of an element α of an algebraic number field K.

Definition 1.87 (Discriminant of a polynomial)**.** Let

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

where $n \in \mathbb{N}$ and $a_n \neq 0$. Let $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ be the roots of $f(x)$. The discriminant of $f(x)$ is the quantity

$$\operatorname{disc}(f(x)) = a_n^{2n-2} \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2 \in \mathbb{C}.$$

Theorem 1.88. *Let* K *be an algebraic number field of degree* n*. Let* $\alpha \in K$*. Then*

$$D(\alpha) = \operatorname{disc}(\operatorname{fld}_K(\alpha)).$$

Theorem 1.89. *Let* K *be an algebraic number field of degree* n*. Let* $\alpha \in K$*. Then*

$$K = \mathbb{Q}(\alpha) \text{ if and only if } D(\alpha) \neq 0.$$

Theorem 1.90. *Let* K *be an algebraic number field of degree* n*.*

1. *If* $\omega_1, \ldots, \omega_n \in K$ *then*

$$D(\omega_1, \ldots, \omega_n) \in \mathbb{Q}.$$

2. *If* $\omega_1, \ldots, \omega_n \in O_K$ *then*

$$D(\omega_1, \ldots, \omega_n) \in \mathbb{Z}.$$

3. *If* $\omega_1, \ldots, \omega_n \in K$ *then*

   $D(\omega_1, \ldots, \omega_n) \neq 0$ *if and only if* $\omega_1, \ldots, \omega_n$ *are linearly independent over* $\mathbb{Q}$.

1.5.4 Ideals in Algebraic Number Theory

Theorem 1.91. *Let* K *be an algebraic number field of degree* n*. Let* I *be a nonzero ideal in* O_K*. Then there exist* $\eta_1, \ldots, \eta_n \in I$ *such that*

$$D(\eta_1, \ldots, \eta_n) \neq 0.$$

Theorem 1.92. *Let* K *be an algebraic number field of degree* n*. Let* I *be a nonzero ideal of* O_K*. There there exist elements* $\eta_1, \ldots, \eta_n$ *of* I *such that every element* α *of* I *can be expressed uniquely in the form*

$$\alpha = x_1\eta_1 + \cdots + x_n\eta_n,$$

where $x_1, \ldots, x_n \in \mathbb{Z}$.

Theorem 1.93. *Let* K *be an algebraic number field. Then* O_K *is a Noetherian domain.*

Definition 1.94 (Basis of an ideal)**.** Let K be an algebraic number field of degree n. Let I be a nonzero ideal of O_K. If $\{\eta_1, \ldots, \eta_n\}$ is a set of elements of I such that every element $\alpha \in I$ can be expressed uniquely in the form

$$\alpha = x_1\eta_1 + \cdots + x_n\eta_n \, (x_1, \ldots, x_n \in \mathbb{Z})$$

then $\{\eta_1, \ldots, \eta_n\}$ is called a basis for the ideal I.

Definition 1.95 (Discriminant of an ideal)**.** Let K be an algebraic number field of degree n. Let I be a nonzero ideal of O_K. Let $\{\eta_1, \ldots, \eta_n\}$ be a basis of I. Then the discriminant $D(I)$ of the ideal I is the nonzero integer given by

$$D(I) = D(\eta_1, \ldots, \eta_n).$$

Definition 1.96 (Integral basis of an algebraic number field)**.** Let K be an algebraic number field. A $\mathbb{Z}$-basis for O_K is called an integral basis for K.

Theorem 1.97. *Let K be a quadratic field. Let m be the unique squarefree integer such that $K = \mathbb{Q}(\sqrt{m})$. Then $\{1, \sqrt{m}\}$ is an integral basis for K if $m \not\equiv 1 \pmod 4$ and $\left\{1, \frac{1+\sqrt{m}}{2}\right\}$ is an integral basis for K if $m \equiv 1 \pmod 4$.*

Definition 1.98 (Discriminant of an algebraic number field)**.** Let K be an algebraic number field of degree n. Let $\{\eta_1, \ldots, \eta_n\}$ be an integral basis for K. Then $D(\eta_1, \ldots, \eta_n)$ is called the discriminant of K and is denoted by $d(K)$.

Theorem 1.99. *Let K be a quadratic field. Let m be the unique squarefree integer such that $K = \mathbb{Q}(\sqrt{m})$. Then the discriminant $d(K)$ of K is given by*

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

Definition 1.100 (Norm of an ideal)**.** Let K be an algebraic number field of degree n. Let I be a nonzero ideal of O_K. Then the norm of the ideal I, written $N(I)$, is the positive integer defined by

$$N(I) = \sqrt{\frac{D(I)}{d(K)}}.$$

Definition 1.101 (Index of θ)**.** Let K be an algebraic number field. Let $\theta \in O_K$ be such that $K = \mathbb{Q}(\theta)$. Then the index of θ, written $\text{ind}\theta$, is the positive integer given by

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

Theorem 1.102. *Let K be an algebraic number field of degree n. Let $\theta \in O_K$ be such that $K = \mathbb{Q}(\theta)$. Then $\{1, \theta, \theta^2, \ldots, \theta^{n-1}\}$ is an integral basis for K if and only if* $\text{ind}\theta = 1$.

Theorem 1.103. *Let K be an algebraic number field of degree n. Let $\theta \in O_K$ be such that $K = \mathbb{Q}(\theta)$. If $D(\theta)$ is squarefree then $\{1, \theta, \ldots, \theta^{n-1}\}$ is an integral basis for K.*

Theorem 1.104 (Stickelberger's Theorem)**.** *Let K be an algebraic number field. Then*

$$d(K) \equiv 0 \text{ or } 1 \pmod 4.$$

1.5.5 Ideals in a Dedekind Domain

It's known that the ring of algebraic integers O_K of an algebraic number field K is a Dedekind domain. Therefore we are interested in how ideals act in this sort of structure. The motivation for the study of ideal theory is to restore unique factorization when working in the ring of integers of K.

Definition 1.105 (Fractional Ideal)**.** Let D be an integral domain. Let K be the quotient field of D. A nonempty subset A of K with the following three properties:

1. $\alpha \in A, \beta \in A \Longrightarrow \alpha + \beta \in A$,
2. $\alpha \in A, r \in D \Longrightarrow r\alpha \in A$, and
3. there exists $\gamma \in D$ with $\gamma \neq 0$ such that $\gamma A \subseteq D$

is called a fractional ideal of D. An ideal in the ordinary sense (let $\gamma = 1$) is a fractional ideal, and is often referred to as an *integral ideal*.

Theorem 1.106. *If D is a Dedekind domain, every proper integral ideal is a product of prime ideals and this factorization is unique in the sense that if*

$$P_1 P_2 \cdots P_k = Q_1 Q_2 \cdots Q_l,$$

where the P_i and Q_j are prime ideals, then $k = l$, and after relabeling (if necessary)

$$P_i = Q_i, \ i = 1, 2, \ldots, k.$$

Recall that the fundamental theorem of arithmetic for integers states that every integer can be written uniquely as a product of primes. This next theorem for ideals is analogous.

Corollary 1.107. *Let K be an algebraic number field. Then every proper integral ideal of O_K can be expressed uniquely up to order as a product of prime ideals.*

Definition 1.108. Let D be a Dedekind domain. Let A and B be nonzero integral ideals of D. We say that A divides B, written $A \mid B$, if there exists an integral ideal C of D such that $B = AC$.

1.5.6 Norm of a Prime Ideal

Theorem 1.109. *Let K be an algebraic number field. Let P be a prime ideal of O_K. Then there exists a unique rational (integer) prime p such that*

$$P \mid \langle p \rangle.$$

The rational prime p in the above theorem is called the prime lying below P since $P \supseteq \langle p \rangle$. In this case, we would likewise say that the prime ideal P is lying above the rational prime p.

Definition 1.110. Let K be an algebraic number field of degree n. Let P be a prime ideal of O_K. Let p be a rational prime lying below P. Then the unique positive integer e such that

$$P^e \mid \langle p \rangle, P^{e+1} \nmid \langle p \rangle$$

is called the ramification index of P in K and is written $e_K(P)$.

Theorem 1.111. *Let K be an algebraic number field with $[K : \mathbb{Q}] = n$. Let P be a prime ideal of O_K. Let p be the rational prime lying below P. Then*

$$N(P) = p^f$$

for some integer $f \in \{1, 2, \ldots, n\}$.

Definition 1.112. Let K be an algebraic number field with $[K : \mathbb{Q}] = n$. Let p be the rational prime lying below P. Then the positive integer f such

that

$$N(P) = p^f$$

is called the inertial degree of P in O_K and is denoted by $f_K(P)$.

Theorem 1.113. *Let K be an algebraic number field with $[K : \mathbb{Q}] = n$. Let p be a rational prime. Suppose that the principal ideal $\langle p \rangle$ factors in O_K in the form*

$$\langle p \rangle = P_1^{e_1} \cdots P_g^{e_g},$$

where $P_1, \ldots, P_g$ are distinct prime ideals of O_K and $e_1, \ldots, e_g$ are positive integers. Suppose that f_i is the inertial degree of P_i ($i = 1, 2, \ldots, g$) in K, that is, $f_i = f_K(P_i)$. Then

$$e_1 f_1 + \cdots + e_g f_g = n.$$

Definition 1.114. The positive integer g in the above theorem is called the decomposition number of p in K and is written $g_K(p)$ with $g_K(p) \leq n$..

Definition 1.115. Let K be an algebraic number field of degree n and p be a rational prime. Let

$$\langle p \rangle = P_1^{e_1} \cdots P_r^{e_r}$$

be the prime ideal factorization of $\langle p \rangle$ in K. If $e_i > 1$ for some $i = 1, 2, \ldots, r$ then p is said to ramify in K. If $e_i = 1$ for $i = 1, 2, \ldots, r$ then p is said to be unramified in K.

Proposition 1.116. *[Nar90, p. 159] If $\mathfrak{p}$ is a prime ideal of a Dedekind domain R unramified in both K_1/K and K_2/K then it is also unramified in the composite extension K_1K_2/K.*

Theorem 1.117. *Let K be an algebraic number field. Then the rational prime p ramifies in K if and only if $p \mid d(K)$.*

Theorem 1.118. *Let K be an algebraic number field. Let I be an nonzero ideal of O_K.*

(a) If $N(I) = p$, where p is a prime, then I is a prime ideal.

(b) $N(I) \in I$.

1.5.7 Factoring Primes in a Quadratic Field

Let p be a rational prime and let K be a quadratic field. Since the degree of K over $\mathbb{Q}$ is 2, we know that the decomposition number $g = g_K(p) \leq 2$ so that $g = 1$ or 2.

If $g = 2$, then by Theorem 1.113

$$e_1 f_1 + e_2 f_2 = 2$$

so that

$$e_1 = f_1 = e_2 = f_2 = 1.$$

If $g = 1$, then

$$e_1 f_1 = 2$$

so that

$$(e_1, f_1) = (2, 1) \text{ or } (1, 2).$$

Therefore, we have three different cases:

1. $g = 2, e_1 = f_1 = e_2 = f_2 = 1$,
2. $g = 1, e_1 = 2, f_1 = 1$,
3. $g = 1, e_1 = 1, f_1 = 2$.

In other words,

1. $\langle p \rangle = P_1 P_2,\ N(P_1) = N(P_2) = p,\ P_1 \neq P_2$,
2. $\langle p \rangle = P^2,\ N(P) = p$,
3. $\langle p \rangle = P,\ N(P) = p^2$.

It is important to note that the ideal norm is multiplicative. This next theorem gives necessary and sufficient conditions for the above cases to occur. It is the essential theorem to use when deciding how ideals factor into primes in quadratic fields.

Definition 1.119. If m is a positive integer, we say that the integer a is a quadratic residue of m if $\gcd(a, m) = 1$ and the congruence $x^2 \equiv a \pmod{m}$ has a solution. If the congruence has no solution, then a is a quadratic nonresidue of m.

Definition 1.120. Let p be an odd prime and a be an integer not divisible by p. The Legendre symbol $\left(\frac{a}{p}\right)$ is defined by

$$\left(\frac{a}{p}\right) = \begin{cases} 1 \text{ if } a \text{ is a quadratic residue of } p \\ -1 \text{ if } a \text{ is a quadratic nonresidue of } p \end{cases}$$

Theorem 1.121. *Let K be a quadratic field so that there exists a squarefree integer m such that $K = \mathbb{Q}(\sqrt{m})$. Let p be a rational prime.*

1. *If $p > 2$, $\left(\frac{m}{p}\right) = 1$ or $p = 2$, $m \equiv 1 \pmod{8}$ then*

$$\langle p \rangle = P_1 P_2,$$

   where P_1 and P_2 are distinct prime ideals with $N(P_1) = N(P_2) = p$.

2. *If $p > 2$, $p \mid m$ or $p = 2, m \equiv 2$ or $3 \pmod{4}$ then*

$$\langle p \rangle = P^2,$$

   where P is a prime ideal with $N(P) = p$.

3. *If $p > 2$, $\left(\frac{m}{p}\right) = -1$ or $p = 2$, $m \equiv 5 \pmod{8}$ then*

$$\langle p \rangle \text{ is a prime ideal of } O_K.$$

Using the previous theorem, we can now express the factorizations of the ideals $\langle p \rangle$ into prime ideals of O_K in the quadratic field $K = \mathbb{Q}(\sqrt{m})$ as follows:

$$\langle 2\rangle = \begin{cases} \langle 2\rangle, & \text{if } m \equiv 5 \pmod 8, \\ \langle 2, \frac{1}{2}(1+\sqrt{m})\rangle\langle 2, \frac{1}{2}(1-\sqrt{m})\rangle, & \text{if } m \equiv 1 \pmod 8, \\ \langle 2, 1+\sqrt{m}\rangle^2, & \text{if } m \equiv 3 \pmod 4, \\ \langle 2, \sqrt{m}\rangle^2, & \text{if } m \equiv 2 \pmod 4, \end{cases}$$

and for $p > 2$,

$$\langle p\rangle = \begin{cases} \langle p\rangle, & \text{if } p \nmid m \text{ and } x^2 \equiv m \pmod p \text{ is insolvable}, \\ \langle p, x+\sqrt{m}\rangle\langle p, x-\sqrt{m}\rangle & \text{if } p \nmid m \text{ and } x^2 \equiv m \pmod p \text{ is solvable}, \\ \langle p, \sqrt{m}\rangle^2, & \text{if } p \mid m. \end{cases}$$

1.5.8 Factoring Primes in a Monogenic Number Field

Definition 1.122. Let K be an algebraic number field. K is monogenic if there exists $\theta \in O_K$ such that $\{1, \theta, \theta^2, \ldots, \theta^{n-1}\}$ is an integral basis for K.

The following theorem shows how to factor the ideal $\langle p\rangle$ (p a rational prime) into prime ideals in a monogenic number field.

Theorem 1.123 (Dedekind's Theorem)**.** *Let $K = \mathbb{Q}(\theta)$ be an algebraic number field of degree n with $\theta \in O_K$. Let p be a rational prime. Let*

$$f(x) = irr_{\mathbb{Q}}(\theta) \in \mathbb{Z}[x].$$

If p is not a divisor of the index of θ, and

$$f(x) \equiv g_1(x)^{e_1} \cdots g_r(x)^{e_r} \pmod p,$$

is the decomposition of $f(x) \pmod p$ where $g_1(x), \ldots, g_r(x)$ are distinct, monic, irreducible polynomials in $\mathbb{Z}_p[x]$ and $e_1, \ldots, e_r$ are positive integers, then there exists r distinct prime ideals of O_K, $P_1, \ldots, P_r$ with

$$\langle p\rangle = P_1^{e_1} \cdots P_r^{e_r}$$

and

$$N(P_i) = p^{deg\ g_i},\ i = 1, 2, \ldots, r.$$

Furthermore,

$$P_i = \langle p, g_i(\theta) \rangle,\ i = 1, 2, \ldots, r.$$

Example 1.124. Let $K = \mathbb{Q}(\sqrt[3]{2})$. We want to factor the ideal $\langle 11 \rangle$ as a product of prime ideals in O_K. Let $\theta = \sqrt[3]{2}$ so that the minimal polynomial of θ is $x^3 - 2$. An integral basis for $K = \mathbb{Q}(\theta)$ is $\{1, \theta, \theta^2\}$ so that K is monogenic. Factoring $x^3 - 2$ modulo 11, we get

$$x^3 - 2 = (x + 4)(x^2 + 7x + 5) \pmod{11},$$

where $x + 4$ and $x^2 + 7x + 5$ are both irreducible modulo 11. Therefore, by Theorem 1.123, we have

$$\langle 11 \rangle = PQ$$

where

$$P = \langle 11, \theta + 4 \rangle,\ Q = \langle 11, \theta^2 + 7\theta + 5 \rangle$$

are distinct prime ideals with

$$N(P) = 11,\ N(Q) = 11^2 = 121.$$

Chapter 2

Group Coverings and Intersective Polynomials

2.1 Group Coverings with Examples

In this section, we discuss group covers, which will be integral in finding our intersective polynomials.

Definition 2.1. Let H be a subgroup of a group G. Let g be a fixed element of G that is not a member of H. Then the elements gh_ig^{-1} for all h_i in H, $i = 1, 2, \ldots$ generates the conjugate subgroup gHg^{-1}. If for all g, $gHg^{-1} = H$, then H is a normal (or self-conjugate or invariant) subgroup.

Definition 2.2. Let G be a group. Two subgroups H_1 and H_2 of G are called conjugate subgroups if there is an element g in G such that $gH_1g^{-1} = H_2$.

Proposition 2.3. *Let G be a group and R be a relation on G defined by $a \sim b$ if a is conjugate to b. Then $a \sim b$ if there is a g in G such that $a = gbg^{-1}$. Then R is an equivalence relation, that is, conjugation adheres to the three following properties:*

1. *$a \sim a$ (Reflexive)*
2. *If $a \sim b$ then $b \sim a$ (Symmetric)*
3. *If $a \sim b$ and $b \sim c$ then $a \sim c$ (Transitive)*

Definition 2.4. A group is n-coverable if it is a union of conjugates of n proper subgroups, whose total intersection is trivial. More explicitly, let

G be a finite group. Let $H_1, \ldots, H_n$ be the proper subgroups of G, each having $k_1, \ldots k_n$ distinct conjugates (including the subgroup itself), notated as $H_i^{(j)} = \{gH_ig^{-1} \mid g \in G\}$ for $1 \leq j \leq k_i$.

Now let $\mathcal{H}_i = \bigcup_{j=1}^{k_i} H_i^{(j)}$. The set-theoretical union of the $\mathcal{H}_i$ is called a covering for G if $G = \bigcup_{i=1}^{n} \mathcal{H}_i$, where all of the conjugates of all the subgroups in the union have trivial intersection.

When we talk about n-coverable groups we will always assume that $n > 1$ as the next lemma establishes that no group is 1-coverable.

Lemma 2.5. *Let G be a finite group. Then G is not 1-coverable.*

Proof. Let G be a finite group of order $|G|$ and let H be a proper subgroup of G. The conjugates of H we denote as H_i, for $i = 1, 2, \cdots k$.

Now let $G = \bigcup_{i=1}^{k} H_i$ and let $N_G(H) = \{g \in G \mid gHg^{-1} = H\}$ be the normalizer of H in G. Note that $H \subsetneq N_G(H)$ since H is not a normal subgroup of G. The number of conjugates of H is the index of $N_G(H)$ in G, which is less than or equal to $|G|/|H|$, i.e.

$$k \leq |G|/|H|.$$

However, if you only count the identity once, then the number of elements in the union of the conjugates of H is at most

$$|H| \cdot \frac{|G|}{|H|} - (k-1) = |G| - k + 1.$$

Since H is a proper subgroup of G, k is at least 2. Thus the number of elements in the union of the conjugates of H is less than $|G|$, and thus a 1-cover is impossible □

Lemma 2.6. *A cyclic group G cannot be n-coverable for $n > 1$.*

Proof. Suppose that G is cyclic with $G = \langle g \rangle$ for some $g \in G$ and suppose that H is a proper subgroup of G.

Now suppose that G is n-coverable for $n > 1$. Then the element g must be contained in one of the conjugates of H since G is composed of the union of the conjugates. Then this subgroup contains $\langle g \rangle = G$. However the conjugate of a proper subgroup is proper, contradicting that it contains G. Thus G is not n-coverable. □

2.1.1 2-Coverable Groups

Groups that are 2-coverable ($n = 2$) are of particular interest. It has been proven in Bubboloni [Bub98] that the symmetric group S_m is 2-coverable if and only if $3 \leq m \leq 6$ and the alternating group A_m is 2-coverable if and only if $4 \leq m \leq 8$.

The Frobenius Group

Definition 2.7. A finite group G is said to be a Frobenius group if there is a non-trivial subgroup H of G such that $H \cap gHg^{-1} = \{1\}$ whenever $g \notin H$. This gives a decomposition

$$G = \bigcup_{gH \in G/H} (gHg^{-1} \backslash \{1\}) \cup K$$

where K is the subset defined as the identity element 1 together with all the non-identity elements that are not conjugate to any element of H. The subset K is called the Frobenius kernel of G and H is called the Frobenius complement.

Interestingly enough, there is a great amount of structure on K and thus on G, shown in a theorem of Frobenius himself.

Theorem 2.8. *Let G be a Frobenius group with Frobenius complement H and Frobenius kernel K. Then K is a normal subgroup of G and therefore G is the semidirect product $K \rtimes H$ of H and K.*

The Frobenius group is of interest because it has been proven in Sonn [Son08] that all Frobenius groups are 2-coverable. An example of an intersective polynomial with a Frobenius Galois group is given in Section 2.2.2.

A_4, The Alternating Group of 4 Letters

Consider A_4, the alternating group on 4 letters. We will show that A_4 is 2-coverable with subgroups isomorphic to V_4 and $\mathbb{Z}/3\mathbb{Z}$ respectively. Now

$$A_4 = \{1, (12)(34), (13)(24), (14)(23), (123), (132), (124), (142), (134), (143), (234), (243)\}.$$

Consider

$$H_1 = \{1, (12)(34), (13)(24), (14)(23)\}.$$

Then H_1 is isomorphic to V_4, the Klein-4 group, and further $[A_4 : H_1] = 3$. H_1 is normal in A_4 and so the only conjugate of H_1 in A_4 is itself. Now consider

$$H_2 = \{1, (123), (132)\}, H_3 = \{1, (124), (142)\}, H_4 = \{1, (134), (143)\}, H_5 = \{1, (234), (243)\}.$$

Each of these subgroups are isomorphic to $\mathbb{Z}/3\mathbb{Z}$. Furthermore, they are all conjugate to one another.

We show that H_2, H_3, H_4, H_5 are conjugate subgroups by finding elements in A_4 such that all of the H_i transitively conjugate with each other. This will finalize the result. Note that the conjugation of the identity element 1 is always the identity element. The necessary conjugations are given below:

$$(124)H_2(142) = H_5$$
$$(124)H_5(142) = H_4$$
$$(123)H_4(132) = H_3$$

Therefore, $H_2 \sim H_5$, $H_5 \sim H_4$, and $H_4 \sim H_3$ and thus $H_i \sim H_j$ for $2 \leq i, j \leq 5$.

Taking the union of all 5 groups above, with $\mathcal{H}_1 = H_1$ and $\mathcal{H}_2 = H_2 \cup$

$H_3 \cup H_4 \cup H_5$, we conclude that

$$A_4 = \mathcal{H}_1 \cup \mathcal{H}_2$$

with trivial intersection. Thus $\{\mathcal{H}_1, \mathcal{H}_2\}$ is a 2-cover of A_4.

S_3, The Symmetric Group on 3 Letters

We now consider S_3, the symmetric group on 3 letters. The two subgroups of S_3, A_3 and C_2, the cyclic group of order 2 (and its conjugates) form a cover. Recall

$$S_3 = \{1, (12), (13), (23), (123), (132)\}.$$

Now consider the subgroups

$$H_1 = \{1, (123), (132)\}$$

and

$$H_2 = \{1, (12)\}, H_3 = \{1, (13)\}, H_4 = \{1, (23)\}.$$

The subgroup H_1 has index 2 and is therefore normal. This is the subgroup A_3. We claim that the three subgroups H_2, H_3, and H_4 are conjugate subgroups. Indeed, letting $g_1 = (23)$ and $g_2 = (12)$, it is easy to see that

$$g_1(12){g_1}^{-1} = (13)$$
$$g_2(13){g_2}^{-1} = (23)$$

which verifies the claim so that $H_2 \sim H_3$ and $H_3 \sim H_4$. Then by transitivity, $H_2 \sim H_4$ and they are all conjugate subgroups. Taking the union of all four groups above, we can show that for $\mathcal{H}_1 = H_1$ and $\mathcal{H}_2 = H_2 \cup H_3 \cup H_4$,

$$S_3 = \mathcal{H}_1 \cup \mathcal{H}_2$$

with trivial intersection. Thus $\{\mathcal{H}_1, \mathcal{H}_2\}$ is a 2-cover of S_3.

D_5, The Dihedral Group of Order 10

Recall that D_5 is the group of symmetries of a regular pentagon with order 10. Interestingly enough, the dihedral group can be viewed as a semi-direct product with $D_5 = C_5 \rtimes C_2$. The subgroups of D_5 either have order 5 or order 2, thus D_5 has only cyclic subgroups.

We will work with the following group presentation of D_5:

$$D_5 = \{1, r, r^2, r^3, r^4, f, fr, fr^2, fr^3, fr^4\} = \langle f, r \mid r^5 = f^2 = 1, frf = r^{-1} \rangle$$

where r represents the rotation of the pentagon and f represents the flip of the pentagon over its vertical axis. The subgroups of D_5 are $H_1 = \langle r \rangle$, which is normal because it has index 2 in D_5 and isomorphic to C_5, and the subgroups $H_2 = \langle f \rangle, H_3 = \langle fr \rangle, H_4 = \langle fr^2 \rangle, H_5 = \langle fr^3 \rangle$, and $H_6 = \langle fr^4 \rangle$, all isomorphic to C_2. Notice that $H_1, \ldots, H_6$ are conjugate subgroups via the relations

$$\begin{aligned} rH_2r^{-1} &= H_5 \\ r^2H_5r^{-2} &= H_6 \\ fH_6f^{-1} &= H_3 \\ rH_3r^{-1} &= H_4 \end{aligned}$$

Therefore, for $\mathcal{H}_1 = H_1$ and $\mathcal{H}_2 = H_2 \cup H_3 \cup H_4 \cup H_5 \cup H_6$, a 2-cover for D_5 is $\{\mathcal{H}_1, \mathcal{H}_2\}$.

D_p, The Dihedral Group of Order $2p$

We now generalize a cover for the dihedral group of order $2p$. We will use Sylow theory to show that all dihedral groups of order $2p$ are 2-coverable.

Theorem 2.9 (Lagrange's Theorem)**.** *If G is a finite group and H is a subgroup of G, then the order of H divides the order of G (that is $|H| \mid |G|$) and the number of left cosets of H in G equals $|G|/|H|$.*

While the consequence of this theorem is prevalent in group theory, the converse isn't always true: for any given divisor m of $|G|$, there doesn't necessarily exist a subgroup H of G such that $|H| = m$. For example, the alternating group on 4 letters, A_4, has order 12 but has no subgroup of order 6. We can, however, use a partial converse to Lagrange's theorem well known as Sylow's Theorem.

Definition 2.10. Let G be a group and let p be a prime.

1. A group of order p^n for some $n \geq 1$ is called a p-group. Subgroups of G which are p-groups are called p-subgroups.

2. If G is a group of order $p^n m$, where $p \nmid m$, then a subgroup of order p^n is called a Sylow p-subgroup of G.

Theorem 2.11. *For every prime factor p with multiplicity n of the order of a finite group G, there exists a Sylow p-subgroup of G, of order p^n.*

Theorem 2.12. *Given a finite group G and a prime number p, all Sylow p-subgroups of G are conjugate to each other, i.e. if H and K are Sylow p-subgroups of G, then there exists an element g in G with $g^{-1}Hg = K$.*

Theorem 2.13. *Let p be a prime factor with multiplicity n of the order of a finite group G, so that the order of G can be written as $p^n m$, where $n > 0$ and p does not divide m. Let n_p be the number of Sylow p-subgroups of G. Then the following hold:*

1. *n_p divides m, which is the index of the Sylow p-subgroup in G.*

2. *$n_p \equiv 1 \pmod{p}$.*

3. *$n_p = |G : N_G(P)|$, where P is any Sylow p-subgroup of G and N_G denotes the normalizer of P in G.*

Lemma 2.14 (Cavior's Theorem)**.** *If $n \geq 3$, the number of subgroups of D_n is $\tau(n)+\sigma(n)$, where $\tau(n)$ denotes the number of divisors of n and represents the number of cyclic subgroups of D_n, and $\sigma(n)$ denotes the sum of divisors of n and represents the number of noncyclic subgroups of D_n.*

Theorem 2.15. *There are two kinds of subgroups for a dihedral group D_n given by*

$$D_n = \langle r, f : r^n = f^2 = e, frf = r^{-1} \rangle$$

(see [Con]):

1. *Subgroups of the form $\langle r^d \rangle$, where $d \mid n$. There is only one such subgroup for each d. The total number of such subgroups is $\tau(n)$, where $\tau(n)$ denotes the number of positive divisors of n.*

2. *Subgroups of the form $\langle r^d, r^k f \rangle$ where $d \mid n$ and $0 \leq k < d$. There are d such subgroups for each such divisor d. The total number of such subgroups is $\sigma(n)$, the sum of positive divisors of n.*

Because the order of D_p is $2p$, by Theorem 2.11 there exists a Sylow 2-subgroup and a Sylow p-subgroup of D_p. The index of the Sylow p-subgroup is 2, and is therefore normal. Since n_p divides 2 and is also congruent to 1 mod p, it must be true that $n_p = 1$, implying that there exists only 1 Sylow p-subgroup. By the first condition above, there are subgroups $\langle r \rangle$ and $\langle r^p \rangle$ of D_p. Because $r^p = e$, we have $\langle r^p \rangle = \{e\}$. As $|\langle r \rangle| = p$, we see that $\langle r \rangle$ is a Sylow p-subgroup of D_p, hence is unique by the above argument.

Condition 2 also implies the existence of subgroups of the form $\langle r^d, fr^k \rangle$ where $d \mid p$ and $0 \leq k < d$. The case where $d = 1$ yields the entire group. For $d = p$ there are p such subgroups, all of order 2. These p groups are all conjugate groups by Theorem 2.12. Therefore for $\mathcal{H}_1 = \langle r \rangle$ and $\mathcal{H}_2 = \bigcup_{k=0}^{p-1} \left\langle fr^k \right\rangle$, $\{\mathcal{H}_1, \mathcal{H}_2\}$ forms a cover for D_p.

2.1.2 The Holomorph $\mathbb{Z}_{32} \rtimes \mathbb{Z}_{32}^*$

We will introduce some theorems that are proven in general in Chapter 4 for the holomorph $\mathbb{Z}_{2^e} \rtimes \mathbb{Z}_{2^e}^*$. This will allow us to state a 3-cover for the single case where $e = 5$. Let $\mathcal{G}$ be the group

$$\mathcal{G} \simeq \mathbb{Z}_{32} \rtimes \mathbb{Z}_{32}^*.$$

Consider the subgroups $\{H_1, H_2, H_3\}$ of $\mathcal{G}$ defined by

$$H_1 = \{(b, 5^c) : b = 0, 1, \ldots, 31,\ c = 0, 1, \ldots, 7\},$$

$$H_2 = \{(0, d) : d = 1, 3, \ldots, 31\},$$

$$H_3 = \langle (1, -1), (3, -5) \rangle .$$

We will show that these three subgroups form a 3-cover for $\mathcal{G}$.

Lemma 2.16. *The conjugates of the subgroup*

$$H_2 = \{(0, d) : d = 1, 3, \ldots, 31\}$$

of the group

$$\mathcal{G} \simeq \mathbb{Z}_{32} \rtimes \mathbb{Z}_{32}^*.$$

have the form

$$\{(n(d-1), d) : d = 1, 3, \ldots, 31\},$$

where n is a fixed integer modulo 32.

Lemma 2.17. *The conjugates of the subgroup*

$$H_3 = \langle (1, -1), (3, -5) \rangle$$

of the group

$$\mathcal{G} \simeq \mathbb{Z}_{32} \rtimes \mathbb{Z}_{32}^*.$$

have the form

$$\langle (m, -1), (3m, -5) \rangle ,$$

for a fixed odd integer m modulo 32.

We begin by showing $\mathcal{G}$ is equal to the union of the conjugates of the subgroups H_i, $i = 1, 2, 3$. For notation, H_i^c denotes a conjugate of H_i. We consider a typical element

$$(k, j) \in \mathcal{G}$$

where k is any integer modulo 32 and j is any odd integer modulo 32. We may write $j = \pm 5^{2a}$ or $\pm 5^{2a+1}$ for a nonnegative integer a. Some of the cases require that we set $k = 2w$ or $k = 2w + 1$. The following table summarizes all of the containments.

Type	1	2	3	4
Element	$(k, 5^a)$	$(2w, -(5)^a)$	$(2w+1, -(5)^{2a+1})$	$(2w+1, -(5)^{2a})$
Belongs to	H_1	H_2^c	H_3^c	H_3^c

It can easily be shown that the four above inclusions are satisfied, that is, all elements of $\mathcal{G}$ are contained in some conjugate of the H_i.

All of these subgroups/containments have trivial intersection, and thus $\{H_1, H_2, H_3\}$ forms a cover for $\mathcal{G}$.

2.2 Intersective Polynomials

2.2.1 Introduction

In this section, we introduce intersective polynomials and provide an overview of the theory used to show that a family of polynomials is intersective.

Definition 2.18 (Intersective Polynomial)**.** A monic polynomial $f(x)$ with integer coefficients is called intersective if it has no root in the rational numbers $\mathbb{Q}$ but has a root modulo m for all positive integers $m > 1$.

The reason why intersective polynomials are interesting is that they provide counterexamples to the local global principle. This principle states that the existence or non-existence of solutions in $\mathbb{Q}$ (global) of a diophantine equation can be detected by studying, for each $p \leq \infty$, the solutions of the equation in the p-adic field $\mathbb{Q}_p$ (local) [Gou93].

Intersective polynomials have applications in combinatorial number theory, intersective sets, multiple recurrence in ergodic theory and Diophantine approximation. The reader should consult Lê [Lê14], Bergelson, Leibman

and Lesigne [BLL08] and Lê and Spencer [LS14]. Intersective polynomials also arise in the context of number fields and function fields. Information on these topics can be found Bergelson and Robertson [BR] and Yamagishi [Yam].

Sonn [Son08, Thm 2.2] proved that every finite, noncyclic, solvable group G can be realized as the Galois group over $\mathbb{Q}$ of an intersective polynomial, with the noncyclic condition being necessary. The same statement was also established by Sonn [Son09] for realizable nonsolvable Galois groups. These papers also explicitly give a method of constructing intersective polynomials.

Intersective polynomials are challenging to construct. Single examples of intersective polynomials with Galois group isomorphic to the alternating group A_n, $4 \leq n \leq 8$ or to the symmetric group S_n, $3 \leq n \leq 6$ are given by Rabayev and Sonn [RS13]. These groups are 2-coverable so that the intersective polynomial will have two irreducible factors over $\mathbb{Q}$. For example, in the case where the Galois group is A_4, they prove that the polynomial

$$(x^4 - 10x^3 - 7x^2 + 3x + 2)(x^3 + 89x^2 + 2586x + 24649)$$

is intersective, and in the case where the Galois group is S_4, they prove that the polynomial

$$(x^4 - 5x^2 + x + 4)(x^3 + 10x^2 + 9x + 1)$$

is intersective.

Candidates for intersective polynomials are constructed by forming the product of the defining polynomials of the fixed fields corresponding to the subgroups in the n-cover via Galois theory. The only infinite families of intersective polynomials that we are aware of appear in [LSY14] and in the papers published that appear in this thesis.

2.2.2 The Frobenius Group

The Frobenius group is of interest because it has been proven in Sonn [Son08] that all Frobenius groups are 2-coverable and that there exists a

polynomial $f(x)$ which is the product of two irreducible polynomials in $\mathbb{Q}[x]$ with Frobenius Galois group G and having a root modulo m for all $m > 1$.

A polynomial of particular interest with Frobenius Galois group was presented in [Bra01] that has the form

$$f(x) = (x^p - 2)\Phi_p(x)$$

where $\Phi_p(x)$ denotes the pth cyclotomic polynomial with p an odd prime. The proof that $f(x)$ is intersective is as follows:

Let q be a prime. If p does not divide $q - 1$, then 2 is a pth power in the p-adic integers $\mathbb{Z}_q$, and so $x^p - 2$ has a root mod q. If $p \mid q - 1$, then $\mathbb{Z}_q$ contains primitive pth roots of unity, and thus $\Phi_p(x)$ has a root mod q. Therefore $f(x)$ has a root mod q for all primes q.

Of course, this is a special case that is easy to show because of the construction of the Frobenius group. For other groups, more advanced methods need to be employed.

2.2.3 Hensel's Lemma

Showing that a polynomial $f(x)$ has a solution mod m for every integer $m > 1$ is equivalent to showing that it has a solution mod p^j for each prime p and positive integer j. The equivalence is a consequence of the Chinese Remainder Theorem. An infinite family of intersective polynomials has been found in Hyde, Lee, and Spearman [HLS14] where we use Hensel's Lemma and a refined version of Hensel's Lemma to lift certain polynomial solutions modulo p to arbitrarily high powers of p. We state the two lemmas below and then give the family of polynomials in question.

Theorem 2.19 (Hensel's Lemma)**.** *(see [INM95, p. 87]) Suppose that $f(x)$ is a polynomial with integral coefficients. If $f(a) \equiv 0 (\text{mod } p^j)$ and $f'(a) \not\equiv 0 (\text{mod } p)$, then there is a unique $t (\text{mod } p)$ such that $f(a + tp^j) \equiv 0 (\text{mod } p^{j+1})$.*

If the condition $f'(a) \not\equiv 0 (\text{mod } p)$ holds, then the root a is called nonsingular. By repeated application of Hensel's Lemma, a nonsingular root a of $f(x) \equiv$

$0(\text{mod } p)$ may be lifted to a root modulo p^j, for $j = 2, 3, \ldots$. The refined version of Hensel's Lemma which, in the case of a singular root, enables us to lift their solutions modulo arbitrarily high prime powers. This version is as follows:

Theorem 2.20 (Hensel-Rychlik Lemma)**.** *(see [INM95, p. 89]) Let $f(x)$ be a polynomial with integral coefficients. Suppose that $f(a) \equiv 0(\text{mod } p^j)$, that $p^\tau \parallel f'(a)$ and that $j \geq 2\tau+1$. If $b \equiv a(\text{mod } p^{j-\tau})$ then $f(b) \equiv f(a)(\text{mod } p^j)$ and $p^\tau \parallel f'(b)$. Moreover there is a unique $t(\text{mod } p)$ such that $f(a+tp^{j-\tau}) \equiv 0(\text{mod } p^{j+1})$.*

Using these lemmas, we were able to show that for n, a cubefree integer not equal to 1, the polynomial

$$f(x) = (x^3 - n)(x^2 + 3)$$

is intersective if and only if the prime factors of n are of the form $3k+1$ and $n \equiv 1(\text{mod } 9)$.

2.2.4 Decomposition Groups

When elementary methods cannot be applied to intersective polynomial problems, more advanced theory must be introduced to establish the intersective property. One method is to use decomposition groups, which will be used extensively later in this thesis. We give their definition now.

Definition 2.21. The decomposition group $G(\mathfrak{p})$ is the set of elements $\sigma \in Gal(L/\mathbb{Q})$ such that $\sigma(\mathfrak{p}) = \mathfrak{p}$, where $\mathfrak{p}$ is a prime ideal in L and $L/\mathbb{Q}$ is the extension of L over $\mathbb{Q}$.

To form intersective polynomials, we first need to discover whether or not intersective polynomials can be formed with the group we are working with. Once we know that the conditions are satisfied, we can use Galois and field theory to form the factors that our intersective polynomial will be composed of. The method is outlined in detail next.

Let G be a finite, noncyclic group. We first have to show that G is n-coverable for some $n > 1$, that is to show G is the union of conjugates of n proper subgroups, the intersection of whose conjugates is trivial. Suppose that the Galois group of $f(x)$, denoted $Gal(f)$, is isomorphic to G and let L denote the splitting field of $f(x)$ so that $Gal(f) = Gal(L/\mathbb{Q})$. If every decomposition group $G(\mathfrak{p})$ for $\mathfrak{p}$ a prime ideal in L is contained in a conjugate of one of the proper subgroups in the n-cover then we know that an intersective polynomial can be constructed.

Showing that every decomposition group for the prime ideals in the splitting field are contained in the proper subgroups is where the bulk of the work lies. The methodology changes depending on the Galois group you are working within but for A_4 and D_5, we took advantage of prime ideal factorization theory to deduce which subgroups the decomposition group lay within. For A_4, we use Dedekind's theorem for prime ideal factorization in a monogenic field. For D_5, we use known theory on dihedral trinomials to deduce prime ideal factorization.

Using the subgroup-subfield correspondence in Galois theory, form the product of the set of n monic polynomials with integer coefficients that define the subfields of L corresponding to the n subgroups forming the cover. The resulting polynomial is intersective.

In practice, when constructing intersective polynomials, it can happen that a decomposition group is cyclic so that containment in the n-cover is automatic.

Chapter 3

Intersective Polynomials with Specified Galois Group

3.1 Intersective Polynomials with Galois Group A_4

3.1.1 Introduction

Recall that a monic polynomial $f(x)$ with integer coefficients is called intersective if it has no root in the rational numbers $\mathbb{Q}$ but has a root modulo m for all positive integers $m > 1$. Sonn [Son08, Thm 2.2] proved that every finite, noncyclic, solvable group G can be realized as the Galois group over $\mathbb{Q}$ of an intersective polynomial, with the noncyclic condition being necessary. The same statement was also established by Sonn [Son09] for realizable nonsolvable Galois groups. We will use the method described in Section 2.2.4 to find an infinite family of intersective polynomials with Galois group A_4.

We first begin by utilizing the knowledge that $G \simeq A_4$ is 2-coverable. Using Sonn's theory, we will show that every decomposition group $G(\mathfrak{p})$ for $\mathfrak{p}$ a prime ideal in L, the splitting field, is contained in a conjugate of one of the proper subgroups in the 2-cover.

Using the subgroup-subfield correspondence in Galois theory, we then form the product of the set of two monic polynomials with integer coefficients that define the subfields of L corresponding to the two subgroups forming the cover. The resulting polynomial is intersective.

In this chapter, we give infinitely many intersective polynomials with Galois group A_4 and nonisomorphic splitting fields. Next we will give some

preliminaries for this family and in Section 3.1.2, we prove our theorem and give some examples. We now state our main theorem.

Theorem 3.1. *There are infinitely many positive integers t such that $t(t^2+108)$ is squarefree. Let t be such an integer and define $f_t(x)$ and $g_t(x)$ by*

$$f_t(x) = x^4 + 18x^2 - 4tx + t^2 + 81 \tag{3.1}$$

and

$$g_t(x) = x^3 - (t^2+108)x + 4t^2 + 432.$$

Then the polynomial

$$f_t(x)g_t(x)$$

is intersective and has Galois group A_4. Furthermore for these values of t the splitting fields of $f_t(x)g_t(x)$ are nonisomorphic.

We begin by recalling from Rabayev and Sonn [RS13] that a 2-cover of A_4 consists of the Sylow 2-subgroup and a Sylow 3-subgroup of A_4. The Sylow 2-subgroup is normal in A_4 and isomorphic to the Klein 4-group. We will construct the family of intersective polynomials from the polynomials given by Spearman [Spe06]. The following proposition summarizes their relevant properties.

Proposition 3.2. *Suppose that t is a positive integer and that $t(t^2+108)$ is squarefree. Let θ_t denote a root of $f_t(x)$ given by (3.1). Then $K_t = \mathbb{Q}(\theta_t)$ is a quartic field with field discriminant $d(K_t) = 2^8t^2(t^2+108)^2$, whose ring of integers has a power integral basis, namely $\{1, \theta_t, \theta_t^2, \theta_t^3\}$. Furthermore, the Galois group of $f_t(x)$ is isomorphic to A_4 and the fields K_t are distinct.*

The resolvent cubic is a cubic polynomial defined from a monic quartic polynomial $q(x)$, where the coefficients of the resolvent cubic can be obtained from the coefficients of $q(x)$ using only basic arithmetic operations. Knowing the roots of the resolvent cubic is useful for finding the roots of $q(x)$. We remark that the resolvent cubic of $f_t(x)$ is $x^3 - 18x^2 - 4(t^2+81)x + 56t^2 + 5832$, which after translating to eliminate the x^2 term and scaling, simplifies to

$g_t(x)$. The polynomials $f_t(x)$ and $g_t(x)$ correspond to the subgroups giving the 2-cover of A_4 using the subfield-subgroup correspondence of Galois theory.

3.1.2 Proof of Theorem

Proof. The fact that there are infinitely many integers t such that

$$t(t^2 + 108)$$

is squarefree follows from a theorem of Erdös [Erd53]. We note that t must be squarefree and must not be divisible by 2 or 3. The fact that the Galois group of $f_t(x)g_t(x)$ is isomorphic to A_4 follows from Proposition 3.2 and the remark after it. The confirmation that $f_t(x)g_t(x)$ is intersective requires us to show that the decomposition group $G(\mathfrak{p})$ is contained in either the Sylow 2-subgroup or a Sylow 3-subgroup of A_4 for any prime ideal $\mathfrak{p}$ in the splitting field L of $f_t(x)$. The groups in the cover are the Klein 4 group, $\mathbb{Z}/3\mathbb{Z}$, and the Sylow subgroups.

If $\mathfrak{p}$ is unramified in L then $G(\mathfrak{p})$ is cyclic as noted by Sonn [Son09] so the containment is automatic. Now let $\mathfrak{p}$ be a prime ideal in L lying above the ramified rational prime p. It suffices to show that $G(\mathfrak{p})$ is a proper subgroup of A_4. As $Gal(f_t)$ acts transitively on the set of prime ideals in L lying above p (see Rosen [Ros02], Proposition 9.2) we deduce that $G(\mathfrak{p})$ is a proper subgroup of A_4 if there are at least two prime ideals in L lying above p. If α_t denotes a root of $g_t(x)$, then L is the compositum of $\mathbb{Q}(\theta_t)$ and $\mathbb{Q}(\alpha_t)$ (because the degrees must multiply to 12) so that p must ramify in at least one of these fields by Proposition 1.116. We recall from Proposition 3.2 that the field discriminant of $\mathbb{Q}(\theta_t)$ is equal to $2^8t^2(t^2 + 108)^2$ while the polynomial discriminant of $g_t(x)$ is equal to $2^2t^2(t^2 + 108)^2$. Since these discriminants contain the same prime factors we deduce that p must ramify in $\mathbb{Q}(\theta_t)$.

Now consider all primes that divide the discriminant. We note that the conditions of Theorem 1.123 are satisfied for $f_t(x)$ and its root θ_t as $f_t(x)$ is the miniminal polynomial for θ_t and $\text{ind}(\theta_t) \neq 0 \pmod{p}$. We will also

make use of the following theorem.

Theorem 3.3. *[Nar90, p. 262] If $L/\mathbb{Q}$ is a normal extension of an algebraic number field, G is its Galois group, and $\mathfrak{p}$ is a prime ideal of O_K, then the index of the decomposition group in $Gal(L/\mathbb{Q})$ equals the number of prime ideals lying above $\mathfrak{p}$ in L.*

Before we begin, we will also state a theorem by Llorente and Nart [LN83] that gives the decomposition of primes in cubic fields K defined by $f(x) = x^3 - ax + b$, where $a, b \in \mathbb{Z}$.

Theorem 3.4. *Let K be a cubic field and let $K = \mathbb{Q}(\theta)$, where θ is a root of an irreducible polynomial of the form*

$$f(X) = X^3 - aX + b,\ a, b \in \mathbb{Z}$$

The discriminant of $f(X)$ is $\Delta = 4a^3 - 27b^2$ and if $D(K)$ is the field discriminant of K, then $\Delta = ind(\theta)^2 \cdot D(K)$. Let $s_p = v_p(\Delta)$ and $\Delta_p = \Delta/p^{s_p}$ for every prime p. The primes of $\mathbb{Q}$ decompose in K as follows:

Decomposition of 2:

a, b even:	$1 \le v_2(b) \le v_2(a)$	$2 = P^3$
	$1 = v_2(a) < v_2(b)$	$2 = P \cdot Q^2$
a even, b odd:	.....	$2 = P \cdot Q$
a odd, b even:	s_2 *odd:*	$2 = P \cdot Q^2$
	s_2 *even:* $\Delta_2 \equiv 3 \pmod 4$	$2 = P \cdot Q^2$
	s_2 *even:* $\Delta_2 \equiv 5 \pmod 8$	$2 = P \cdot Q$
	s_2 *even:* $\Delta_2 \equiv 1 \pmod 8$	$2 = P \cdot Q \cdot R$
a, b odd:	.....	$2 = P$

Decomposition of 3:

$$
\begin{array}{lll}
3 \mid a, 3 \mid b\text{:} & \begin{cases} 1 \le v_3(b) \le v_3(a) & 3 = P^3 \\ 1 = v_3(a) < v_3(b) & 3 = P \cdot Q^2 \end{cases} \\
3 \nmid a\text{:} & \begin{cases} a \equiv -1 \pmod 3 & 3 = P \cdot Q \\ a \equiv 1 \pmod 3 \begin{cases} 3 \nmid b & 3 = P \\ 3 \mid b & 3 = P \cdot Q \cdot R \end{cases} \end{cases} \\
3 \mid a, 3 \nmid b\text{:} & \begin{cases} a \not\equiv 3 \pmod 9 \begin{cases} b^2 \equiv a+1 \pmod 9 & 3 = P \cdot Q^2 \\ b^2 \not\equiv a+1 \pmod 9 & 3 = P^3 \end{cases} \\ a \equiv 3 \pmod 9 \begin{cases} b^2 \equiv a+1 \pmod{27} \begin{cases} s_3 \text{ odd:} & 3 = P \cdot Q^2 \\ s_3 \text{ even:} \begin{cases} \Delta \equiv -1 \pmod 3 & 3 = P \cdot Q \\ \Delta \equiv 1 \pmod 3 \begin{cases} s_3 = 6 & 3 = P \\ s_3 > 6 & 3 = P \cdot Q \cdot R \end{cases} \end{cases} \end{cases} \\ b^2 \not\equiv a+1 \pmod{27} & 3 = P^3 \end{cases} \end{cases}
\end{array}
$$

Decomposition of $p > 3$:

$$
\begin{array}{lll}
p \mid a, p \mid b\text{:} & \begin{cases} 1 \le v_p(b) \le v_p(a) & p = P^3 \\ 1 = v_p(a) < v_p(b) & p = P \cdot Q^2 \end{cases} \\
p \mid a, p \nmid b\text{:} & \begin{cases} p \equiv -1 \pmod 3 & p = P \cdot Q \\ p \equiv 1 \pmod 3 \begin{cases} (b/p)_3 = 1 & p = P \cdot Q \cdot R \\ (b/p)_3 \ne 1 & p = P \end{cases} \end{cases} \\
p \nmid a, p \mid b\text{:} & \begin{cases} (a/p) = 1 & p = P \cdot Q \cdot R \\ (a/p) = -1 & p = P \cdot Q \end{cases} \\
p \nmid ab\text{:} & \begin{cases} s_p \text{ odd}: & p = P \cdot Q^2 \\ s_p \text{ even}: \begin{cases} (\Delta_p/p) = 1 \begin{cases} f(X) \text{ has some root } (\mathrm{mod}\ p) & p = P \cdot Q \cdot R \\ f(X) \text{ has no roots } (\mathrm{mod}\ p) & p = P \end{cases} \\ (\Delta_p/p) = -1 & p = P \cdot Q \end{cases} \end{cases}
\end{array}
$$

Case 1: First we consider $p = 2$, and its factorization in $\mathbb{Q}(\theta_t)$. We have

$$f_t(x) \equiv x^4 (\mathrm{mod}\, 2),$$

so that $\langle 2\rangle = \wp^4$ for some prime ideal $\wp$ in $\mathbb{Q}(\theta_t)$ by Theorem 1.123. The factorization of $\langle 2\rangle$ in the cubic field defined by $g_t(x)$ can be deduced from Theorem 3.4. We find that

$$\langle 2\rangle = P_1P_2P_3$$

for prime ideals P_1, P_2, and P_3 in $\mathbb{Q}(\alpha_t)$. Combining these two factorizations shows that in L we have

$$\langle 2\rangle = (\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3)^4$$

for prime ideals $\mathfrak{p}_1, \mathfrak{p}_2$, and $\mathfrak{p}_3$ in L. Recall by Theorem 3.3 that the index of the decomposition group is equal to the number of prime ideals lying above $\langle 2\rangle$ in L so that the order of the decomposition group is 4. This implies that the decomposition group of a prime ideal in L lying above $\langle 2\rangle$ is isomorphic to the Sylow 2-subgroup which is of course contained in the 2-cover.

Case 2: Next we treat primes p dividing t. If only one prime ideal $\mathfrak{p}$ in L lies above p it follows that only one prime ideal of $\mathbb{Q}(\theta_t)$ lies above p. Factoring f_t modulo p yields

$$f_t(x) \equiv (x^2+9)^2 (\mathrm{mod}\, p).$$

The factor x^2+9 is reducible mod p if and only if $p \equiv 1(\mathrm{mod}\ 4)$ so that -1 is a square modulo p. If $p \equiv 3(\mathrm{mod}\ 4)$, then x^2+9 is irreducible mod p. Since $\mathbb{Q}(\theta_t)$ is monogenic with ring of integers $\mathbb{Z}[\theta_t]$ we have $\mathrm{ind}(\theta_t) \not\equiv 0(\mathrm{mod}\, p)$. Applying Theorem 1.123 we find that $\langle p\rangle = \wp^2$ if $p \equiv 3(\mathrm{mod}\ 4)$ while $\langle p\rangle = \wp_1^2\wp_2^2$ if $p \equiv 1(\mathrm{mod}\ 4)$, where $\wp, \wp_1$, and $\wp_2$ are prime ideals.

Turning to the cubic field defined by $g_t(x)$ and again using Theorem 3.4, we see that the prime ideal factorization of $\langle p\rangle$ has the form

$$\langle p\rangle = P_1P_2P_3.$$

Thus in L we have the possible factorizations

$$\langle p \rangle = (\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3)^2$$

or

$$\langle p \rangle = (\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4\mathfrak{p}_5\mathfrak{p}_6)^2,$$

according to whether $p \equiv 3 (\text{mod } 4)$ or $p \equiv 1 (\text{mod } 4)$. Therefore, depending on whether $p \equiv 3 (\text{mod } 4)$ or $p \equiv 1 (\text{mod } 4)$, the decomposition group of a prime ideal in L lying above $\langle p \rangle$ is isomorphic to either the Sylow 2-subgroup or the cyclic group of order 2, both of which are contained in the 2-cover.

Case 3: Finally we treat the prime divisors of $t^2 + 108$ which we recall are not equal to 2 or 3. The identity

$$432 f_t(x) - (2x + t)(6x - t)^3 = (t^2 + 108)(72x^2 - 16xt + t^2 + 324)$$

shows that modulo p, $f_t(x)$ has two roots of multiplicities 1 and 3. Using Theorem 1.123 we see that the prime ideal factorization of $\langle p \rangle$ in $\mathbb{Q}(\theta_t)$ has the form

$$\langle p \rangle = \wp_1 \wp_2^3. \tag{2}$$

Theorem 3.4 implies that the prime ideal factorization of $\langle p \rangle$ in the cubic field defined by $g_t(x)$ has the form

$$\langle p \rangle = P^3. \tag{3}$$

The prime ideal factors of $\langle p \rangle$ in L each have the same ramification index e and inertial degree (see Narkiewicz [Nar90, Theorem 4.6]). We see that e must be divisible by 3 from equation (3) forcing $\wp_1$ in equation (2) to have the factorization

$$\wp_1 = \mathfrak{p}_1^3$$

in the normal relative cubic extension $L/\mathbb{Q}(\theta_t)$. Equality of inertial degrees ensures that $\wp_2$ does not remain prime in $L/\mathbb{Q}(\theta_t)$, while equality of

ramification indices implies that $\wp_2$ does not ramify in $L/\mathbb{Q}(\theta_t)$. The only remaining possibility for the prime ideal factorization of $\wp_2$ in $L/\mathbb{Q}(\theta_t)$ is

$$\wp_2 = \mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4$$

so that the final factorization of $\langle p \rangle$ is

$$\langle p \rangle = (\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4)^3$$

Thus in this case the decomposition group of a prime ideal lying above $\langle p \rangle$ is isomorphic to the Sylow 3-subgroup which is contained in the 2-cover. Since the decomposition groups of the prime ideals in L lying above $\langle p \rangle$ are contained in the 2-cover for each of the three possible cases, we conclude that $f(x)$ is intersective. □

We finish by summarizing the decomposition groups in the following table, using the notation C_n to denote the cyclic group of order n.

Table 3.1: Decomposition groups of the ramified primes in L

p (prime) in $\mathbb{N}$	Factorization of $\langle p \rangle$ in L	Decomposition Group
$p = 2$	$\langle 2 \rangle = (\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3)^4$	$C_2 \times C_2$
$p \mid t$ $p \equiv 1 (\mathrm{mod}\ 4)$	$\langle p \rangle = (\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4\mathfrak{p}_5\mathfrak{p}_6)^2$	C_2
$p \mid t$ $p \equiv 3 (\mathrm{mod}\ 4)$	$\langle p \rangle = (\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3)^2$	$C_2 \times C_2$
$p \mid t^2 + 108$	$\langle p \rangle = (\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4)^3$	C_3

Below are some examples of intersective polynomials obtained from our theorem.

Table 3.2: Examples of intersective polynomials with Galois group A_4

t	$t(t^2+108)$	Intersective Polynomial
1	109	$(x^4+18x^2-4x+82)(x^3-109x+436)$
5	$5\cdot 7\cdot 19$	$(x^4+18x^2-20x+106)(x^3-133x+532)$
7	$7\cdot 157$	$(x^4+18x^2-28x+130)(x^3-157x+628)$
11	$11\cdot 229$	$(x^4+18x^2-44x+202)(x^3-229x+916)$

3.2 Intersective Polynomials with Galois Group D_5

3.2.1 Introduction

In this section, we study dihedral quintic trinomials and give necessary and sufficient conditions under which they give rise to intersective polynomials. Infinite families of intersective polynomials with Galois group D_5, the dihedral group of order 10 are given in [LSY14]. In the previous chapter, the number field was monogenic and we were able to take advantage of a theorem of Dedekind (Theorem 1.123) for ideal factorization. However, the number fields defined by dihedral quintic trinomials we consider in this chapter are not monogenic and hence we will need a different approach.

For the family of polynomials in this section, the intersective property is investigated by appealing to the formula for the field discriminant of the quintic number fields defined by these trinomials, as given in [SW02]. We will also employ the theory of ideal factorization in dihedral fields of prime degree as described in [Coh99]. In this section, we briefly summarize the information we need on field discriminants, while in Section 3.2.2, we study the decomposition groups associated with our family of trinomials. In Section 3.2.3, we prove our theorem, and in Section 3.2.4, we provide a method of construction for intersective polynomials and show that we can obtain infinitely many such polynomials.

Algebraic Preliminaries

In this section, we give the algebraic preliminaries and results on field discriminants required to study our intersective polynomials. We recall the parametrization of trinomials x^5+ax+b with a solvable Galois group given in [RYZ82] or [Web79, p. 376]. Explicitly, if a and b are rational numbers and the Galois group of x^5+ax+b is solvable, then a and b are given by

$$a = \frac{5^5\lambda\mu^4}{(\lambda-1)^4(\lambda^2-6\lambda+25)}$$
$$b = \frac{5^5\lambda\mu^5}{(\lambda-1)^4(\lambda^2-6\lambda+25)}$$

with λ, $\mu \in \mathbb{Q}$, $\lambda \neq 1$, $\mu \neq 0$. Parametrizing the values of λ for which the discriminant of x^5+ax+b is equal to a square restricts us to trinomials with Galois group D_5. Making the change of variables

$$\lambda = 5\frac{u+1}{u-1},\ \frac{5\mu}{\lambda-1} = v,$$

now makes the discriminant of x^5+ax+b equal to

$$D = \frac{5^6(u+1)^4(2u^3+4u^2+11u+8)^2}{2^4(u^2+4)^5}v^{20}.$$

This discriminant is a perfect square if and only if u^2+4 is a perfect square. Therefore, setting $u = \beta - 1/\beta$ for some $\beta \in Q$ and setting $\alpha = v/(\beta^2+1)$, then letting $\beta = m/n$ for $m, n \in \mathbb{Z}$ and $d = 2n^2/\alpha$, we obtain the following presentation up to scaling.

For the irreducible dihedral quintic $x^5+ax+b \in \mathbb{Z}[x]$, there exist coprime integers m and n, and integers i, $j = 0$ or 1, such that

$$\begin{aligned} a &= 2^{2-4i}5^{1-4j}d_2(m^2-mn-n^2)E^2F, \\ b &= 2^{4-5i}5^{-5j}d_1(2m-n)(m+2n)E^3F \end{aligned} \tag{2}$$

where d_1^2 is the largest square dividing m^2+n^2, d_2^5 is the largest fifth power

dividing $m^2 + mn - n^2$, and

$$E = (m^2 + n^2)/d_1^2, \qquad F = (m^2 + mn - n^2)/d_2^5.$$

The choice of i and j, as well as the values of E and F, ensures that the resulting polynomial $x^5 + ax + b$ satisfies the condition that there does not exist a prime number p such that

$$p^4 \mid a \qquad \text{and} \qquad p^5 \mid b.$$

This condition is required, for example, when calculating field discriminants of trinomials which can be seen in more detail in Llorente, Nart, and Vila [LNV84]. If it were the case that $p^4 \mid a$ and $p^5 \mid b$, then we could rewrite our quintic in the form

$$x^5 + p^4cx + p^5d$$

for integers c and d and substitute $x = px$ to obtain

$$p^5x^5 + p^5cx + p^5d$$

which, after dividing by p^5, becomes

$$x^5 + cx + d.$$

For a dihedral quintic polynomial $f(x)$ of prime degree with root θ and number field $K = \mathbb{Q}(\theta)$, the field discriminant has the form

$$\left(d(k)f^2\right)^{(p-1)/2} \tag{3}$$

where k is the quadratic subfield of the splitting field L of $f(x)$ while the integer f is called the conductor of L/k [Coh99, p. 491]. We require some facts about the discriminants of the quintic fields defined by the trinomials defined earlier in this chapter. We recall from [SW02] the following two Propositions giving the discriminant of K.

Proposition 3.5. *If θ is a root of a dihedral quintic trinomial as parametrized*

by (2) and $K = \mathbb{Q}(\theta)$, then the discriminant of the field K is given by

$$d(K) = 2^{\alpha}5^{\beta} \prod_{\substack{p\neq 2,5 \\ p|E}} p^2 \prod_{\substack{p\neq 2,5 \\ p|F}} p^4 \tag{4}$$

where

$$\alpha = \begin{cases} 4 & \text{if } m \equiv n+1 \pmod 2 \\ 6 & \text{if } m \equiv n \equiv 1 \pmod 2 \end{cases}$$

and

$$\beta = \begin{cases} 0 & m \equiv 3n \pmod 5, E \equiv 0 \pmod 5 \\ & \text{or} \\ & m \equiv 2n \pmod 5, m \equiv 57n \pmod{125}, E \equiv 0 \pmod 5. \\ 2 & m \equiv 3n \pmod 5, E \not\equiv 0 \pmod 5 \\ & \text{or} \\ & m \equiv 2n \pmod 5, m \equiv 57n \pmod{125}, E \not\equiv 0 \pmod 5 \\ 6 & m \not\equiv 2n, 3n \pmod 5 \\ & \text{or} \\ & m \equiv 2n \pmod 5, m \not\equiv 57n \pmod{125}, E \not\equiv 0 \pmod 5 \\ 8 & m \equiv 2n \pmod 5, m \not\equiv 57n \pmod{125}, E \equiv 0 \pmod 5 \end{cases}$$

Proposition 3.6. *With the same notation as the previous proposition, we have*

$$d(K) = d(k)^2 f^4 \tag{5}$$

where

$$f = 5^{\theta} \prod_{1\leq v_p(b)\leq v_p(a)} p,$$

and

$$\theta = \begin{cases} 0 & \text{if } 5 \nmid a \text{ or } 5^2 \parallel a, 5^3 \mid b. \\ 1 & \text{if } 5 \parallel a, 5 \nmid b \text{ or } 5^2 \parallel a, 5^2 \parallel b. \\ 2 & \text{if } 5^4 \parallel a, 5^4 \parallel b. \end{cases}$$

3.2.2 The Decomposition Groups

In this section, we treat four different cases (in order) of the decomposition groups of the prime ideals lying above the rational primes: $p = 2$, $p = 5$, $p \mid E$ and $p \mid F$. Proposition 3.5 shows that these cover all cases of ramified primes. If we intend to show that a particular decomposition group is cyclic, then it suffices to show that it is a proper subgroup of D_5 since the two proper cyclic subgroups of D_5 form our 2-cover. Equivalently, we show that there is more than one prime ideal lying above p. This is deduced by a theorem of Narkiewicz [Nar90, Theorem 6.5]. By knowing the factorization of the prime ideals in the splitting field, we can use the theorem below to find the index of the decomposition group and thus know whether or not the decomposition group lies within our cover.

Theorem 3.7. *If L/K is a normal extension of an algebraic number field, G its Galois group, $\mathfrak{p}$ a prime ideal of O_K, and P a prime ideal of lying above $\mathfrak{p}$, then the index of the decomposition group of the ideal P is equal to the number of prime ideals lying above $\mathfrak{p}$ in L.*

We now state some theory from Cohen [Coh99], where we have altered the notation to match our own. Recall that L is the normal closure of the quintic, dihedral extension K and the quadratic extension $k = \mathbb{Q}(\sqrt{t})$, and the integer $f(L/k)$ is the conductor of L/k, which provides a quantitative measure of the ramification within the extension. Also, the odd prime number l is the degree of the number field extension $K/\mathbb{Q}$ (in our case, $l = 5$).

Proposition 3.8. *[Coh99, Prop. 10.1.26(9)] If p is totally ramified in $L/\mathbb{Q}$, in other words if $\langle p \rangle = P^{2l}$ for some prime ideal P, then p is totally ramified in $K/\mathbb{Q}$, and in addition, $p \mid l$.*

Proposition 3.9. *[Coh99, Prop. 10.1.28(2)] The ideal p is totally ramified in $K/\mathbb{Q}$ if and only if $p \mid f$.*

Lemma 3.10. *Let $\mathfrak{p}$ be a prime ideal lying above 2 in the splitting field of a dihedral quintic trinomial. Then the decomposition group $G(\mathfrak{p})$ is cyclic.*

Proof. By way of contradiction, assume that there is only one prime ideal lying above 2. It was shown in [SWY07] that the prime 2 is a common index divisor of K and that 2 ramifies in the unique quadratic subfield of L. This implies that 2 ramifies in K as well since by Proposition 3.6, $2 \mid d(K)$. Because there is only one prime ideal lying above 2, we deduce that 2 is totally ramified in L. This contradicts Proposition 3.8 as $2 \nmid 5$. Hence $G(\mathfrak{p})$ is cyclic. □

Lemma 3.11. *Let K be the number field defined by a dihedral quintic trinomial. Let $\mathfrak{p}$ be a prime ideal lying above 5 in the splitting field of the trinomial. Set $\beta = v_5(d(K))$ and recall that $k = \mathbb{Q}\left(\sqrt{t}\right)$ is the quadratic subfield of the splitting field L of $f(x)$. Then the decomposition group $G(\mathfrak{p})$ is cyclic if and only if*

$$\beta = 2, 4$$

or

$$\beta = 8 \text{ and } \left(\frac{t}{5}\right) = +1.$$

Proof. We treat cases according to the power β of 5 in the discriminant of K as given in Proposition 3.5. According to Proposition 3.5, $\beta \in \{0, 2, 6, 8\}$.

Case 1: If $\beta = 0$ then 5 is unramified in L as it is unramified in both K and the quadratic field k. Thus for a prime ideal $\mathfrak{p}$ lying above 5, the decomposition group $G(\mathfrak{p})$ is cyclic and contained in the 2-cover.

Case 2: Next suppose $\beta = 2$. It was shown in the proof of Proposition 4.2 of [SW02] that the prime ideal decomposition of 5 in K is given by

$$\langle 5 \rangle = P_1 P_2^2 P_3^2.$$

Thus more than one prime ideal lies above 5 in L so that for a prime ideal $\mathfrak{p}$ lying above 5, the decomposition group $G(\mathfrak{p})$ is cyclic.

Case 3: Next we treat the case $\beta = 6$. Referring to (5) with $p = 5$, since $5^6 \mid\mid d(K)$ and $d(k)$ is free of odd squares, we deduce that $5 \mid f$. Using Proposition 3.9, we see that 5 is totally ramified in K. Further, from Proposition 3.6, we deduce that $5 \mid d(k)$ so that 5 ramifies in k. Hence 5 is totally ramified in L so that there is only one prime ideal lying above 5 in L. The decomposition group for this prime ideal is all of D_5, which is not cyclic and not contained in the 2-cover.

Case 4: The remaining case is $\beta = 8$. The discriminant formula in Proposition 3.6 implies that

$$5 \nmid d(k), \qquad 5 \mid f,$$

so that 5 is unramified in k and by Proposition 3.9, 5 is totally ramified in K. Thus one prime ideal in L lies over 5 if and only if the ideal $\langle 5 \rangle$ remains prime in k. By Theorem 1.121, this occurs precisely when

$$\left(\frac{t}{5}\right) = -1,$$

showing that the associated decomposition group is all of D_5, so is not cyclic. In the situation where $\langle 5 \rangle$ splits in k, showing that two prime ideals lie above 5 in L, the decomposition groups are cyclic. This occurs precisely when

$$\left(\frac{t}{5}\right) = +1,$$

proving the lemma. □

For the next two lemmas, we note the easily proved statement that if $p \neq 2, 5$ is a prime, then p cannot divide both E and F.

Lemma 3.12. *Suppose that $p \neq 2, 5$ is a prime such that $p \mid E$. Then the decomposition group of a prime $\mathfrak{p}$ lying above p is cyclic.*

Proof. The hypothesis in this lemma implies that p ramifies in k so that

$$\langle p \rangle = \wp^2,$$

and it follows from Proposition 3.5 that $p \mid d(K)$ so p ramifies in K. If only one prime ideal lies above p in L then this is also true in K so that p is totally ramified in K. In conclusion, p is totally ramified in L which is impossible by Proposition 3.8 as $p \neq 5$. Hence the factorization of $\wp$ in L contains more than one prime ideal, implying that the decomposition group of each such prime is a proper subgroup of D_5 and is hence cyclic. □

Lemma 3.13. *Suppose that $p \neq 2, 5$ is a prime such that $p \mid F$. Then the decomposition group of a prime $\mathfrak{p}$ lying above p is cyclic if and only if*

$$\left(\frac{t}{p}\right) = +1.$$

Proof. Certainly p is not ramified in k so it either splits or remains prime. However we see from Proposition 3.5 and 3.6 that $p \mid f$, so that by Proposition 3.9, p is totally ramified in K. Thus more than one prime ideal in L lies over p if and only if p splits in k, or equivalently

$$\left(\frac{t}{p}\right) = +1.$$

In this case, the decomposition group is contained in a conjugate of the 2-cover of D_5 so it is cyclic. □

3.2.3 Proof of Theorem

For a rational prime p and a nonzero integer n, the notation $v_p(n) = a$ means that we have $p^a \parallel n$, that is, $p^a \mid n$ but $p^{a+1} \nmid n$. Utilizing this notation, we now state our main theorem.

Theorem 3.14. *Let $f(x) = x^5 + ax + b \in \mathbb{Z}[x]$ have Galois group D_5. Let θ be a root of $f(x)$. Set $K = \mathbb{Q}(\theta)$. Let $d(K)$ denote the field discriminant of K. Let t be the unique, squarefree integer such that $k = \mathbb{Q}\left(\sqrt{t}\right)$ is the*

quadratic subfield of the splitting field L of $f(x)$. Then the polynomial

$$\left(x^5 + ax + b\right)\left(x^2 - t\right) \tag{1}$$

is intersective with Galois group D_5 if and only if

$$v_5(d(K)) \neq 6$$

and

$$\text{if } v_5(d(K)) = 8 \text{ then } \left(\frac{t}{5}\right) = +1,$$

and for all primes $p > 5$

$$\text{if } p^4 \mid d(K) \text{ then } \left(\frac{t}{p}\right) = +1.$$

Proof. Suppose that $(x^5 + ax + b)(x^2 - t)$ is intersective. Then for any prime ideal in L, the decomposition group is cyclic. Lemma 3.11 shows that $v_5(d(K)) \neq 6$ and if $v_5(d(K)) = 8$ then

$$\left(\frac{t}{5}\right) = +1.$$

For any prime with $p^4 \mid d(K)$, we have $p \mid F$ and Lemma 3.13 shows that if a prime ideal lying above p in L has a cyclic decomposition group, then

$$\left(\frac{t}{p}\right) = +1.$$

Conversely, we show that all decomposition groups are cyclic. This is certainly the case for prime ideals in L lying above an unramified rational prime p. If $p = 2$, then Lemma 3.10 shows that any associated decomposition groups are cyclic. If $p = 5$, then Lemma 3.11, combined with the conditions on 5 stated in the theorem, show that any associated decomposition groups are cyclic. Lemma 3.12 shows that for any prime $p > 5$ with $p \mid E$, all associated decomposition groups are cyclic. Finally, Lemma 3.13, combined with the stated conditions on primes dividing F, equivalently $p > 5$ and

$p^4 \mid d(K)$, ensures that all decomposition groups are cyclic. Thus $(x^5+ax+b)(x^2-t)$ is intersective and clearly has Galois group D_5. □

3.2.4 Examples

We first begin by giving some examples illustrating our main theorem in the following table. Note that the chosen values of a and b satisfy (2).

Table 3.3: Parameter Values and Their Associated Polynomials

m	n	$d(K)$	$(x^5+ax+b)(x^2-t)$			Intersective Yes/No?	Reason
			a	b	t		
1	1	$2^6 \cdot 5^6$	-5	12	-10	No	$v_5(d(K)) = 6$ Insolvable in $\mathbb{Q}_5$
3	1	$2^6 \cdot 11^4$	11	44	-2	Yes	$v_5(d(K)) = 0, \left(\frac{-2}{11}\right) = +1$ Has a root in $\mathbb{Q}_p$ $\forall$ prime p
1	0	$2^4 \cdot 5^6$	20	32	-5	No	$v_5(d(K)) = 6$ Insolvable in $\mathbb{Q}_5$
2	11	$2^4 \cdot 19^4$	10564	51072	-1	No	$v_5(d(K)) = 0$, but $\left(\frac{-1}{19}\right) = -1$ Insolvable in $\mathbb{Q}_{19}$
1	7	$2^6 \cdot 5^2 \cdot 41^4$	11275	61500	-10	Yes	$v_5(d(K)) = 2, \quad \left(\frac{-10}{41}\right) = +1$ Has a root in $\mathbb{Q}_p$ $\forall$ prime p
11	3	$2^6 \cdot 5^8 \cdot 13^2 \cdot 29^4$	241986875	51448247500	-26	No	$v_5(d(K)) = 8, \left(\frac{-26}{5}\right) = +1$, but $\left(\frac{-26}{29}\right) = -1$ Insolvable in $\mathbb{Q}_{29}$
6	13	$2^4 \cdot 5^8 \cdot 11^4 \cdot 41^2$	9754002500	242601920000	-41	Yes	$v_5(d(K)) = 8, \left(\frac{-41}{5}\right) = +1, \left(\frac{-41}{11}\right) = +1$ Has a root in $\mathbb{Q}_p$ $\forall$ prime p

We now show that infinitely many intersective polynomials can be constructed using our theorem. In [RYZ82, Example 4], Roland, Yui and Zagier derived an infinite set of dihedral quintic trinomials with $F = f = 1$. Using formula (5) in Proposition 3.6 with $f = 1$ and the fact that $v_p(d(k)) \leq 1$ for an odd prime, we can easily deduce that the conditions of our main theorem are satisfied. This gives the following corollary to our theorem.

Corollary 3.15. *Suppose that m, n are given by*

$$m = f(r,s),\ n = f(s,-r),$$

or

$$m = -f(r,s) + 2f(s,-r),\ n = 2f(r,s) + f(s,-r),$$

for integers r, s with

$$f(r,s) = 2r^5 - 5r^4s + 10r^3s^2 + 5rs^4 + s^5$$

and

$$\Delta(r,s) = (f(r,s)^2 + f(s,-r)^2)/5.$$

Then with a and b given by (2) we have

$$(x^5 + ax + b)(x^2 + \Delta(r,s))$$

is intersective if

$$r \not\equiv 2s (\text{mod } 5),$$

while

$$(x^5 + ax + b)(x^2 + 5\Delta(r,s))$$

is intersective if

$$r \equiv 3s (\text{mod } 5).$$

Using the examples following Theorem 2 in [RYZ82], in the following table we give the values of r, s, m, and n, the corresponding quadratic subfield k, the field discriminant $d(K)$, and the intersective polynomial produced by our Corollary. The values in this table were produced with the help of the computer algebra software Maple$^{\text{TM}}$.

Table 3.4: Intersective Polynomials Produced Using Corollary

r	s	m	n	k	$d(K)$
1	1	13	21	$\mathbb{Q}(\sqrt{-2 \cdot 61})$	$(2^3 \cdot 61)^2$
1	2	144	233	$\mathbb{Q}(\sqrt{-5 \cdot 3001})$	$(2^2 \cdot 5 \cdot 3001)^2$
1	2	322	521	$\mathbb{Q}(\sqrt{-3001})$	$(2^2 \cdot 3001)^2$
1	4	2446	3987	$\mathbb{Q}(\sqrt{-17 \cdot 257401})$	$(2^2 \cdot 17 \cdot 257401)^2$
1	5	6477	10649	$\mathbb{Q}(\sqrt{-13 \cdot 1195021})$	$(2^3 \cdot 13 \cdot 1195021)^2$
1	7	29269	49083	$\mathbb{Q}(\sqrt{-2 \cdot 13063261})$	$(2^3 \cdot 13063261)^2$
1	7	68897	107621	$\mathbb{Q}(\sqrt{-2 \cdot 13063261})$	$(2^3 \cdot 5 \cdot 13063261)^2$
2	3	1597	2584	$\mathbb{Q}(\sqrt{-13 \cdot 141961})$	$(2^2 \cdot 13 \cdot 141961)^2$
2	5	11039	17868	$\mathbb{Q}(\sqrt{-29 \cdot 41 \cdot 74201})$	$(2^2 \cdot 29 \cdot 41 \cdot 74201)^2$
3	1	367	269	$\mathbb{Q}(\sqrt{-2 \cdot 5 \cdot 41 \cdot 101})$	$(2^3 \cdot 5 \cdot 41 \cdot 101)^2$
3	1	171	1003	$\mathbb{Q}(\sqrt{-2 \cdot 41 \cdot 101})$	$(2^3 \cdot 41 \cdot 101)^2$
3	2	1028	1591	$\mathbb{Q}(\sqrt{-13 \cdot 55201})$	$(2^2 \cdot 13 \cdot 55201)^2$
4	3	5831	9242	$\mathbb{Q}(\sqrt{-61 \cdot 15661})$	$(2^2 \cdot 61 \cdot 15661)^2$
4	3	12653	20904	$\mathbb{Q}(\sqrt{-61 \cdot 15661})$	$(2^2 \cdot 5 \cdot 61 \cdot 15661)^2$
5	1	4401	277	$\mathbb{Q}(\sqrt{-2 \cdot 13 \cdot 101 \cdot 1481})$	$(2^3 \cdot 13 \cdot 101 \cdot 1481)^2$
5	4	21174	33823	$\mathbb{Q}(\sqrt{-41 \cdot 821 \cdot 9461})$	$(2^2 \cdot 41 \cdot 821 \cdot 9461)^2$
8	1	50217	-11606	$\mathbb{Q}(\sqrt{-5 \cdot 13 \cdot 8173681})$	$(2^2 \cdot 5 \cdot 13 \cdot 8173681)^2$
8	1	-73429	88828	$\mathbb{Q}(\sqrt{-13 \cdot 8173681})$	$(2^2 \cdot 13 \cdot 8173681)^2$

$(x^5 + ax + b)(x^2 - t)$		
a	b	t
-405589	9987164	-122
12086953942100	-72540492158684000	-15005
-12086737798076	72550005665852352	-75025
3313637326184074053956	-505677611146965620655322432	-4375817
128783546396420228711099	-384062273485624077484287261 40	-31070546
418267520774122024034953 1	-214879534985497860209804087 5540	-26126522
-249258207513090566888938 2725	955595633888663521123313344465 3500	-130632610
-22487550931996197164	16600257189596220550773792	-1845493
270320409023732030523239 24	-865467381892883289812868813246 40	-88224989
-34325342094725	597650406547546500	-41410
216596445368171	408729111659573348	-207050
-14093859584995428524	463005250073880374039712	-717613
-1460789163238843866236	164167653953588413305312960	-955321
938754748284345136870100	-418035937984409159057821684000	-4776605
396367183999732006139	49695536440652420291999740	-3889106
-33219802329664023939936 71356	156522688692545824263299014254 53120	-318466721
476153875778542065173992 76900	290395831685848919478209698254 032000	-531289265
-129030862586096816582700 11564	471538454128083451015339001654 246304	-2656446325

Chapter 4

The Holomorph $\mathbb{Z}_{2^e} \rtimes \mathbb{Z}_{2^e}^*$

4.1 Introduction

Jacobson and Vélez [JV90] determined the Galois group of an irreducible binomial $x^{2^e} - a$ over $\mathbb{Q}$ for integers e and a with $e \geq 3$. This Galois group is a full subgroup of the holomorph of the cyclic group of order 2^e. Explicitly, this holomorph is the set $\mathbb{Z}_{2^e} \times \mathbb{Z}_{2^e}^*$ with binary operation given by

$$(\alpha, u)\,(\beta, v) = (\alpha + u\beta, uv)\,,$$

which we recognize as $\mathbb{Z}_{2^e} \rtimes \mathbb{Z}_{2^e}^*$, the semi-direct product of the cyclic group $\mathbb{Z}_{2^e}$ with $\mathbb{Z}_{2^e}^*$. A subgroup of $\mathbb{Z}_{2^e} \rtimes \mathbb{Z}_{2^e}^*$ is full if the projections onto $\mathbb{Z}_{2^e}$ and $\mathbb{Z}_{2^e}^*$ are surjective. If θ is a root of $x^{2^e} - a$, $\zeta = \exp(2\pi i/2^e)$, and the Galois group of $x^{2^e} - a$ is $\mathbb{Z}_{2^e} \rtimes \mathbb{Z}_{2^e}^*$, then the automorphism (α, u) of the splitting field $\mathbb{Q}\,(\theta, \zeta)$ of $x^{2^e} - a$ is defined by

$$(\alpha, u)(\theta) = \zeta^\alpha \theta \qquad \text{and} \qquad (\alpha, u)(\zeta) = \zeta^u.$$

The group $\mathbb{Z}_{2^e}^*$ is not cyclic but is generated by the residue classes $\{-1, 5\}$ modulo 2^e. We shall use $\mathcal{G}$ to denote this holomorph. There are two purposes to this paper. First we give an n-cover of $\mathcal{G}$, that is a collection of proper subgroups of $\mathcal{G}$, the union of whose conjugates equals $\mathcal{G}$, and whose intersection is trivial. We show that $\mathcal{G}$ has a 3-cover. Then we use our 3-cover to produce a new family of intersective polynomials with Galois group $\mathcal{G}$. Such polynomials are monic, have integer coefficients, and have no rational root but have roots with respect to every modulus. Equivalently these polynomials have a root in every p-adic field $\mathbb{Q}_p$.

Without loss of generality and for convenience, we shall impose a scaling condition on our binomials; namely, we shall assume that our binomial $x^{2^e}-a$ has the property that for any prime number p we have

$$p^{2^e} \nmid a. \tag{1}$$

Scaling polynomials will not alter the property of their being intersective nor of course their Galois group. We state our main theorems now.

Theorem 4.1. *Let e be an integer with $e \geq 3$. Let $\mathcal{G}$ be the group*

$$\mathcal{G} \simeq \mathbb{Z}_{2^e} \rtimes \mathbb{Z}_{2^e}^*.$$

The subgroups $\{H_1, H_2, H_3\}$ of $\mathcal{G}$ defined by

$$H_1 = \left\{(b, 5^c) : b = 0, 1, \ldots, 2^e - 1,\ c = 0, 1, \ldots, 2^{e-2} - 1\right\},$$

$$H_2 = \{(0, d) : d = 1, 3, \ldots, 2^e - 1\},$$

$$H_3 = \langle (1, -1), (3, -5) \rangle,$$

form a 3-cover of $\mathcal{G}$.

We note that the elements $(1, -1)$, $(3, -5)$ commute in $\mathcal{G}$ and a simple calculation shows that H_3 has order 2^e.

Theorem 4.2. *Let a be an integer satisfying the scaling assumption (1). The polynomial*

$$\left(x^{2^e} - a\right)(x^2 + 1)\left(x^{2^{e-1}} + a\right)$$

is intersective and has Galois group $\mathcal{G} \simeq \mathbb{Z}_{2^e} \rtimes \mathbb{Z}_{2^e}^*$ if and only if

$$a \neq \pm d^2, \pm 2d^2$$

for all integers d, and

$$\text{if } \ p \mid a,\ p \equiv 3 (\text{mod } 4) \text{ then } p^{2^{e-1}} \parallel a \text{ and } \left(\frac{-a/p^{2^{e-1}}}{p}\right) = 1, \tag{a}$$

and one of the following conditions holds.

$$a \equiv 1 (\text{mod } 2^{e+2}), \tag{b}$$

$$a \equiv -1 (\text{mod } 2^{e+1}),$$

or

$$2^{2^{e-1}} \parallel a \text{ and } a/2^{2^{e-1}} \equiv -1 (\text{mod } 2^{e+1}).$$

For examples of polynomials that are intersective or non-intersective (with reason), refer to the table at the end of this chapter.

In Section 4.2, we use a theorem of Jacobson and Vélez [JV90] to determine binomials $x^{2^e} - a$ with Galois group $\mathcal{G}$. In Section 4.3, we derive the properties of the subgroups for our 3-cover of $\mathcal{G}$. Finally, in Sections 4.4 and 4.5 we prove Theorems 4.1 and 4.2.

4.2 Binomials $x^{2^e} - a$ with Galois group $\mathcal{G}$

For two algebraic number fields K and L we denote their compositum by KL.

Proposition 4.3 ([DF04], Corollary 20, pg. 592)**.** *If K and L are number fields and $K/\mathbb{Q}$ is Galois then*

$$[KL : \mathbb{Q}] = \frac{[K : \mathbb{Q}] \cdot [L : \mathbb{Q}]}{[K \cap L : \mathbb{Q}]} \tag{2}$$

Lemma 4.4. *Let a, e be integers with $e \geq 3$. The binomial*

$$x^{2^e} - a$$

is irreducible over $\mathbb{Q}$ and has Galois group

$$\mathcal{G} \simeq \mathbb{Z}_{2^e} \rtimes \mathbb{Z}_{2^e}^*$$

if and only if

$$a \neq \pm d^2, \ \pm 2d^2$$

for all integers d.

Proof. Let $\zeta = \exp(2\pi i/2^e)$ and θ be a root of $x^{2^e} - a$. Set $K = \mathbb{Q}(\zeta)$ and $L = \mathbb{Q}(\theta)$. We note that $K/\mathbb{Q}$ is Galois. Suppose that $x^{2^e} - a$ is irreducible over $\mathbb{Q}$ and has Galois group $\mathcal{G}$. Irreducibility implies that $a \neq d^2$ for all integers d. The splitting field of $x^{2^e} - a$ is the compositum of K and L, thus we have

$$|\mathcal{G}| = 2^{2e-1} = [KL : \mathbb{Q}] = 2^e \cdot 2^{e-1} = [K : \mathbb{Q}] \cdot [L : \mathbb{Q}]. \tag{3}$$

If $a = -d^2$, (respectively, $-2d^2, 2d^2$) then

$$\left(\frac{\theta^{2^{e-1}}}{d}\right)^2 = -1, (\text{respectively } \left(\frac{\theta^{2^{e-1}}}{d}\right)^2 = -2, \ \left(\frac{\theta^{2^{e-1}}}{d}\right)^2 = 2),$$

so that

$$K \cap L \supseteq \mathbb{Q}(\sqrt{-1}), \ (\text{respectively } \mathbb{Q}(\sqrt{-2}), \ \mathbb{Q}(\sqrt{2})).$$

Equation (2) now shows that (3) is impossible. Thus $a \neq \pm d^2, \pm 2d^2$ for all integers d.

Now suppose that $a \neq \pm d^2, \pm 2d^2$ for all integers d. Irreducibility is deduced from the Vahlen-Capelli Theorem [Cap01], [Vah95], which states that $x^n - a$ is reducible over $\mathbb{Q}$ if and only if for some prime $p > 1$, $p \mid n$ and $a = b^p$ or $4 \mid n$ and $a = -4b^4$, for some integer b. Both possibilities are ruled out by assumption. We determine the Galois group of $x^{2^e} - a$ by a degree argument. Since

$$\sqrt{a} = \pm\theta^{2^{e-1}}$$

we deduce that

$$\sqrt{a} \in L.$$

Using [Wei09, Corollary 4.5.4], we see that the quadratic subfields of $\mathbb{Q}(\zeta)$ are precisely

$$\mathbb{Q}(\sqrt{-1}), \ \ \mathbb{Q}(\sqrt{-2}), \ \ \text{and} \ \ \mathbb{Q}(\sqrt{2}).$$

Since $a \neq \pm d^2, \pm 2d^2$ for all integers d, $\sqrt{a}$ does not belong to any of these

quadratic subfields, hence $\sqrt{a}$ does not belong to $\mathbb{Q}(\zeta)$. It follows from [JV90, Theorem A(b)] that the Galois group of $x^{2^e} - a$ is $\mathcal{G}$, completing the proof. □

4.3 n-cover of $\mathcal{G} \simeq \mathbb{Z}_{2^e} \rtimes \mathbb{Z}_{2^e}^*$

Lemma 4.5. *The group*

$$\mathcal{G} \simeq \mathbb{Z}_{2^e} \rtimes \mathbb{Z}_{2^e}^*$$

is not 2*-coverable.*

Proof. Suppose that for two proper subgroups H_1 and H_2 of $\mathcal{G}$, $\{H_1, H_2\}$ is a 2-cover for $\mathcal{G}$. We write

$$|H_1| = 2^a \quad \text{and} \quad |H_2| = 2^b$$

for positive integers a and b. Since these subgroups are proper subgroups of $\mathcal{G}$ and $|\mathcal{G}| = 2^{2e-1}$, we have

$$1 \leq a, b < 2e - 1. \tag{4}$$

The normalizer of H_1 (respectively H_2) strictly contains H_1 (respectively H_2) (see [Fra02, Cor. 36.7]). Consequently the number of conjugates of H_1 and H_2 satisfy

$$|\mathcal{G} : N(H_1)| \leq \frac{2^{2e-1}}{2^{a+1}} = 2^{2e-a-2} \quad \text{and} \quad |\mathcal{G} : N(H_2)| \leq \frac{2^{2e-1}}{2^{b+1}} = 2^{2e-b-2}$$

so that the number of elements in the union of the conjugates of H_1 and H_2, after removing one for the identity element which is counted at least twice, is at most

$$2^a 2^{2e-a-2} + 2^b 2^{2e-b-2} - 1 \leq 2^{2e-1} - 1 < 2^{2e-1}$$

using (4). Hence $\mathcal{G}$ is not 2-coverable. □

In order to give the proof of Theorem 4.1, we need to determine the

conjugates of the subgroups specified in that theorem. The subgroup H_1 is normal, but H_2 and H_3 are not. The next two lemmas determine the conjugates of H_2 and H_3.

Lemma 4.6. *The conjugates of the subgroup*

$$H_2 = \{(0, d) : d = 1, 3, \ldots, 2^e - 1\}$$

of the group

$$\mathcal{G} \simeq \mathbb{Z}_{2^e} \rtimes \mathbb{Z}_{2^e}^*.$$

have the form

$$\{(n(d-1), d) : d = 1, 3, \ldots, 2^e - 1\},$$

where n is a fixed integer modulo 2^e.

Proof. We begin by conjugating a typical element of H_2 with an arbitrary element (k, j) with inverse $(-kj^{-1}, j^{-1})$ in $\mathcal{G}$ which leads us to

$$\begin{aligned}&(-kj^{-1}, j^{-1})(0, d)(k, j)\\ &= (kj^{-1}(d-1), d),\end{aligned}$$

so assuming that

$$kj^{-1} \equiv n (\text{mod } 2^e)$$

we have produced a conjugate of H_2 with elements of the form

$$(n(d-1), d).$$

Reversing this calculation proves the Lemma. □

Lemma 4.7. *The conjugates of the subgroup*

$$H_3 = \langle (1, -1), (3, -5) \rangle$$

of the group

$$\mathcal{G} \simeq \mathbb{Z}_{2^e} \rtimes \mathbb{Z}_{2^e}^*.$$

have the form

$$\langle (m,-1),(3m,-5)\rangle\,,$$

for a fixed odd integer m modulo 2^e.

Proof. Conjugating the generators of H_3 with an arbitrary element (k,j) with inverse $(-kj^{-1},j^{-1})$ in $\mathcal{G}$ gives

$$\begin{aligned}&(-kj^{-1},j^{-1})(3,-5)(k,j)\\&=(3m,-5),\end{aligned}$$

and

$$\begin{aligned}&(-kj^{-1},j^{-1})(1,-1)(k,j)\\&=(m,-1),\end{aligned}$$

where the odd integer m satisfies

$$m\equiv j^{-1}(1-2k)\pmod{2^e}.$$

Furthermore, as j and k can be freely chosen modulo 2^e we conclude that if m is an odd integer modulo 2^e then

$$\langle (m,-1),(3m,-5)\rangle\,,$$

is a conjugate of H_3. □

Now we give the proof of Theorem 4.1.

4.4 Proof of Theorem 4.1

Proof. We begin by showing $\mathcal{G}$ is equal to the union of the conjugates of the subgroups H_i, $i=1,2,3$. For notation, H_i^c denotes a conjugate of H_i. We consider a typical element

$$(k,j)\in\mathcal{G}$$

where k is any integer modulo 2^e and j is any odd integer modulo 2^e. We may write $j = \pm 5^{2a}$ or $\pm 5^{2a+1}$ for a nonnegative integer a. Some of the cases require that we set $k = 2w$ or $k = 2w + 1$. The following table summarizes all of the containments.

Type	1	2	3	4
Element	$(k, 5^a)$	$(2w, -(5)^a)$	$(2w+1, -(5)^{2a+1})$	$(2w+1, -(5)^{2a})$
Belongs to	H_1	H_2^c	H_3^c	H_3^c

Type 1 inclusion is obvious from the definition of H_1. To demonstrate Type 2 inclusion we use Lemma 4.6 and determine n and d from

$$(2w, -(5)^a) = (n(d-1), d).$$

We set $d = -(5)^a$ and determine n from the linear congruence

$$n(-(5)^a - 1) \equiv 2w (\text{mod } 2^e),$$

noting that

$$\gcd((5)^a + 1, 2^e) = 2.$$

For the third type, we use Lemma 4.7 and determine nonnegative integers r and s together with a positive integer m such that

$$(2w+1, -(5)^{2a+1}) = (m, -1)^r (3m, -5)^s.$$

An easy calculation shows that

$$(3m, -5)^{2a+1} = \left(-m \left(\frac{(-5)^{2a+1} - 1}{2} \right), (-5)^{2a+1} \right).$$

We choose $r = 0$, $s = 2a + 1$ and m satisfying the linear congruence

$$-m \left(\frac{(-5)^{2a+1} - 1}{2} \right) \equiv 2w + 1 \text{ (mod } 2^e),$$

noting that $\gcd\left(\left(\frac{(-5)^{2a+1}-1}{2}\right), 2^e\right) = 1$, to complete type 3 containment. For the last case, using Lemma 4.7 and setting $r = 1$, $s = 2a$ we get

$$(m, -1)(3m, -5)^{2a} = \left(m\left(\frac{(-5)^{2a}+1}{2}\right), -(5)^{2a}\right)$$

and determining m from the solvable congruence

$$m\left(\frac{(-5)^{2a}+1}{2}\right) \equiv 2w + 1 (\text{mod } 2^e)$$

establishes the final inclusion.

To establish the result that the intersection of the conjugates of the H_i is trivial, we prove the stronger statement that there are two conjugates of H_2 with trivial intersection. Recalling Lemma 4.6, we choose $n = 1$ and $n = 2$ and compare the conjugate subgroups

$$H_2 = \{((d-1), d) : d = 1, 3, \ldots, 2^e - 1\}$$

and

$$H_2^c = \left\{(2(d'-1), d') : d' = 1, 3, \ldots, 2^e - 1\right\}.$$

Since each second component of these ordered pairs occurs exactly once, an element belonging to the intersection of these two conjugate subgroups must satisfy $d' = d$. Further we deduce from the first component that

$$2(d-1) \equiv d - 1 (\text{mod } 2^e),$$

leading to the conclusion that

$$d \equiv 1 (\text{mod } 2^e).$$

Thus the only element in the intersection of these conjugates is the identity $(0, 1)$, so that

$$\{H_1, H_2, H_3\}$$

yields a 3-cover of $\mathcal{G}$. □

4.5 Proof of Theorem 4.2

We begin by giving defining polynomials for the subfields of the splitting field of $x^{2^e} - a$ corresponding to the subgroups in the 3-cover via Galois theory.

Lemma 4.8. *Suppose that the Galois group of $x^{2^e} - a$ is isomorphic to $\mathbb{Z}_{2^e} \rtimes \mathbb{Z}_{2^e}^*$. Let θ be a root of $x^{2^e} - a$ and suppose that $\zeta = \exp(2\pi i/2^e)$. Let H_1, H_2, and H_3 be the subgroups specified in Theorem 4.1. Let K_1, K_2, and K_3 be the fixed fields corresponding to these subgroups by Galois theory. Then*

$$\begin{aligned} K_1 &= \mathbb{Q}(i) \text{ with defining polynomial } f_1(x) = x^2 + 1, \\ K_2 &= \mathbb{Q}(\theta) \text{ with defining polynomial } f_2(x) = x^{2^e} - a, \\ K_3 &= \mathbb{Q}\left(\zeta\theta^2\right) \text{ with defining polynomial } f_3(x) = x^{2^{e-1}} + a. \end{aligned}$$

Proof. We recall that for a typical element of (k, j) of the Galois group $\mathcal{G}$ that

$$(k, j)(\theta) = \zeta^k \theta \qquad \text{and} \qquad (k, j)(\zeta) = \zeta^j.$$

An easy exercise now shows that the elements i (respectively, θ, $\zeta\theta^2$) are fixed by H_1 (respectively H_2, H_3). Furthermore their degrees over $\mathbb{Q}$ are equal to, in each case, the index of the subgroup under which they are fixed. The result now follows. □

The following result characterizes k-th powers in the p-adic integers, $\mathbb{Z}_p$ (see for example Castillo [Cas11, Lemma 2.7]). We let S_p^k denote the set of nonzero k-th powers in $\mathbb{Z}_p$.

Proposition 4.9. *Let g be a primitive root modulo p. We have*

$$S_p^k = \left\{ p^{km} g^{k\ell} (1 + p^{\varepsilon+1+v_p(k)} c) : m \geq 0, \ell \geq 0, c \in \mathbb{Z}_p \right\},$$

where

$$\varepsilon = \begin{cases} 1 & \text{if } p = 2, \\ 0 & \text{if } p > 2. \end{cases}$$

The following lemma is concerned with power congruences.

Lemma 4.10. *Let p be a prime satisfying $p \equiv 3 (\mathrm{mod}\ 4)$ and suppose that b is an integer not divisible by p. Then the congruence*

$$x^{2^k} \equiv b (\mathrm{mod}\ \ p^\ell)$$

is solvable for all positive integers k and ℓ if and only if b is a quadratic residue modulo p. Equivalently, for all fixed positive integers k, $x^{2^k} - b$ has a root in $\mathbb{Q}_p$ if and only if b is a quadratic residue mod p.

Proof. Setting $k = \ell = 1$ in the assumed solvable congruence shows that b is a quadratic residue modulo p. Conversely, since $p \equiv 3 (\mathrm{mod}\ 4)$ then the quadratic residues modulo p are quartic residues, octic residues and so on. Thus

$$x^{2^k} \equiv b (\mathrm{mod}\ \ p)$$

is solvable for all positive integers k. Furthermore as $p \nmid b$ a standard application of Hensel's Lemma for any fixed integer k now shows that.

$$x^{2^k} \equiv b (\mathrm{mod}\ \ p^\ell)$$

is solvable for all positive integers ℓ. The equivalent statement that $x^{2^k} - b$ has a root in $\mathbb{Q}_p$ is immediate. □

Now we give the proof of Theorem 4.2.

Proof. Suppose that a is an integer satisfying the scaling assumption (1), and set

$$F(x) = (x^{2^e} - a)(x^2 + 1)(x^{2^{e-1}} + a).$$

It follows from Lemma 4.8 that the roots of the second and third factors of $F(x)$ can be expressed in terms of the roots of $x^{2^e} - a$ so that $F(x)$ and $x^{2^e} - a$ have the same Galois group. This Galois group is $\mathcal{G}$ if and only if $a \neq \pm d^2, \pm 2d^2$ for all integers d by Lemma 4.4. To finish we must establish the conditions for $F(x)$ to be intersective. We study solvability of $F(x)$ for

various classes of prime powers by working in $\mathbb{Q}_p$.

Case 1: $p = 2$. The first factor of $F(x)$ is solvable in $\mathbb{Q}_2$ if and only if a is a 2^e-th power in $\mathbb{Q}_2$. Using Proposition 4.9, with $g = 1$, we deduce that

$$a = 2^{2^e m}(1 + 2^{e+2}c)$$

for $c \in \mathbb{Z}$. By the scaling assumption (1), $m = 0$ so that we can write the equivalent statement

$$a \equiv 1 (\text{mod } 2^{e+2})$$

The second factor $x^2 + 1$ clearly has no root in $\mathbb{Q}_2$. We consider the third factor which has a root in $\mathbb{Q}_2$ if and only if $-a$ is a 2^{e-1}-st power in $\mathbb{Q}_2$. Using Proposition 4.9, with $m = 0$ and $g = 1$, we deduce that

$$-a = 2^{2^{e-1}m}(1 + 2^{e+1}c)$$

where $c \in \mathbb{Z}$. From the scaling assumption (1), we see that either $m = 0$ or $m = 1$ so that

$$-a = (1 + 2^{e+1}c) \qquad \text{or} \qquad -a = 2^{2^{e-1}}(1 + 2^{e+1}c)$$

for $c \in \mathbb{Z}$. Thus we have established all the conditions for $p = 2$.

Case 2: $p \equiv 1 (\text{mod } 4)$. Since $\left(\frac{-1}{p}\right) = +1$, a straightforward application of Hensel's Lemma [INM95, p. 87] shows that $x^2 + 1$ is solvable in $\mathbb{Q}_p$.

Case 3: $p \equiv 3 (\text{mod } 4)$. Suppose that $p \nmid a$. We begin by showing that the first or third factor of $F(x)$ always has a root in $\mathbb{Q}_p$. By Lemma 4.10 with $k = e$, the first factor of $F(x)$ is solvable in $\mathbb{Q}_p$ if and only if

$$\left(\frac{a}{p}\right) = 1. \tag{5}$$

Again by Lemma 4.10, with $k = e - 1$, the third factor of $F(x)$ has a root

in $\mathbb{Q}_p$ if and only if

$$\left(\frac{-a}{p}\right) = 1 \qquad \text{so that} \qquad \left(\frac{a}{p}\right) = -1,$$

establishing solvability in $\mathbb{Q}_p$ in this case. Now suppose that $p \mid a$. Writing

$$a = p^t a_1$$

where t is a positive integer and recalling the scaling assumption (1) we deduce that $0 \leq t < 2^e$. The inequality on t combined with Proposition 4.9 shows that a is not a 2^e-th power in $\mathbb{Q}_p$ so that the first factor of $F(x)$ cannot have a root in $\mathbb{Q}_p$. The second factor of $F(x)$ cannot have a root in $\mathbb{Q}_p$ since -1 is not a square modulo p. Thus solvability of $F(x)$ in $\mathbb{Q}_p$ depends on the third factor of $F(x)$. This factor

$$x^{2^{e-1}} + a$$

has a root in $\mathbb{Q}_p$ if and only if $-a$ is a 2^{e-1}-st power in $\mathbb{Q}_p$ which implies that

$$p^{2^{e-1}} \parallel a.$$

Further by Lemma 4.10 with $k = e - 1$ we must have

$$\left(\frac{-a/p^{2^{e-1}}}{p}\right) = 1$$

establishing the conditions in the theorem. □

Below is a table of polynomials for different values of a that uses the conditions stated in Theorem 4.2. Some are intersective and some are not. For those that are not, the reason is provided to the reader.

Table 4.1: Intersective polynomials with Galois group $\mathcal{G} \simeq \mathbb{Z}_{2^e} \rtimes \mathbb{Z}_{2^e}^*$

e	a	$F(x) = (x^{2^e} - a)(x^2 + 1)(x^{2^{e-1}} + a)$
3	65	Intersective
3	33	Not intersective, violates (a), no root in $\mathbb{Q}_3$ or $\mathbb{Q}_{11}$.
3	-17	Intersective
4	$-3^8 \cdot 97$	Intersective
4	41	Not intersective, violates (b), no root in $\mathbb{Q}_2$.
4	-97	Intersective
5	641	Intersective
5	3^{16}	Not intersective, violates (a) and (b), no root in $\mathbb{Q}_2$ or $\mathbb{Q}_3$.
5	-3^{16}	Intersective

Chapter 5

Future Work and Conclusion

5.1 Future Work

5.1.1 Covering Dihedral Groups D_n

Given a dihedral group D_p of order $2p$, find intersective polynomials that represent any dihedral group of order $2p$. The coverings for these groups are easy to find but the theory required to form intersective polynomials may need to be constructed or researched fully.

A possible extension of the problem above could be given a dihedral group D_{pq} of order $2pq$, find a cover for this dihedral group: first for small ordered groups, then perhaps a generalization. Once a cover is constructed, form families of intersective polynomials with this dihedral Galois group.

Then, find out of if it's possible to find a cover for small dihedral groups of any order $2n$. It may be helpful working with the case when n is odd or when n is even.

5.1.2 Covering Semi-Direct Products $\mathbb{Z}_m \rtimes \mathbb{Z}_m^*$

It is well known that prime dihedral groups are semi-direct products of $\mathbb{Z}_p$ with $\mathbb{Z}_2$. This may lead to interesting conclusions about semi-direct products in general. Or conversely, it may be possible to use theory about semi-direct products to form intersective polynomials represented by dihedral Galois groups.

Instead of the specific holomorph used in this thesis, find a cover for more generalized semi-direct products $\mathbb{Z}_m \rtimes \mathbb{Z}_m^*$, then construct intersective polynomials that represent these products.

5.1.3 Product of Two Simplest Cubics

For $a \in \mathbb{N}$, let $f = x^3 - ax^2 - (a+3)x - 1$ and let $K = K_a$ be the cyclic cubic number field generated by a root α of f. The splitting field for the product of two of these polynomials would be isomorphic to $C_3 \times C_3$. Find intersective polynomials constructed as the product of these types of cubics.

5.1.4 Hilbert Class Polynomials

Given a number field K, there is a finite Galois extension L of K such that

1. L is an unramified Abelian extension of K.

2. Any unramified Abelian extension of K lies in L.

The field L above is called the Hilbert class field of K. Now let $K = \mathbb{Q}(\sqrt{D})$, where D is a negative fundamental discriminant (not equal to 1, not divisible by any square of any odd prime, and satisfies $d \equiv 1 \pmod 4$ or $d \equiv 8, 12 \pmod{16}$).

Let $C(D)$ be the set of all reduced quadratic forms $[a, b, c]$ of the discriminant D. Then the Hilbert class polynomial is defined to be

$$H_D(X) = \prod_{[a,b,c] \in C(D)} \left(X - j\left(\frac{-b + i\sqrt{D}}{2a} \right) \right)$$

where $j(\alpha)$ is the j-invariant or j-value of α. This polynomial has degree equal to the class number of the imaginary quadratic field defined by D.

It is of interest that this polynomial is in fact the minimal polynomial for the Hilbert class field defined above. Due to the nature of this field, all primes are unramified and thus the decomposition group for each prime ideal is cyclic. Therefore, the decomposition group for every prime ideal in the Hilbert class field L of K is contained in a proper subgroup of L, and intersective polynomials can automatically be constructed.

5.2 Conclusion

The purpose of this thesis was to provide methods to construct infinite families of intersective polynomials with various Galois groups. The methods used in Chapter 3 required relatively recent theory on decomposition groups. In the case of polynomials with Galois group A_4, we were able to take advantage of the monogeneity of the number field of the roots of the polynomials we were studying. However, in the case of the polynomials with Galois group D_5, this wasn't the case and we had to resort to other theory about dihedral groups. In both cases, we found a 2-cover and an infinite parametric family of polynomials that yielded intersectivity.

The methods used in Chapter 4 were more constructive. Using theory about binomials $x^{2^e} - a$, we were able to construct a 3-cover for the Galois group representing these binomials. Then we were able to find the three polynomial factors that correspond to this cover, and from there, generated conditions on a and e for the product of these factors to yield intersective polynomials.

For all three methods used, we also provided examples of such polynomials that are intersective using our theory. It is important to note that only a finite amount were provided from an infinite set; the reader could implement and generate any desired number of such polynomials.

Bibliography

[AW04] S. Alaca and K. S. Williams. *Introductory Algebraic Number Theory*. Cambridge University Press, Cambridge, 2004. → pages 1

[BLL08] V. Bergelson, A. Leibman, and E. Lesigne. Intersective polynomials and the polynomial szemerédi theorem. *Advances in Mathematics*, 219(1):369–388, 2008. → pages 40

[BR] V. Bergelson and D. Robertson. Polynomial multiple recurrence over rings of integers. `http://dx.doi.org/10.1017/etds.2014.138`. → pages 40

[Bra01] R. Brandl. Integer polynomials with roots mod p for all primes p. *Journal of Algebra*, 240:822–835, 2001. → pages 41

[Bub98] D. Bubboloni. Coverings of the symmetric and alternating groups. *Quaderno del Dipartimento di Matematica U. Dini, Firenze*, 7, 1998. → pages 32

[Cap01] A. Capelli. Sulla riduttibilità della funzione $x^n - a$ in campo qualunque di rationalità. *Mathematische Annalen*, 54(4):602–603, 1901. → pages 67

[Cas11] M. Castillo. A note on buchi's problem for p-adic numbers. *Proyecciones Journal of Mathematics*, 30(3):295–302, December 2011. → pages 73

[Coh99] H. Cohen. *Advanced Topics in Computational Number Theory*. Springer-Verlag, 1999. → pages 52, 54, 56, 57

[Con] K. Conrad. Dihedral groups ii. `http://www.math.uconn.edu/~kconrad/blurbs/grouptheory/dihedral2.pdf`. → pages 37

[DF04] D. Dummit and R. Foote. *Abstract Algebra*. Wiley, third edition, 2004. → pages 66

[Erd53] P. Erdös. Arithmetic properties of polynomials. *London Math. Soc.*, 28:416–425, 1953. → pages 46

[Fra02] J. B. Fraleigh. *A First Course in Abstract Algebra*. Addison Wesley, 2002. → pages 1, 68

[Gou93] F. Q. Gouvêa. *p-adic Numbers, An Introduction*. Springer-Verlag, 1993. → pages 39

[HLS14] A.M. Hyde, P.D. Lee, and B.K. Spearman. Polynomials $(x^3 - n)(x^2 + 3)$ solvable modulo any integer. *American Mathematical Monthly*, 121(4):355–358, 2014. → pages 41

[INM95] H. S. Zuckerman I. Niven and H. L. Montgomery. *An Introduction to the Theory of Numbers*. Wiley and Sons, fifth edition, 1995. → pages 41, 42, 75

[JV90] E. T. Jacobson and W. Y. Vélez. The galois group of a radical extension of the rationals. *Manuscripta Math.*, 6:271–284, 1990. → pages 64, 66, 68

[LÎ14] T.H. Lê. Combinatoral and additive number theory. In *Springer Proceedings in Mathematics & Statistics*, volume 101, chapter Problems and results on intersective sets, pages 115–128. Springer, 2014. → pages 39

[LN83] P. Llorente and E. Nart. Effective determination of the decomposition of the rational primes in a cubic field. *Proceedings of the American Mathematical Society*, 87(4):579–585, 1983. → pages 47

[LNV84] P. Llorente, E. Nart, and N. Vila. Discriminants of number fields defined by trinomials. *Acta Arithmetica*, 43:367–373, 1984. → pages 54

[LS14] T.H. Lê and C.V. Spencer. Intersective polynomials and diophantine approximation. *International Mathematics Research Notices*, 2014(5):1153–1173, 2014. → pages 40

[LSY14] M. J. Lavallee, B. K. Spearman, and Q. Yang. Intersective polynomials with galois group d_5. *Math. J. Okayama Univ.*, 56:27–33, 2014. → pages 40, 52

[Nar90] W. Narkiewicz. *Elementary and Analytic Theory of Algebraic Numbers*. Springer, third edition, 1990. → pages 25, 47, 50, 56

[Ros02] M. Rosen. *Number Theory in Function Fields*. Springer-Verlag, New York, 2002. → pages 46

[RS13] D. Rabayev and J. Sonn. On galois realizations of the 2-coverable symmetric and alternating groups. *Communications in Algebra*, 42(1):253–258, 2013. → pages 40, 45

[RYZ82] G. Roland, N. Yui, and D. Zagier. A parametric family of quintic polynomials with galois group D_5. *Journal of Number Theory*, 15:137–142, 1982. → pages 53, 61, 62

[Son08] J. Sonn. Polynomials with roots in $\mathbb{Q}_p$ for all p. *Proceedings of the American Mathematical Society*, 136(6):1955–1960, 2008. → pages 33, 40, 44

[Son09] J. Sonn. Two remarks on the inverse galois problem for intersective polynomials. *Journal de Theorie des Nombres Bordeaux*, 21(2):437–439, 2009. → pages 40, 44, 46

[Spe06] B. K. Spearman. Monogenic A_4 quartic fields. *International Mathematical Forum*, 1(40):1969–1974, 2006. → pages 45

[SW02] B. K. Spearman and K. S. Williams. The discriminant of a dihedral quintic field defined by a trinomial $x^5 + ax + b$. *Canadian Mathematics Bulletin*, 45(1):138–153, 2002. → pages 52, 54, 57

[SWY07] B. K. Spearman, K. S. Williams, and Q. Yang. On the common index divisors of a dihedral field of prime degree. *International Journal of Mathematics and Mathematical Sciences*, 2007, Article ID 89713, 8 pages, 2007. → pages 57

[Vah95] K. Th. Vahlen. Uber reductible binome. *Acta Mathematica*, 19(1):195–198, 1895. → pages 67

[Web79] H. Weber. *Lehrbuch der Algebra*. Chelsea, New York, 1979. → pages 53

[Wei09] S. H. Weintraub. *Galois Theory*. Springer, second edition, 2009. → pages 67

[Yam] S. Yamagishi. Diophantine approximation of polynomials over $\mathbb{F}_q[t]$ satisfying a divisibility condition. `http://dx.doi.org/10.1142/S1793042116500846`. → pages 40