2005

The solvability of polynomials by radicals: A search for unsolvable and solvable quintic examples

Robert Lewis Beyronneau

THE SOLVABILITY OF POLYNOMIALS BY RADICALS: A SEARCH FOR UNSOLVABLE AND SOLVABLE QUINTIC EXAMPLES

A Project
Presented to the
Faculty of
California State University,
San Bernardino

In Partial Fulfillment
of the Requirements for the Degree
Master of Arts
in
Mathematics

by
Robert Lewis Beyronneau
June 2005

THE SOLVABILITY OF POLYNOMIALS BY RADICALS: A SEARCH FOR UNSOLVABLE AND SOLVABLE QUINTIC EXAMPLES

A Project
Presented to the
Faculty of
California State University,
San Bernardino

by
Robert Lewis Beyronneau
June 2005

Approved by:

[redacted]

Belisario Ventura, Committee Chair — 6/6/05 Date

[redacted]

Davida Fischman, Committee Member

[redacted]

Laura Wallace, Committee Member

[redacted]

Charles Stanton, Chair
Department of Mathematics

Terry Hallett

Terry Hallett,
Graduate Coordinator
Department of
Mathematics

ABSTRACT

Starting with the ancient Greeks, mathematicians searched for the answer to the question "Which polygons are constructible with a straightedge and compass." As time passed, mathematicians began to utilize what is known as Abstract Algebra and Group Theory to answer this question.

As a result, Field Theory was born. Using Field Theory many new questions soon arose. One of them was "Which polynomials over Q were and were not solvable by radicals." The examination of this question led to the creation of Galois Theory.

Great anticipation surrounded whether or not a typical quintic polynomial was solvable. When it was found through Galois Theory that a typical quintic polynomial was not solvable, many mathematicians chose to study other topics. Most textbooks these days spend very little time on solvable quintics, giving very few examples, concentrating instead on the impossibility of solving a quintic by radicals.

As a result, I chose to center my research around finding specific examples of quintics that were and were not solvable. In order to do this, I needed to extend my understanding from Galois Theory, and learn about solvable groups. This new knowledge led me to a deeper understanding of symmetric groups. This in turn, helped me devise a method for finding examples of solvable and unsolvable quintics.

In the end, I have found eleven examples of quintics, some which are and are not solvable. I have also provided a method which one may use as a springboard for finding even more solvable and unsolvable quintics.

TABLE OF CONTENTS

LIST OF FIGURES

CHAPTER ONE

INTRODUCTION

Throughout history mathematicians have sought to classify which procedures can be carried out following certain rules. This began with the early Greeks as they sought to determine which polygons were and were not constructible with only a straightedge and compass. As time progressed, mathematicians continued this classification on a variety of topics. One such topic, which began to develop around the 1700's and 1800's was the solvability of polynomials by radicals.

Many great mathematicians worked to find out how to decide which polynomials were and were not solvable by radicals. Among them we have Cardano, Ruffini, Abel, and Galois. As a result of their work, it was discovered that every quadratic, cubic, and quartic are solvable by radicals, and that in general a typical quintic is not solvable. Sometimes throughout history when it is discovered that something cannot be done, interest in that topic ceases to exist and other questions that perhaps might be answered in that area are no longer asked. This is what happened in the case of the unsolvability of the quintic.

Great excitement and anticipation once surrounded the mystery of whether the quintic was solvable by radicals or not. While many great minds set forth to solve that problem, once it was proven that the general quintic is not solvable by radicals, the excitement that fueled the development of a new branch of mathematics called field theory, deflated and the topic of solvability by radicals of the quintic became less important.

As a result, in many textbooks, only the unsolvability of the quintic is considered, and other questions like: Are there any quintics that are solvable by radicals? If so, can we predict whether a quintic will be solvable or not? What methods can we employ to determine whether a specific quintic is solvable?, are not discussed. These are the questions that fueled my research into the topic of the solvability of quintics.

CHAPTER TWO

FIELDS AND THEIR EXTENSIONS

Before we can tackle such a topic like the solvability by radicals we need to get acquainted with some basic field and Galois theory.

Definition 2.1: A field is a set F with two operations called addition and multiplication such that:

(1) F is an abelian group under addition (with identity element 0);

(2) F^*, the set of nonzero elements of F, is an abelian group under multiplication;

(3) multiplication is distributive over addition; that is, for any three elements $a,b,c \in F$, $a(b+c) = ab + ac$ and $(a+b)c = ac + bc$.

Throughout this paper we shall denote the additive inverse of $a \in F$ by $-a$. If $a \in F^*$, then a has a multiplicative inverse as well which we will denote as a^{-1}. Lastly, we will always denote the multiplicative identity element by 1.

Definition 2.2: A subfield of a field E is a subset F such that:

(1) F is a subgroup of E under addition and

(2) F^* is a subgroup of E^* under multiplication.

Clearly, a subfield of a field is itself a field.

Definition 2.3: A number field is any subfield of C.

Note that clearly, Q and R are subfields of C, this means that Q and R are also number fields. We shall denote a subfield F of E by $F \leq E$.

Proposition 2.1: Every number field contains Q.

Proof: Let F be a number field. Then, F is a subfield of C. We must show that F contains Q. Note that our additive and multiplicative identities do not equal each other, that is $0 \neq 1$. However, 0 and 1 in this case are the real rational numbers, and they are in F. Thus if we can show that 0 and 1 generate all of Q we will be done. However, Q is the field generated by Z, thus if we can generate any integer, we can then generate Q. Since we know 1 is in F, we know by closure of addition that $1+1$ is in F, and by our additive inverse we also know that $(-1)+(-1)$ is in F. Thus by induction, for any $n \in Z$, $n \cdot (\pm 1) = \pm(1+1+\ldots+1)1 \in F$, thus for all $n \in Z$, $n \in F$. However, this means that Z is contained in F. Now, any field containing a ring must contain the quotient field of that ring. Thus, F contains the quotient field of Z. However, the quotient field of Z is Q. Thus F contains Q. Thus any $F \leq C$ contains Q.■

Definition 2.4: If $F \leq E$, then we say that E is an extension field of F.

Example 2.1: Since Q is a subfield of R, then R is an extension field of Q.

There are other extensions of the field Q.

Example 2.2: The set $Q(\sqrt{2})=\{z\in C \mid z=a+b\sqrt{2};a,b\in Q\}$ is a number field.

Proof: In order to show $Q(\sqrt{2})=\{z\in C \mid z=a+b\sqrt{2};a,b\in Q\}$ is a number field, there are three things we must show:

(1) $Q(\sqrt{2})$ is a subset of C.

(2) $Q(\sqrt{2})$ is a subgroup of C under addition, and

(3) $Q(\sqrt{2})^*$ is a subgroup of C^* under multiplication.

Let us begin by showing (1) $Q(\sqrt{2})$ is a subset of C.

Since elements in $Q(\sqrt{2})$ are of the form $a+b\sqrt{2}$ where a and b both come from Q which is a subfield of C, clearly $Q(\sqrt{2})$ is a subset of C.

Next let us show that (2) $Q(\sqrt{2})$ is a subgroup of C under addition.

To do this we must show that $Q(\sqrt{2})$ has additive closure, that the associative property holds in $Q(\sqrt{2})$, that there is an additive identity for $Q(\sqrt{2})$, and that inverses exist for every x in $Q(\sqrt{2})$. The associative property holds in $Q(\sqrt{2})$ since $Q(\sqrt{2})$ is a subset of C.

Now we look to show the other three properties. Let x and y be in $Q(\sqrt{2})$ such that $x=a+b\sqrt{2}$ and $y=c+d\sqrt{2}$. Then $x+y=a+b\sqrt{2}+c+d\sqrt{2}=(a+c)+(b+d)\sqrt{2}\in Q(\sqrt{2})$. Thus, $x+y\in Q(\sqrt{2})$, and $Q(\sqrt{2})$ is closed under addition. The additive identity of $Q(\sqrt{2})$ is 0 since for all $x = a + b\sqrt{2}$ in $Q(\sqrt{2})$, $x + 0 = a + b\sqrt{2} = 0 + a + b\sqrt{2} = 0 + x$. Lastly, inverses exist in $Q(\sqrt{2})$, since for all $x = a + b\sqrt{2}$ in $Q(\sqrt{2})$, there exists a $-x = -a - b\sqrt{2}$, such that. $x + (-x) = a + b\sqrt{2} + (-a - b\sqrt{2}) = 0$. Thus, $Q(\sqrt{2})$ is a subgroup of C under addition.

Lastly, let us show (3) $Q(\sqrt{2})^*$ is a subgroup of C^* under multiplication.

To do this we must show that $Q(\sqrt{2})^*$ has multiplicative closure, that the associative property holds in $Q(\sqrt{2})^*$, that there is a multiplicative identity for $Q(\sqrt{2})^*$, and that inverses exist for every x in $Q(\sqrt{2})^*$. The associative property holds in $Q(\sqrt{2})^*$ since $Q(\sqrt{2})^*$ is a subset of C^*. Now we look to show the other three properties.

Let x and y be in $Q(\sqrt{2})^*$ such that $x = a + b\sqrt{2}$ and $y = c + d\sqrt{2}$ with a and b not both zero, and c and d not both zero. Then $xy = (a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2} \in Q(\sqrt{2}) - \{0\}$, thus $xy \in Q(\sqrt{2})^*$, hence $Q(\sqrt{2})^*$ is closed under multiplication. The multiplicative identity of $Q(\sqrt{2})^*$ is 1 since for all $x = a + b\sqrt{2}$ in $Q(\sqrt{2})^*$, $x \cdot 1 = (a + b\sqrt{2}) \cdot 1 = a + b\sqrt{2} = 1 \cdot (a + b\sqrt{2}) = 1 \cdot x$. Lastly, inverses exist in $Q(\sqrt{2})*$, since for all $x=a+b\sqrt{2}$ in $Q(\sqrt{2})*$, there exists a $x^{-1}=\frac{a}{a^2-2b^2}-\left(\frac{b}{a^2-2b^2}\right)\sqrt{2}$, such that.

$$x\cdot x^{-1}=\left(a+b\sqrt{2}\right)\left(\frac{a}{a^2-2b^2}-\left(\frac{b}{a^2-2b^2}\right)\sqrt{2}\right)=\left(\frac{a+b\sqrt{2}}{1}\right)\left(\frac{a-b\sqrt{2}}{a^2-2b^2}\right)=\left(\frac{a^2-2b^2}{a^2-2b^2}\right)=1.$$

Thus, $Q(\sqrt{2})*$ is a subgroup of $C*$ under multiplication. Therefore by (1)-(3), the set $Q(\sqrt{2})=\{z\in C\mid z=a+b\sqrt{2};a,b\in Q\}$ is a number field. Clearly, $Q(\sqrt{2})$ contains Q. Thus, $Q(\sqrt{2})$ is an extension of Q.■

Example 2.3: A very similar proof will show that the set $Q(i)=\{z\in C\mid z=a+bi;a,b\in Q\}$ is also a number field (mainly by replacing $\sqrt{2}$ with i. Thus, $Q(i)$ is an extension of Q.

Proposition 2.2: If F is field and the field E is an extension of F, then E is a vector space over F.

Proof: In order to show this we must show that:

(1) E is an abelian group under addition,

(2) for all β and α in F and x in E, $\beta(\alpha x)=(\beta\alpha)x$,

(3) for all β and α in F, x and y in E,

$\beta(x+y)=\beta x+\beta y$ and $(\beta+\alpha)x=\beta x+\alpha x$, and

(4) for all β in F $1\beta=\beta$.

Let us start by showing (1) E is an abelian group under addition.

Since E is a field, then E is an abelian group under addition.

Now let's show (2) for all β and α in F and x in E, $\beta(\alpha x) = (\beta\alpha)x$.

Since F is a subfield of the field E and multiplication is associative for all β and α in F and x in E, $\beta(\alpha x) = (\beta\alpha)x$.

Moving on, let us show (3) for all β and α in F, x and y in E, $\beta(x+y) = \beta x + \beta y$ and $(\beta+\alpha)x = \beta x + \alpha x$.

Since F is a subfield of E and E itself is a field, the distributive properties hold, thus for all β and α in F, x and y in E, $\beta(x+y) = \beta x + \beta y$ and $(\beta+\alpha)x = \beta x + \alpha x$.

Lastly, let us show (4) for all β in F $1\beta = \beta$.

Since F is a subfield of E and the identity exists in both E^* and F^*, and they are the same identity, $1\beta = \beta$.

Thus, any extension of a field is a vector space over that field. That is, if F is a field and the field E is an extension of F, then E is a vector space over F.■

This means that any extension over Q is also a vector space over Q. Thus, $Q(\sqrt{2})$ and $Q(i)$ are also vector spaces over Q.

Once you start extending fields we can create a tower of fields like those in Figure 1.

$$\begin{tikzcd}
C \arrow[d, dash] & & Q(\sqrt{2}) \arrow[dr, dash] & & Q(i) \arrow[dl, dash] \\
R \arrow[d, dash] & & & Q & \\
Q & & & &
\end{tikzcd}$$

Figure 1. Field Towers

Now once we have established that there are extensions of fields, we might ask is there is a way to order the fields in size. This idea leads us right into our next chapter.

CHAPTER THREE
ORDERING THE EXTENSIONS

The basic tool for ordering the extensions is called the degree of the extension and will be denoted $[E{:}F]$. That is, $[E{:}F]$ will stand for the degree of the extension E over F. $[E{:}F]$ is defined as the dimension of the vector space E over F. That is, $[E{:}F] = \dim_F E$. If an extension field E of a field F is a finite dimensional vector space over F, then E will be called a finite extension of F.

In our first tower of Figure 1, we looked at three fields that also happen to be vector spaces over Q; C, R, and Q. In this example, $[R{:}Q]$ and $[C{:}Q]$ are infinite since the number of elements in a basis for R over Q and C over Q respectively, is infinite. However, $[C{:}R] = 2$ since a basis for C over R is $\{1, i\}$. In our second tower of Figure 1, both $[Q(\sqrt{2}){:}Q]$ and $[Q(i){:}Q]$=2, since the bases for them over Q are $\{1, \sqrt{2}\}$ and $\{1, i\}$ respectively.

Definition 3.1: Let β be an element of E, an extension field of F. We denote $F(\beta)$ to be the smallest subfield of E containing both F and β.

$F(\beta)$ is called the field obtained by adjoining β to F. We may also characterize $F(\beta)$ as the intersection of all the subfields of E which contain β and F. We denote by $F(\beta,\alpha)$ the subfield of E obtained by adjoining α to $F(\beta)$.

Example 3.1: Let $\omega = e^{2\pi i/3} = -\frac{1}{2} + \frac{i\sqrt{3}}{2}$. Then the set $S = \{z \in C \mid z = a + b\omega; a,b \in Q\}$ is an extension of Q of degree 2 and equals $Q(\omega)$.

Proof: In order to show this, there are three things we must show.

(1) S is a subset of C.

(2) S is a subgroup of C under addition, and

(3) S^* is a subgroup of C^* under multiplication.

Let us begin with (1) S is a subset of C.

Since elements in S are of the form $a + b\omega$ where a and b both come from Q which is a subfield of C, clearly S is a subset of C.

Now let us show (2) S is a subgroup of C under addition.

To do this we must show that S has additive closure, that the associative property holds in S, that there is an additive identity for S, and that inverses exist for every x in S.

The associative property holds in S, since S is a subset of C. Now we look to show the other three properties. Let x and y be in S such that $x = a + b\omega$ and $y = c + d\omega$. Then $x + y = a + b\omega + c + d\omega = (a+c) + (b+d)\omega \in S$, thus $x + y \in S$, hence S is closed under addition. The additive identity of S is 0 since for all $x=a+b\omega$ in S, $x+0=a+b\omega=0+a+b\omega=0+x$. Lastly, inverses exist in S, since for all $x=a+b\omega\in S$, there exists a $-x=-a-b\omega$, such that $x+(-x)=a+b\omega+(-a-b\omega)=0$. Thus, S is a subgroup of C under addition.

(3) S^* is a subgroup of C^* under multiplication.

To do this we must show that S^* has multiplicative closure, that the associative property holds in S^*, that there is a multiplicative identity for S^*, and that inverses exist for every x in S^*. The associative property holds in S^* since S^* is a subset of C^*. Now we look to show the other three properties.

Let x and y be non-zero elements of S^* such that $x=a+b\omega$ and $y=c+d\omega$. First note that $\omega^2=-\frac{1}{2}-\frac{i\sqrt{3}}{2}=-1-\omega$ since $\omega^3=1$. Then,

$$xy=(a+b\omega)(c+d\omega)=(ac)+(ad+bc)\omega+ad\omega^2=(ac)+(ad+bc)\omega+ad(-1-\omega)$$

thus, $xy=(ac-bd)+(ad+bc-bd)\omega\in S^*$, hence $xy\in S^*$, therefore S^* is closed under multiplication. The multiplicative identity of S^* is 1 since for all $x=a+b\omega$ in S^*, $x\cdot 1=(a+b\omega)\cdot 1=a+b\omega=1\cdot(a+b\omega)=1\cdot x$.

Lastly, inverses exist in $Q(\omega)^*$, since for all $x=a+b\omega\in Q(\omega)^*$, there exists a $x^{-1}=\frac{a-b}{a^2-ab+b^2}-\left(\frac{b}{a^2-ab+b^2}\right)\omega$, such that

$$x \cdot x^{-1} = (a+b\omega)\left(\frac{a-b}{a^2-ab+b^2} - \left(\frac{b}{a^2-ab+b^2}\right)\omega\right) = (a+b\omega)\left(\frac{a-b-b\omega}{a^2-ab+b^2}\right)$$

$$= \left(\frac{a^2-ab-ab\omega+ab\omega-b^2\omega-b^2\omega^2}{a^2-ab+b^2}\right) = \left(\frac{a^2-ab-b^2\omega-b^2(-1-\omega)}{a^2-ab+b^2}\right)$$

$$= \left(\frac{a^2-ab-b^2\omega+b^2+b^2\omega}{a^2-ab+b^2}\right) = \left(\frac{a^2-ab+b^2}{a^2-ab+b^2}\right) = 1.$$

Thus, S^* is a subgroup of C^* under multiplication.

Therefore by (1)-(3), the set S is a number field. Now since S is a number field, it contains Q. Thus, S is an extension of Q. Also since S is an extension of Q, it is a vector space over Q and has a basis. One basis for S over Q is the set $\{1,\omega\}$. Thus $[Q(\omega){:}Q]=2$. Therefore, $S=\{z\in C \mid z=a+b\omega; a,b\in Q\}$ is an extension of Q of degree 2. Now $\omega\in S$, so $Q(\omega)\subseteq S$. On the other hand if $a+b\omega\in S$, we have that $a+b\omega\in Q(\omega)$. Thus, $S=Q(\omega)$ ■

So we have now seen four examples of finite extensions over a field, all being of degree 2. Are there any of higher degree? Can we manufacture some from the ones we have looked at? Let us look at a very important proposition.

Proposition 3.1: If D is a finite extension of E and E is a finite extension of F, then D is a finite extension of F. Furthermore $[D{:}F]=[D{:}E][E{:}F]$.

Proof: Let $A=\{\alpha_1,\alpha_2,\ldots,\alpha_m\}$ be a basis for E over F, and let $B=\{\beta_1,\beta_2,\ldots,\beta_n\}$ be a basis for D over E. We hope to show that the set $C=\{\alpha_i\beta_j \mid 1\le i\le m, 1\le j\le n\}$ is a basis for D over F.

To do this we must show that:

(1) C spans D over F and

(2) C is linearly independent.

Let us begin with showing (1) C spans D over F.

Suppose $\delta\in D$. Using the basis B, we have $\delta=\delta_1\beta_1+\delta_2\beta_2+\ldots\delta_n\beta_n, \delta_i\in E$. Each of the elements $\delta_i\in E$, $i=1,2,..n$, can be written as $\delta_i=c_{i1}\alpha_1+c_{i2}\alpha_2+\ldots c_{im}\alpha_m, c_{ij}\in F$. If we substitute this expression into the latter expression we end up with $\delta=\sum_{i=1}^{n}\sum_{j=1}^{m}c_{ij}\alpha_j\beta_i$, $c_{ij}\in F$. Thus C spans D over F, since any element of D over F can be written as a linear combination of elements of C.

Now let us show that (2) C is linearly independent.

Suppose that there is a linear relation among the elements of C with coefficients in F such that $\sum_{i=1}^{n}\sum_{j=1}^{m}c_{ij}(\alpha_j\beta_i)=0$, $c_{ij}\in F$.

We will show that this sum is a linear combination of basis elements in B. Since it equals zero, the coefficients must equal zero.

In fact, we can consider this sum as a linear combination of elements in B with coefficients $\delta_i=c_{i1}\alpha_1+c_{i2}\alpha_2+\ldots c_{im}\alpha_m,$. Thus, this means each

$\delta_i = c_{i1}\alpha_1 + c_{i2}\alpha_2 + ...c_{im}\alpha_m = 0$ but because each of the α_i's are linearly independent this implies that each of the c_{ij}'s are zero for $i = 1,2,..n$ and $j = 1,2,...m$. Thus $\sum_{i=1}^{n}\sum_{j=1}^{m} c_{ij}\alpha_j\beta_i = 0 \Rightarrow c_{ij} = 0$ for $i = 1,2,..n$ and $j = 1,2,...m$. Hence, C is linearly independent.

Since we have shown that C is a linearly independent spanning set for D over F; thus it is a basis for D over F.

Since C has a finite number of elements, it follows that D is a finite extension of F, thus

$[D:F] = [D:E][E:F] = mn$.■

Example 3.2: Let us consider $Q(\sqrt{2},i)$ over the field Q. A typical element of $Q(\sqrt{2},i)$ is $x = a + b\sqrt{2} + ci + di\sqrt{2}$, a,b,c, and d in Q. Thus a basis for $Q(\sqrt{2},i)$ over Q is $\{1,\sqrt{2},i,i\sqrt{2}\}$. Thus

$\left[Q(\sqrt{2},i):Q\right] = 4$.

In this case we get a partially ordered set of fields instead of a field tower, which we will call a vax. Now let us look at this vax as shown in figure 2 below.

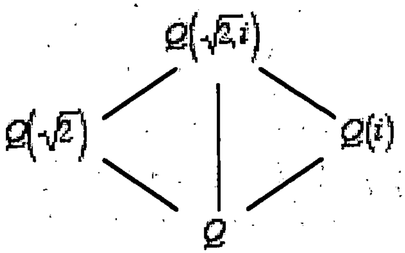

Figure 2. Field Vax

In this field vax, we first saw that $\left[Q\left(\sqrt{2}\right):Q\right]=2$ and $\left[Q(i):Q\right]=2$. Next we can verify that $\left[Q\left(\sqrt{2},i\right):Q\left(\sqrt{2}\right)\right]=2$ using the basis $\left\{i,i\sqrt{2}\right\}$ and that $\left[Q\left(\sqrt{2},i\right):Q(i)\right]=2$ using the basis $\left\{\sqrt{2},i\sqrt{2}\right\}$. Thus utilizing Proposition 3.1 we get that $\left[Q\left(\sqrt{2},i\right):Q\right]=4$.

CHAPTER FOUR

POLYNOMIALS

We now turn our focus to polynomials over a field.

Definition 4.1: A polynomial over a field F in the indeterminate x is an expression of the form $c_0 + c_1x + \ldots + c_nx^n$, where $c_0, c_1, \ldots, c_n$ are elements of F, called the coefficients of the polynomial.

The largest k for which $c_k \neq 0$ is called the degree of f (denoted $\deg f$), and c_k is called the leading coefficient of f. If all coefficients of f are zero, we write $f = 0$ and do not assign a degree to f.

Example 4.1: $f(x) = 10 + 7x + x^2$ is a polynomial over Q, R, and C of degree two.

Example 4.2: $g(x) = 1 + 2ix + x^2$ is only a polynomial over C since the coefficient $2i$ does not exist in Q or R.

Definition 4.2: A polynomial f over F of positive degree which can be factored as $f = gh$ where g and h are polynomials over F of positive degree is called reducible over F; a polynomial of positive degree which cannot be factored is called irreducible over F.

Note that any polynomial of degree 1 is irreducible. Proposition 4.1 on the next page shows that irreducible polynomials behave like prime numbers.

Example 4.3: $f(x) = x^2 + 1$ is irreducible over Q and R yet reducible over C since $f(x) = x^2 + 1 = (x+i)(x-i)$.

Example 4.4: $f(x) = x^2 - 2$ is reducible over R and C since $f(x) = x^2 - 2 = (x + \sqrt{2})(x - \sqrt{2})$, yet irreducible over Q.

Definition 4.3: Any polynomial with leading coefficient 1 will be called a monic polynomial.

Proposition 4.1: Every polynomial over a field can be factored as a product of irreducible polynomials in a way which is unique except for the order and multiplication of factors by constants.

Example 4.5: Let $f(x) = x^4 + 1$. Then f is irreducible over Q but reducible uniquely over $Q(i)$ as $(x^2 + i)(x^2 - 1)$, is reducible over $Q(\sqrt{2})$ as $(x^2 + \sqrt{2}x + 1)(x^2 - \sqrt{2}x + 1)$, and is reducible over $Q(\sqrt{2}, i)$ as $(x + i\sqrt{i})(x - i\sqrt{i})(x + \sqrt{i})(x - \sqrt{i})$.

Eisenstein Irreducibility Criterion: Let f be a polynomial over Q with integral coefficients, say $f(x) = c_0 + c_1 x + \ldots + c_n x^n$. If there is a prime number p such that p divides every coefficient of f except c_n, and p^2 does not divide c_0, then f is irreducible over Q.

Proof: Assume f is not irreducible over Q. Then $f = gh$, and the coefficients of f can be expressed as $c_l = \sum_{j+k=l} a_j b_k$ and suppose $p \mid c_i$ for $i = 0, 1, \ldots, n-1$ but p does not divide c_n and p^2 does not divide c_0. Since $p \mid c_0 = a_0 b_0$ but p^2 does not divide c_0, we have that $p \mid a_0$ or $p \mid b_0$ but not both. Suppose $p \mid a_0$ but p does not divide b_0. Since $p \mid c_1$, we have $p \mid a_1$, since $c_1 = a_0 b_1 + a_1 b_0$ and $p \mid a_0$ but p does not divide b_0.

If we continue this way we will find that $p \mid a_j$, for all j. Thus $p \mid c_l$ for all l, but this is a contradiction since p does not divide c_n. Thus f must be irreducible.■

Example 4.6: Let $f(x) = 2x^3 + 9x^2 + 15x + 3$. Then by the Eisenstein Criterion with $p = 3$, f is irreducible over Q since 3 divides all coefficients except 2 and 9 does not divide 3.

Sometimes the Eisenstein Irreducibility Criterion cannot be applied directly to a polynomial f, but when we compose the polynomial with a linear transformation $x - h$, we get a polynomial g to which the Eisenstein criterion does apply. Since a factorization of f will produce a factorization of g, we have that f is irreducible if g is irreducible. This procedure is illustrated by the following example.

Example 4.7: $f(x) = 4x^3 - 3x - \frac{1}{2}$ is irreducible over Q. First we multiply $f(x)$ by 2 so that it will have integral coefficients, this yields $g(x) = 8x^3 - 6x - 1$.

Clearly, at this point $g(x)$ can not be proved to be irreducible using the Eisenstein criterion, thus we apply the linear transformation $x \to x - 1$ and see if this helps.

Applying this linear transformation we obtain $g(x-1) = 8(x-1)^3 - 6(x-1) - 1 = 8x^3 - 24x^2 + 18x - 3$. Now 3 is a prime that divides all the coefficients except 8, while, 9, which is our prime squared, does not divide 3, thus by the

Eisenstein Criterion $g(x-1)$ is irreducible over Q which implies that $f(x)=4x^3-3x-\frac{1}{2}$ is irreducible over Q.■

Example 4.8: Let $\Phi_p(x)=1+x+x^2+...+x^{p-1}$, where p is prime, show that $\Phi_p(x)=1+x+x^2+...+x^{p-1}$ is irreducible over Q.

Let us consider $\Phi_p(1+x)=1+(1+x)+(1+x)^2+...+(1+x)^{p-1}$. If we expand and gather terms we will see that

$$\Phi_p(1+x)=p+...+\sum_{j=k}^{p-1}\binom{j}{k}x^k+...+x^{p-1},$$

but this means that $p\mid c_0,c_1,...,c_{p-2}$, but does not divide c_{p-1} and p^2 does not divide $p=c_0$, thus $\Phi_p(1+x)$ is irreducible by the Eisenstein Criterion, which implies that $\Phi_p(x)$ is irreducible over Q.■

CHAPTER FIVE

THE ROOTS OF POLYNOMIALS

Now that we have gotten acquainted with polynomials over a given field, we may begin to wonder about the properties of the roots of these polynomials.

Definition 5.1: Let E be an extension field of the field F. An element α of E is algebraic over F if α is a root of some polynomial with coefficients in F. If every element of E is algebraic over F, then E is called an algebraic extension of F.

Example 5.1: If we take E to be $Q(\sqrt{2})$ and F to be Q, then $\sqrt{2}$ is algebraic over Q, since $\sqrt{2}$ is a root of x^2-2 which is a polynomial over Q. Similarly, i is algebraic over Q by taking E to be $Q(i)$, since i is a root of x^2+1 which is a polynomial over Q.

Definition 5.2: Let α be an element of the extension field E of the field F, and suppose α is algebraic over F. Among all the polynomials over F of which α is a root, let f be one with the lowest degree. Then f is called a minimal polynomial for α over F.

Proposition 5.1: If f is a minimal polynomial for α over F then

(1) f is irreducible over F, and

(2) f divides any polynomial over F having α as a root.

Proof: Let us first start with (1) f is irreducible over F.

Let f be a minimal polynomial for α over F. Assume f is not irreducible over F. Then $f=gh$, and since $f(\alpha)=0$ then we must have $g(\alpha)=0$ or $h(\alpha)=0$. If this factorization is nontrivial then we have that the $\deg g<\deg f$ and $\deg h<\deg f$ but this contradicts that f is minimal, thus f is irreducible.

Now let us show (2) f divides any polynomial over F having α as a root.

Now suppose $p(\alpha)=0$, p any polynomial over F having α as a root. Using the division algorithm then $p=qf+r$ where either $r(x)$ is equivalent to the zero polynomial or $r(x)$ is not equivalent to the zero polynomial. If $r(x)$ is not equivalent to the zero polynomial then since $p(\alpha)=0$ this means that $p(\alpha)=qf(\alpha)+r(\alpha)=r(\alpha)=0$. But this means, since $\deg r<\deg f$ that $f(x)$ would not be a minimal polynomial for α over F , which contradicts that f is minimal. Thus, $r(x)$ is equivalent to the zero polynomial in which case $p=qf$, which means $f|p$. Thus if f is a minimal polynomial for α over F then (1) f is irreducible over F, and (2) f divides any polynomial over F having α as a root.■

Note that one result from the preceding proposition is that two minimal polynomials for α over F differ only by a constant factor. We define the minimal polynomial to be the unique monic polynomial among minimal polynomials.

Example 5.2: Find the minimal polynomial of $i\sqrt{2}$ over Q and over $Q(\sqrt{2})$.

In this case the same polynomial will work for both Q and $Q(\sqrt{2})$ since the minimal polynomial is x^2+2.■

The next example shows that the minimal polynomial may differ depending on over which field we consider it.

Example 5.3: Find the minimal polynomial of $\sqrt{2}+\sqrt{3}$ over Q and over $Q(\sqrt{2})$.

First for the minimal polynomial over $Q(\sqrt{2})$. The technique is to take powers of $\sqrt{2}+\sqrt{3}$ and see if there is some combination with a minimal power that will allow $\sqrt{2}+\sqrt{3}$ to be a root. In this case a quadratic will suffice, namely $f(x)=x^2-2\sqrt{2}x-1$, since

$$f(\sqrt{2}+\sqrt{3})=(\sqrt{2}+\sqrt{3})^2-2\sqrt{2}(\sqrt{2}+\sqrt{3})-1=2+3+2\sqrt{6}-4-2\sqrt{6}-1=0.$$

Thus, $f(x)=x^2-2\sqrt{2}x-1$ is the minimal polynomial for $\sqrt{2}+\sqrt{3}$ over $Q(\sqrt{2})$. This is because a monic degree one polynomial will have to be $x-(\sqrt{2}+\sqrt{3})$, which does not have coefficients in Q. Since the minimal polynomial over $Q(\sqrt{2})$ is of degree two and is not over Q no other monic degree two polynomial $g(x)$ over Q can have $\sqrt{2}+\sqrt{3}$ as a root. Otherwise, $g(x)=f(x)$ as $g(x)$ is also a polynomial over $Q(\sqrt{2})$ and $g(x)$ should be a constant multiple of $f(x)$.

We begin our search for the minimal polynomial one degree higher. Let $g(x)$ be the minimal polynomial for $\sqrt{2}+\sqrt{3}$ over Q, then $f|g$, by Proposition 5.1 (ii), because $g(x)$ is also a polynomial over $Q(\sqrt{2})$. Thus we need to have $f(x)=x^2-2\sqrt{2}x-1$ as a factor. Hence, a monic degree three polynomial over Q will have the form $(x-a)f(x)$, with $a\in Q$, which does not have coefficients in Q. Therefore we can conclude that $g(x)$ can not have degree three.

We find that $g(x)=\left(x^2-2\sqrt{2}x-1\right)\left(x^2+2\sqrt{2}x-1\right)=x^4-10x^2+1$ is the minimal polynomial for $\sqrt{2}+\sqrt{3}$ over Q, since $g(x)$ is monic,

$g\left(\sqrt{2}+\sqrt{3}\right)=0\left(\left(\sqrt{2}+\sqrt{3}\right)^2+2\sqrt{2}\left(\sqrt{2}+\sqrt{3}\right)-1\right)=\left(\sqrt{2}+\sqrt{3}\right)^4-10\left(\sqrt{2}+\sqrt{3}\right)^2+1=0$,

and any polynomial with lesser degree cannot have coefficients in Q.■

Proposition 5.2: If E is an extension field of F and $\beta\in E$ is algebraic over F, then $F(\beta)$ is a finite extension of F of degree n, where n is the degree of the minimal polynomial for β over F. Furthermore, the set $\{1,\beta,\beta^2,\ldots,\beta^{n-1}\}$ is a basis for $F(\beta)$ over F, thus $[F(\beta):F]=n$.

Proof: Since $F(\beta)$ is a field and contains β, $F(\beta)$ must also contain the elements $1,\beta,\beta^2,\ldots,\beta^{n-1}$. However, since $F(\beta)$ is a vector space over F it must contain every linear combination $c_0+c_1\beta+c_2\beta^2+\ldots+c_{n-1}\beta^{n-1}$, with our coefficients being in F. Let X denote the set of all such linear combinations. Clearly, X is a vector space over F spanned by $\{1,\beta,\beta^2,\ldots,\beta^{n-1}\}$. Now let us assume that the set $\{1,\beta,\beta^2,\ldots,\beta^{n-1}\}$ is linearly dependent over F. Then $c_0+c_1\beta+c_2\beta^2+\ldots+c_{n-1}\beta^{n-1}=0$, thus β would be a root of the polynomial g over F given by $g(x)=c_0+c_1\beta+c_2\beta^2+\ldots+c_{n-1}\beta^{n-1}$. However, $\deg g<n$, which means g would be the minimal polynomial for β with degree $n-1$, contradicting that the minimal degree for β is n. This means that the set $\{1,\beta,\beta^2,\ldots,\beta^{n-1}\}$ is linearly independent, hence the set $\{1,\beta,\beta^2,\ldots,\beta^{n-1}\}$ is a basis for X over F.

Now all that is left to do is to prove that X is a field. Since X contains F and β, this would imply that $F(\beta)$ is contained in X. Since we already know that X is contained in $F(\beta)$, we should have $F(\beta)=X$.

We must show that X is an additive subgroup and X^* is a multiplicative subgroup of E and E^* respectively.

Since X is the span of a subset of E it clearly is an additive subgroup of E. Now all we need to show is that X^* is a multiplicative subgroup of E^*.

Let f be a minimal polynomial for β over F. Suppose that $\alpha = a_0 + a_1\beta + a_2\beta^2 + \ldots + a_{n-1}\beta^{n-1}$ and that $\delta = d_0 + d_1\beta + d_2\beta^2 + \ldots + d_{n-1}\beta^{n-1}$ are elements of X^*. We can then write $\alpha = g(\beta)$ and $\delta = h(\beta)$, for the polynomials g and h over F given by $g(x) = a_0 + a_1x + a_2x^2 + \ldots + a_{n-1}x^{n-1}$ and $h(x) = d_0 + d_1x + d_2x^2 + \ldots + d_{n-1}x^{n-1}$. By the division theorem we have $gh = qf + r$ where $r = 0$ or $\deg r < \deg f = n$. Since $f(\beta) = 0$ we have

$$0 \neq \alpha \cdot \delta = (g\beta)(h\beta) = (gh)\beta = (qf)\beta + r(\beta).$$

Since $r(\beta) \neq 0$, we have $r \neq 0$, and thus $\deg r < n$, where $r(x) = c_0 + c_1x + c_2x^2 + \ldots + c_{n-1}x^{n-1}$. Thus

$$\alpha \cdot \delta = r\beta = a_0 + c_1\beta + c_2\beta^2 + \ldots + c_{n-1}\beta^{n-1}$$

which is in X^*. So we have closure. Associatively is inherited, while we can use the same identity as in E^*.

Thus all that is left to do is show that every element in X^* has a multiplicative inverse.

Let $\alpha = g\beta = a_0 + a_1\beta + a_2\beta^2 + \ldots + a_{n-1}\beta^{n-1}$. By Proposition 5.1, f, the minimal polynomial for β over F, is irreducible. Therefore 1 belongs to the greatest common divisor of f and g. Therefore, we can find polynomials u and v over F so that the $\deg v, \deg u < \deg f = n$ and $uf + vg = 1$. Since $f(\beta) = 0$, we have $v(\beta)g(\beta) = 1$, thus $\alpha^{-1} = v\beta$ which is in X^*. Thus X^* is a subfield of E^*.

As a result, we have that X is a field, thus $F(\beta) = X$. Therefore, if E is an extension field of F and β is in E

is algebraic over F, then $F(\beta)$ is a finite extension of F of degree n, where n is the degree of the minimal polynomial for β over F. Furthermore, the set $\{1,\beta,\beta^2,\ldots,\beta^{n-1}\}$ is a basis for $F(\beta)$ over F, and since the number of basis elements determine the degree of an extension over a field, $[F(\beta):F]=n$.■

Example 5.4: Since $\sqrt{2}$ is a root of x^2-2 which is the minimal polynomial of $\sqrt{2}$ over Q, then we know that a basis for $Q(\sqrt{2})$ is the set $\{1,\sqrt{2}\}$, and $[Q(\sqrt{2}):\sqrt{2}]=2$, which is equal to the degree of the minimal polynomial.

Definition 5.3: Let f be a polynomial with coefficients in F, and E be an extension of F containing all the roots $\beta_1,\beta_2,\ldots,\beta_n$ of f. Then the splitting field of f in E, is the smallest subfield of E containing F and the roots $\beta_1,\beta_2,\ldots,\beta_n$ of F.

Proposition 5.3: A finite extension is an algebraic extension.

Proof: Let E be a finite extension of the field F, and suppose that $[E:F]=n$. Let $\beta\in E$. The set of $n+1$ elements $\{1,\beta,\ldots,\beta^n\}$ must be linearly dependent.

Therefore, there are elements $c_0,c_1,\ldots,c_n$ in F not all zero such that $c_0+c_1\beta+\ldots+c_n\beta^n=0$, thus β is a root of a polynomial over F and is algebraic.■

CHAPTER SIX

FIXED FIELDS

Now we take a another big step towards the solvability of polynomials by radicals by looking at a very important topic in Galois theory called fixed fields.

Definition 6.1: An automorphism of a field E is a one-to-one onto mapping $\vartheta: E \to E$ which preserves addition and multiplication, that is, $\vartheta(a+b) = \vartheta(a) + \vartheta(b)$ and $\vartheta(ab) = \vartheta(a)\vartheta(b)$ for all $a,b \in E$.

Some easy consequences of Definition 6.1 are the following. If ϑ and ψ are automorphisms of the field E, then so is their composition $\vartheta\psi$. The inverse of an automorphism is again an automorphism. As a result of these facts, the set of automorphisms of a field E is a group which we will denote $\mathscr{G}(E)$.

Definition 6.2: Let ϑ be an automorphism of the field E. We say that ϑ leaves fixed an element $\alpha \in E$ if $\vartheta(\alpha) = \alpha$. We say that ϑ leaves fixed a subset X of E if $\vartheta(\alpha) = \alpha$ for all $\alpha \in X$.

The set $E^{\vartheta} = \{\alpha \in E \mid \vartheta(\alpha) = \alpha\}$ forms a subfield of E, which we call the fixed field of ϑ. E^{ϑ} is a field because ϑ fixes 0 and 1, and the set of fixed elements is closed under addition, multiplication, and additive and multiplicative inverses. It follows that an automorphism of a number field always fixes Q since it fixes 1, and we have already shown that 1 can generate Q. The fixed field of ϑ is the largest subfield of E left fixed by ϑ.

If $\vartheta_1, \vartheta_2, \ldots, \vartheta_n$ are automorphisms of E, then the set $\{\alpha \in E \mid \vartheta_1(\alpha) = \vartheta_2(\alpha) = \ldots = \vartheta_n(\alpha) = \alpha\}$ is called the fixed field of $\vartheta_1, \vartheta_2, \ldots, \vartheta_n$.

Example 6.1: The fixed field of $\vartheta : Q(\sqrt{2}) \to Q(\sqrt{2})$ given by $\vartheta(a + b\sqrt{2}) = a - b\sqrt{2}$, for all $a, b \in Q$, is just Q.

We may argue this is true since there are no fields between $Q(\sqrt{2})$ and Q, while $Q(\sqrt{2})$ has dimension 2 over Q. Thus, as ϑ fixes a field, it must leave all of $Q(\sqrt{2})$ fixed or just fix Q. Since we know it does not leave all of $Q(\sqrt{2})$ fixed it must just fix all of Q.■

Example 6.2: Let $\zeta = e^{2i\pi/5}$ and $\vartheta : Q(\zeta) \to Q(\zeta)$ given by $\vartheta(\zeta) = \bar{\zeta} = \zeta^4$. Then the fixed field of ϑ is $Q(\sqrt{5})$.

Proof: Note that ζ satisfies $\zeta^5 - 1 = 0$. Now $g(x) = x^5 - 1 = (x-1)(x^4 + x^3 + x^2 + x + 1) = (x-1)\Phi_5(x)$, and we showed in Example 4.8 that $\Phi_5(x)$ is irreducible over Q. Thus $(x^4 + x^3 + x^2 + x + 1) = \Phi_5(x)$ is the minimal polynomial of $\zeta = e^{2i\pi/5}$ over Q. This means that $[Q(\zeta):Q] = 4$ and that ζ generates a basis $\{1, \zeta, \zeta^2, \zeta^3\}$.

Thus $Q(\zeta) = \{c_0 + c_1\zeta + c_2\zeta^2 + c_3\zeta^3 \mid c_j \in Q, j = 0,1,2,3\}$, and if β is in $Q(\zeta)$, $\beta = c_0 + c_1\zeta + c_2\zeta^2 + c_3\zeta^3$, where $c_j \in Q, j = 0,1,2,3$. Now we apply ϑ to β.

$\vartheta(\beta)=\vartheta\left(c_0+c_1\zeta+c_2\zeta^2+c_3\zeta^3\right)=c_0+c_1\zeta^4+c_2\zeta^3+c_3\zeta^2$. From the minimal polynomial we get that $\zeta^4+\zeta^3+\zeta^2+\zeta+1=0$, and hence $\zeta^4=-\left(\zeta^3+\zeta^2+\zeta+1\right)$. Thus, $\vartheta\left(c_0+c_1\zeta+c_2\zeta^2+c_3\zeta^3\right)=c_0+c_1\zeta^4+c_2\zeta^3+c_3\zeta^2$ which equals $c_0-c_1\left(\zeta^3+\zeta^2+\zeta+1\right)+c_2\zeta^3+c_3\zeta^2$ and therefore, $\vartheta\left(c_0+c_1\zeta+c_2\zeta^2+c_3\zeta^3\right)=\left(c_0-c_1\right)-c_1\zeta+\left(c_3-c_1\right)\zeta^2+\left(c_2-c_1\right)\zeta^3$. Hence, if β is in the fixed field of ϑ, we must have

$$c_0+c_1\zeta+c_2\zeta^2+c_3\zeta^3=\left(c_0-c_1\right)-c_1\zeta+\left(c_3-c_1\right)\zeta^2+\left(c_2-c_1\right)\zeta^3$$

which holds if and only if $c_1=0$ and $c_2=c_3$. Thus the elements β fixed by ϑ have the form $\beta=c_0+c_2\left(\zeta^2+\zeta^3\right)$.

Now ζ^2 and ζ^3 are complex conjugates of each other so when we add them their imaginary parts will cancel. Thus, $\zeta^2+\zeta^3$ is the real number $2\cos\left(4\pi/5\right)$, which using trigonometric identities yields that $\zeta^2+\zeta^3=-\frac{1}{2}\left(1+\sqrt{5}\right)$.

Therefore an element $\beta\in Q(\zeta)$ is fixed by ϑ if and only if $\beta=c+d\sqrt{5}$. That is, the fixed field of ϑ is $Q\left(\sqrt{5}\right)$. ■

Example 6.3: The group $G=\left\{id,\zeta\to\zeta^2,\zeta\to\zeta^3,\zeta\to\zeta^4\right\}$, where id denotes the automorphism $\zeta\to\zeta$, has fixed field Q.

Proof: We determine the fixed field of each automorphism, and then intersect the fixed fields, in order to find the fixed field or the group. Let β be in $Q(\zeta)$. Then $\beta=c_0+c_1\zeta+c_2\zeta^2+c_3\zeta^3$, where $c_j\in Q, j=0,1,2,3$.

Under $\vartheta_1 : \zeta \to \zeta^2$, $\beta = c_0 + c_1\zeta + c_2\zeta^2 + c_3\zeta^3 \to c_0 + c_1\zeta^2 + c_2\zeta^4 + c_3\zeta^1$. However, $\zeta^4 = -(\zeta^3 + \zeta^2 + \zeta + 1)$. Thus we have

$$\beta \to c_0 + c_1\zeta^2 + c_2(-(\zeta^3 + \zeta^2 + \zeta + 1)) + c_3\zeta^1 .$$

Hence, $\beta \to (c_0 - c_2) + (c_3 - c_2)\zeta^1 + (c_1 - c_2)\zeta^2 + c_2\zeta^3$. This means that $\vartheta_1(\beta) = \beta$ if and only if $c_0 = c_0 - c_2, c_1 = (c_3 - c_2), c_2 = (c_1 - c_2), c_3 = c_2$. Thus $c_1 = c_2 = c_3 = 0$ Hence the fixed field of ϑ_1 is Q.

A similar calculation for $\zeta \to \zeta^3$ shows that $\zeta \to \zeta^3$ has fixed field Q as well. From the previous example we know that $\zeta \to \zeta^4$ fixes $Q(\sqrt{5})$, and the identity automorphism fixes all of $Q(\zeta)$. Thus taking the intersection of all the fixed fields we obtain that the group $G = \{id, \zeta \to \zeta^2, \zeta \to \zeta^3, \zeta \to \zeta^4\}$ has fixed field Q.■

We have the following proposition whose proof can be found in [2, page 108]

Proposition 6.1: If F is the fixed field of a finite group G of automorphisms of E, then $[E:F] = o(G)$ (the order of G).

Example 6.4: We can say that the group $G = \{id, \zeta \to \zeta^2, \zeta \to \zeta^3, \zeta \to \zeta^4\}$, from example 6.3 can be denoted as $\mathscr{G}(Q(\zeta), Q) = \{id, \zeta \to \zeta^2, \zeta \to \zeta^3, \zeta \to \zeta^4\}$ since this group of automorphisms of $Q(\zeta)$ fixes Q. While applying Proposition 6.1 to this example we get that $[Q(\zeta):Q] = 4$

since $\mathscr{G}(Q(\zeta),Q)$ has order 4. This follows from Proposition 6.1 since according to the proposition the order of the group of automporshims is equal to the degree of the extension E over F, that is the order of the group of automorphisms is equal to the degree $Q(\zeta)$ over Q.

CHAPTER SEVEN

GALOIS EXTENSIONS

Definition 7.1: A field E is a Galois extension of F if F is the fixed field of a finite group of automorphism of E, which is called the Galois group of E over F and is denoted by $\mathscr{G}(E/F)$.

Example 7.1: $Q(\zeta)$, of Example 6.2, is a Galois extension of Q since by Examples 6.3 and 6.4 there exists a finite group of automorphisms of $Q(\zeta)$, which fixes Q. In this example $\mathscr{G}(Q(\zeta)/Q)=\{id,\zeta\to\zeta^2,\zeta\to\zeta^3,\zeta\to\zeta^4\}$, is our Galois group.

Example 7.2: $Q(\zeta)$ is a Galois extension of $Q(\sqrt{5})$ since by Example 6.2 there exists a finite group of automorphisms of $Q(\zeta)$, which fixes $Q(\sqrt{5})$. In this example $\mathscr{G}(Q(\zeta)/Q(\sqrt{5}))=\{id,\zeta\to\zeta^4\}$, is our Galois group.

Proposition 7.1 The Fundamental Theorem of Galois Theory: Let E be a Galois extension of the field F. If B is a field between E and F, then E is a Galois extension of B and $\mathscr{G}(E/B)$ is a subgroup of $\mathscr{G}(E/F)$. Furthermore, B is a Galois extension of F if and only if $\mathscr{G}(E/B)$ is a normal subgroup of $\mathscr{G}(E/F)$, in which case $\mathscr{G}(B/F)$ is isomorphic to the quotient group $\mathscr{G}(E/F)/\mathscr{G}(E/B)$.

The proof of this theorem will not be given here. Instead we will illustrate all the parts of this theorem using examples 6.2-7.1. A proof can be found in [2, page 112].

Example 7.2: Let $E=Q(\zeta)$, $B=Q(\sqrt{5})$, and $F=Q$. Since $Q(\sqrt{5})$ is between $Q(\zeta)$ and Q, and we know that $Q(\zeta)$ is a Galois extension of Q, then $Q(\zeta)$ is a Galois extension of $Q(\sqrt{5})$. Furthermore, $Q(\sqrt{5})$ is a Galois extension of Q if and only if $\mathscr{G}(Q(\zeta)/Q(\sqrt{5}))$ is a normal subgroup of $\mathscr{G}(Q(\zeta)/Q)$. Moreover in this case $\mathscr{G}(Q(\sqrt{5})/Q)$ is isomorphic to the quotient group $\mathscr{G}(Q(\zeta)/Q)/\mathscr{G}(Q(\zeta)/Q(\sqrt{5}))$, which is isomorphic to the cyclic group of order 2, Z_2. We also note here that the degree of a Galois extension is equal to the order of the Galois group, which follows from Proposition 6.1.

Now we are getting ready to answer the questions that motivated my project. However, in order to introduce the main theorem, Galois' Theorem, which helps us determine when a general polynomial is solvable by radicals, we must first introduce solvable groups.

CHAPTER EIGHT

SOLVABLE GROUPS

In order to define solvable group, we need the following six definitions.

Definition 8.1: A normal series for a finite group G is a sequence of subgroups of G, $\{e\} = G_0 \subset G_1 \subset \ldots \subset G_n = G$, such that G_{i-1} is a proper normal subgroup of G_i for $i = 1,2,\ldots,n$.

Definition 8.2: The factors of a normal series are the quotient groups $G_1/G_0, G_2/G_1, \ldots, G_n/G_{n-1}$.

Definition 8.3: A refinement of a normal series is a normal series which contains all the subgroups of the original normal series (and perhaps more).

Definition 8.4: A refinement which is not identical with the original series is called a proper refinement.

Definition 8.5: A composition series for a finite group is a normal series which has no proper refinements.

Definition 8.6: A group is simple if its only normal subgroups are itself and the trivial group.

Let us look at a few examples that illustrate the concepts just defined.

Example 8.1: Let us look at a normal series for Z_8. The subgroups of Z_8 are: $Z_8, \{0,2,4,6,\}, \{0,4\}, \{0\}$. Thus a composition series for Z_8 is:

$$\{e\} = \{0\} \subset \{0,4\} \subset \{0,2,4,6\} \subset \{0,1,2,3,4,5,6,7\} = Z_8 .$$

First we note this is a normal series since each subgroup is a proper normal subgroup of the one above it in the series since the groups are abelian.

In addition this is a series which has no proper refinement. Thus it is also a composition series. The factors of this series are $\{0,1,2,3,4,5,6,7\}/\{0,2,4,6\} \cong Z_2, \{0,2,4,6\}/\{0,4\} \cong Z_2, \{0,4\}/\{0\} \cong Z_2$. Each of these factors are simple since the only normal subgroup it has is itself and the trivial group.

Note that any group of order p, where p is prime is a simple group, since the only subgroups a group of order p can have is itself and the trivial subgroup, each which are normal subgroups.

Example 8.2: Now let us consider the Dihedral group $D_8 = \{id,(1234),(1432),(13)(24),(14)(23),(12)(34),(13),(24)\}$, and create a composition series for it. A subgroup of D_8 is $E_8 = \{id,(13)(24),(14)(23),(12)(34)\}$, the subgroup of all the even permutations in D_8, which is a normal subgroup of D_8 because it is the intersection of D_8 with a normal subgroup of S_5, namely A_5. Thus we can then finish the composition series for D_8 by letting $B = \{id,(14)(23)\}$, thus the composition series for D_8 is:

$$\{id\} \subset B \subset E_8 \subset D_8$$

as ut will follow from the next proposition. The factors of our composition series for D_8 then are $D_8/E_8 \cong Z_2, E_8/B \cong Z_2, B/\{id\} \cong Z_2$. Each of them is a simple group.

Proposition 8.1 A normal series is a composition series if and only if each factor is a simple group.

Proof: Assume that G is a finite group and that $\{e\} = G_0 \subset G_1 \subset \ldots \subset G_n = G$ is a normal series for G. If $\{e\} = G_0 \subset G_1 \subset \ldots \subset G_n = G$ is not a composition series, then we can obtain a proper refinement of $\{e\} = G_0 \subset G_1 \subset \ldots \subset G_n = G$ by inserting a new group G' into the series at some point, say $G_k \subset G' \subset G_{k+1}$. This means that G'/G_k is a nontrivial normal subgroup of G_{k+1}/G_k. Thus, G_{k+1}/G_k is not a simple group. Hence, if a normal series is not a composition series then some factors are not simple groups.

On the other hand, if G_{k+1}/G_k is not simple for some k, then there is a normal subgroup G'', such that $\{e\} \subset G'' \subset G_{k+1}/G_k$. It follows that $G'' = G'/G_k$, where $G_k \subset G' \subset G_{k+1}$, G_k is a normal subgroup of G', and G' is a normal subgroup of G_{k+1}. Thus, $\{e\} = G_0 \subset G_1 \subset \ldots \subset G_k \subset G' \subset G_{k+1} \subset \ldots \subset G_n = G$ is a proper refinement. Therefore the original series is not a composition series. Hence, if the factors are not simple, then the normal series is not a composition series. Therefore, a normal series is a composition series if and only if each factor group is a simple group.■

Definition 8.7: A finite group is solvable if it has a composition series in which each factor is a cyclic group.

Example 8.3: Z_8 is a solvable group since it has a composition series in which each factor is a cyclic group, see example 8.1.

Example 8.4: D_8 is a solvable group since it has a composition series in which each factor is a cyclic group (see Example 8.2).

Proposition 8.2: Let H be a proper normal subgroup of a group G. Then G is solvable if and only if H and G/H are solvable.

Though this proposition is quite important, it ends up not being useful for our purposes. A proof is given in [2, page 56]. One proposition that will be useful for this project is the following.

Proposition 8.3: Any subgroup of a solvable group is solvable.

Proof: Assume that H is a subgroup of a solvable group G. Since G is solvable there exists a composition series for G, say $\{e\} = G_0 \subset G_1 \subset \ldots \subset G_n = G$. Now consider the series

$$\{e\} = H_0 = H \cap G_0 \subset H_1 = H \cap G_1 \subset \ldots \subset H \cap G_n = H_n = H \qquad (8.3.1)$$

We must show that this series is a normal series and that each of the factors of this series are cyclic. To show that our series is a normal series we will show that $H \cap G_i$ is a normal subgroup of $H \cap G_{i+1}$ by proving that for all $a \in H \cap G_{i+1}$, $a(H \cap G_i)a^{-1}$ is contained in $H \cap G_i$.

Let $a \in H \cap G_{i+1}$, then $a(H \cap G_i)a^{-1}$ is contained in H, since $a \in H$. Also, $a(H \cap G_i)a^{-1}$ is contained in G_i because G_i is normal in G_{i+1}. Hence $a(H \cap G_i)a^{-1}$ is contained in $H \cap G_i$. Thus, $H \cap G_i$ is a normal subset of $H \cap G_{i+1}$

Now we show that each factor is cyclic. To do this we will need the second isomorphism theorem.

Proposition 8.4: If H and N are subgroups of a group G, and N is normal in G, then there is an isomorphism of groups, $NH/N \approx H/(H \cap N)$.

So if we let $G = G_i$, $N = G_{i-1}$, $H = H \cap G_i$, then since we know that $N = G_{i-1}$ is normal in $G = G_i$, then we have that: $G_{i-1}(H \cap G_i)/G_{i-1} \approx (H \cap G_i)/((H \cap G_i) \cap G_{i-1})$. However, $(H \cap G_i)/((H \cap G_i) \cap G_{i-1}) = (H \cap G_i)/(H \cap G_{i-1})$. Thus we have that:

$$G_{i-1}(H \cap G_i)/G_{i-1} \approx (H \cap G_i)/((H \cap G_i) \cap G_{i-1}) = (H \cap G_i)/(H \cap G_{i-1}).$$

Now, $G_{i-1}(H \cap G_i)/G_{i-1}$ is a subgroup of G_i/G_{i-1}. However, since $G_{i-1}(H \cap G_i)/G_{i-1} \approx (H \cap G_i)/((H \cap G_i) \cap G_{i-1}) = (H \cap G_i)/(H \cap G_{i-1})$ we get that $(H \cap G_i)/(H \cap G_{i-1})$ is isomorphic to a subgroup of a cyclic group, since we know that G_i/G_{i-1} is cyclic. But, any subgroup of a cyclic group is cyclic (this is proven by taking the element in the subgroup which is the smallest power of the generator of the group, and checking that this element is the generator for the subgroup.) Thus $(H \cap G_i)/(H \cap G_{i-1})$ is a cyclic group.

Therefore, (8.3.1) is a normal series whose factors are cyclic. It follows that any subgroup of a solvable group is solvable.■

Proposition 8.5: All groups with order below 60 are solvable.

One way to prove this theorem is to use the Sylow Theorems to prove it for each group of order one to fifty-nine. First we will recall the Sylow Theorems, and then verify the proposition for some groups with order between one and sixty relevant to this project. These groups are the ones that appear as transitive subgroups of S_5.

First Sylow Theorem: If p is prime and p^n divides the order of a finite group G, then G has a subgroup of order p^n.

We recall that a subgroup of G of order p^n, where p^n is the highest power of p dividing the order of G, is called a p-Sylow subgroup of G.

Second Sylow Theorem: All the p-Sylow subgroups of a finite group are conjugate.

Third Sylow Theorem: The number of p-Sylow groups of a finite group is a divisor of their common index and is congruent to 1 modulo p.

Example 8.5: A group of order p, where p is a prime, is solvable.

Proof: Let G be a group of order p. Then we note that the only subgroup of G is the trivial group. Thus the composition series for G is $\{id\} \subset G$ which is a normal series, while the only factor is $G/\{id\} = G \approx Z_p$. Since Z_p is cyclic, G is a solvable group if it has order p.■

Example 8.6: A group of order pq, where p and q are prime, is solvable.

Proof: Let G be a group of order pq, where p and q are prime and $p>q$. Then we note that p is the highest power of p that divides pq. Thus the First Sylow Theorem guarantees us that G has a p-Sylow subgroup of order p, call it B. Thus, by the Third Sylow Theorem the number of p-Sylow groups must be a divisor of q and congruent to 1 modulo p, the only such number is the number 1. Thus, there is only one p-Sylow group of order p, and by the Second Sylow Theorem this subgroup equals each of its conjugates, thus it must be normal. Thus we can create a composition series were each factor is cyclic. Hence G is solvable. (The series is the series $id \subset B \subset G$, and the factors are $G/B \approx Z_q, B/id \approx Z_p$).■

Example 8.7: A group of order 5 is solvable.

Proof: This follows directly from Example 8.5.■

Example 8.8: A group of order 10 is solvable.

Proof: This follows directly from Example 8.5.■

The fact we just proved, that any group of order 10 has a normal subgroup of order 5, will be important in the next proof.

Example 8.9: A group of order 20 is solvable.

Proof: Let G be a group of order 20. Then we note that 5 is the highest power of 5 that divides 20. Thus the First Sylow Theorem guarantees us that G has a 5-Sylow subgroup of order 5, call it B. Thus by the Third Sylow Theorem the number of 5-Sylow groups must be a divisor of 4 and congruent to 1 modulo 5, the only such number is the number 1. Thus, there is only one 5-Sylow group of order 5, and by the Second Sylow Theorem 2 this subgroup equals each of its conjugates, thus it must be normal. So we can create a normal series $id \subset B \subset G$. Now, G/B will either be isomorphic to Z_4 or K_4 since they are the only two groups of order four up to isomorphisms. For example, $Z_2 \times Z_2$ is isomorphic to K_4, the Klein group. If it is isomorphic to Z_4 then the factors of the normal series are cyclic, and we have the composition series $\{e\} \subset Z_2 \subset Z_4 \subset G$. Thus G is solvable in this case.

If G/B is not isomorphic to Z_4, then G/B is isomorphic to K_4, which is isomorphic to $Z_2 \times Z_2$. Thus G/B has a normal subgroup isomorphic to Z_2. However, recall the theorem which states that if you have a quotient map $\psi: G \to G/H$, H normal, that if K is a normal subgroup of G/H, then $\psi^{-1}(K)$ is a normal subgroup of G. Thus, since Z_2 is a normal subgroup of K_4, by our quotient map $\psi: G \to K_4$, there exists a normal subgroup of G of order 10, let's call it C, such that $\psi(C) = Z_2$. As a result, we could then begin a new series which starts with G, continues with C, and then by Example 8.8, C is guaranteed to have a normal subgroup of order 5, call it A. Thus, we have the series:

$$\{e\} \subset A \subset C \subset G$$

which is a composition series whose factors have all prime order since $G/C \approx Z_2$, $C/A \approx Z_2$, and $A/\{id\} \approx Z_5$, and therefore are cyclic. Thus any group of order 20 is solvable.■

CHAPTER NINE
SYMMETRIC GROUPS
AND SOLVABILITY

The symmetric groups and their subgroups appear as Galois groups of polynomials. In Chapter 10 we will be determine the Galois groups of quintics. We study symmetric groups to prepare the ground for our work.

One family of groups that will be important for our purpose is the symmetric groups and their subgroups.

Definition 9.1: The set S_n is the set of all permutations on n letters. S_n is called the symmetric groups, and it forms a group under the operation of composition.

Definition 9.2: Let $a_1,\ldots,a_k$ be distinct positive integers. The k-cycle $(a_1 \ldots a_k)$ is the permutation which carries a_1 to a_2, a_2 to a_3, ..., and a_k to a_1.

We will use cycle notation throughout this paper.

Example 9.1: $S_3 = \{id, (123), (132), (12), (13), (23)\}$.

Definition 9.3: A cyclic permutation of order 2 $(a_1 a_2)$ which simply interchanges a_1 and a_2 is called a transposition.

Definition 9.4: An even permutation is one that can be written as the product of an even number of transpositions.

Definition 9.5: The subset of all even permutations of S_n is called the alternating group and it is denoted by A_n and is a subgroup of S_n.

Example 9.2: $A_3=\{id,(123),(132)\}=\{id,(12)(23),(13)(23)\}$

Proposition 9.1: Every permutation of n letters is the product of disjoint cyclic permutations in exactly one way, except for the order of the factors.

Proof: Let $\pi\in S_n$. Define the relation $x\equiv_\pi y$ if and only if $y=\pi^i(x)$. It is easy to check that this is an equivalence relation. Thus, $\equiv_\pi$ induces a decomposition of $\{1,2,..n\}$ into disjoint subsets. Since $\equiv_\pi$ is an equivalence relation, these are equivalence classes. Take an equivalence class S, and $s\in S$. Then there is a smallest positive integer m such that $\pi^m(s)=s$. It follows that π restricted to S is the $m-cycle$ $(s\pi(s)...\pi^{m-1}(s))$.

Let $\alpha_1,...,\alpha_k$ be the cycles that π induces in the equivalence classes. These cycles are disjoint, as the equivalence classes are disjoint. We claim that $\pi=\alpha_1...\alpha_k$. In fact, if $a\in\{1,2,...,n\}$, say a is in the i^{th} equivalence class, on which π is the cycle α_i, then $\pi(a)=\alpha_i(a)$. On the other hand, $\alpha_1..\alpha_k(a)=\alpha_i(a)$, as the cycles are disjoint. Thus, $\pi=\alpha_1...\alpha_k$. The cycles are unique, as the equivalence classes are also unique.■

Proposition 9.2: S_n is generated by the transpositions (12), (23), ..., $((n-1)n)$.

Outline of proof: First we will note that using the transpositions (12), (23), ..., $((n-1)n)$ we can get any transposition of the form $(1k)$ for $k=2,3,..n$, or example we can get $(14)=(12)(23)(34)(32)(21)$ and say $(35)=(34)(45)(43)$. Once we have that, we can use the fact that any cycle can be written as the product of transpositions in the following way: $(a_1a_2a_3...a_{k-1}a_k)$ as $(a_1a_k)(a_1a_{k-1})...(a_1a_3)(a_1a_2)$. Thus any element of S_n could be obtained as a product of transpositions, as any element of S_n is a product of disjoint cycles.■

Proposition 9.3: S_n is generated by the transposition (12) and the n-cycle $(12...n)$:

Outline of proof: We can generate all the transpositions of the form $((k-1)k)$ for $k=2,...,n$ by taking $(123...n)(12)(n...321)=(23)$, and then obtaining $(123...n)(23)(n...321)=(34)$ until you have all the transpositions (12), (23), . . . , $((n-1)n)$. Then by Proposition 9.2, all of S_n will be generated by (12) and $(12...n)$.■

Proposition 9.4: Every even permutation on n letters, $n\geq 3$, is the product of cyclic permutations of order 3.

First note that there are no cyclic permutations of order 3 in S_n for $n=1$ or $n=2$, but there is always an even permutation, namely the identity. Therefore the proposition is false for $n<3$.

Proof: We will now prove the proposition for $n\geq 3$ using induction.

The even permutations for $n=3$ are the identity, $(123)=(12)(23)$, and $(132)=(13)(23)$. Since (123) and (132) are of order 3, and $(123)(132)=id$, the proposition holds for $n=3$.

Now suppose that the proposition holds true for every $k<n$, and suppose we have an element of A_n, call it π. Let $\pi(k)=\pi_k$. The permutation $\sigma=(\pi_n ni)\cdot\pi$, where $\pi_i=n$, satisfies $\sigma(n)=(\pi_n ni)\pi(n)=(\pi_n ni)\pi_n=n$, and is even. Since σ leaves n fixed and is an even permutation, the induction hypothesis yields that σ is the product of 3-cycles, say $\sigma=\alpha_1\alpha_2..\alpha_n$. Setting $\alpha_0=(\pi_n in)$ we have $\alpha_0\alpha_1\alpha_2..\alpha_n=\alpha_0\sigma=(\pi_n in)(\pi_n ni)\pi=\pi$ and thus we have expressed π as a product of 3-cycles.■

Proposition 9.5: The alternating group A_n is simple except when $n=4$.

Proof: In the case of $n=4$ we know that A_4 is not simple because it has a normal subgroup of order 4, $\{id,(13)(24),(14)(23),(12)(34)\}$. In the case that $n<4$ the order of A_n is either 1 or 3, thus A_n must be simple. Now consider the case in which $n>4$.

Let N be a nontrivial normal subgroup of A_n for $n>4$. We must show that $N=A_n$. The first step is to see that N contains a 3-cycle. Let $\alpha\neq id$ be an element of N which leaves fixed as many elements of $\{1,2,...,n\}$ as possible. As guaranteed by Proposition 9.1, let $\alpha=\alpha_1\alpha_1...\alpha_s$ where α_i are disjoint cycles, which we can assume are in order of decreasing length. Renumbering if necessary, we may assume that $\alpha_1 = (12...k)$ and, when $s > 1$, that $\alpha_2 = ((k+1)(k+2)...l)$. There are several cases to consider.

Case 1: α moves each of the numbers $1,2,3,4,5$. (This occurs when $s > 2$, when $s = 2$ and $\alpha = (12...k)((k+1)(k+1)...l)$ with $l > 4$, or when $s = 1$ and $\alpha = \alpha_1 = (12..k)$ for $k > 4$.) Setting $\beta = (345)$, the element $\beta^{-1}\alpha^{-1}\beta$ belongs to the normal subgroup we called N, and thus $\beta^{-1}\alpha^{-1}\beta\alpha \in N$. However, the permutation $\beta^{-1}\alpha^{-1}\beta\alpha$ leaves
the number 1 fixed in addition to leaving fixed all the elements fixed by α. This is a contradiction of the choice of α, thus Case 1 is impossible.

Case 2: α moves each of the numbers $1,2,3,4$ and no others. (This occurs when $\alpha = (12)(34)$, since (1234) is an odd permutation.) Setting $\beta = (345)$ again allows the element $\beta^{-1}\alpha^{-1}\beta$ to belong to the normal subgroup we called N, and thus $\beta^{-1}\alpha^{-1}\beta\alpha \in N$. However, if we compute $\beta^{-1}\alpha^{-1}\beta\alpha$, $\beta^{-1}\alpha^{-1}\beta\alpha = (345) = \beta$. Thus, $\beta \in N$ and β moves fewer elements than α. This contradiction makes Case 2 impossible.

Case 3: α moves each of the numbers $1,2,3$ and no others. (This occurs when $\alpha = (123)$) There are no other cases to consider now that cases 1 and 2 have been eliminated. Thus, we have shown that N contains a $3-cycle$, which without loss of generality we can assume is (123).

We can see that N contains all $3-cycles$ by letting an even permutation by denoted as $\sigma = \begin{pmatrix} 1 & 2 & 3 & \ldots \\ i & j & k & \ldots \end{pmatrix}$. Then, $\sigma(123)\sigma^{-1} = (ijk)$ belongs to the normal subgroup N. If we vary i,j, and k, we will obtain all the $3-cycles$. Thus since every even permutation of n letters, $n \geq 3$, is the product of cyclic permutation of order 3, $N = A_n$.■

Proposition 9.6: A_n is not abelian for $n > 3$.

Proof: This is true since for example $(123)(234) = (12)(34)$ but $(234)(123) = (13)(24)$ and $(13)(24) \neq (13)(24)$, and these permutations are in all A_n for $n > 3$.■

It follows from Proposition 9.5 that the only proper normal subgroups of S_n are A_n and $\{id\}$. Thus the normal series for S_n given in the following proposition is the only possible normal series for S_n. It also follows from Proposition 9.5 that A_n is not solvable.

Proposition 9.7: For $n > 4$, the symmetric group S_n is not solvable.

Proof: For $n > 4$ we know that A_n is simple, thus the only possible normal series for S_n, $\{id\} \subset A_n \subset S_n$, is a composition series for S_n. However, A_n is not abelian for $n > 3$ as shown above in Proposition 9.6. Also, there is not one generator for A_n for $n > 3$, thus A_n is not cyclic. Thus our factor groups which are A_n and Z_2 are not both cyclic. Thus, S_n is not solvable for $n > 4$.■

Definition 9.6: A subgroup H of S_n is transitive if for every pair of elements $i,j \in \{1,2,\ldots,n\}$ there is an element or permutation $\pi \in H$ such that $\pi(i) = j$.

Proposition 9.8: Let H be a transitive subgroup of S_p where p is a prime number. If H contains a transposition, then $H = S_p$.

Proof: Suppose without loss of generality that (12) is the transposition that H contains. Define an equivalence relation on the set $\{1,2,\ldots,p\}$ as $i \sim j$ if and only if the transposition $(ij) \in H$. Since H is transitive each equivalence class has the same number of elements. In fact, if there is an element in H, call it ϕ, such that $\phi_1 = \phi(1) = i$, then ϕ yields a one to one correspondence from the equivalence class of 1 to that of i since $(1k) \in H$ if and only if $(i\phi_k) = (\phi_i\phi_k) = \phi \cdot (1k) \cdot \phi^{-1} \in H$. That is any element equivalent to i must also be equivalent to k. The number of elements in any equivalence class, call it s, must divide the prime p, and thus $s = 1$ or $s = p$.

On the other hand, the equivalence class of 1 contains at least 2 elements 1 and 2. Therefore there can only be one equivalence class which has p elements. Therefore, H contains all the transpositions of S_p. Since every permutation is a product of transpositions, we have that $H = S_p$.■

CHAPTER TEN
MOVING TOWARDS QUINTIC EXAMPLES

As we consider which quintics are solvable by radicals, we will begin to see the importance of Proposition 9.8. Before we can actually get to our examples we will need six propositions.

In this, and in the following chapters, we will consider only irreducible polynomials as some of our theorems only work with irreducible polynomials.

Definition 10.1: Let f be a polynomial over a number field F. The equation $f(x)=0$ is said to be solvable by radicals if all the roots of f can be obtained from elements of F by a finite sequence of rational operations (addition, subtraction, multiplication, and division) and extractions of n^{th} roots.

Proposition 10.1 (Galois' Theorem): Let f be a polynomial over a number field F and let E be its splitting field. The equation $f(x)=0$ is solvable by radicals if and only if the Galois group $\mathscr{G}(E/F)$ is solvable.

This proposition is essential in determining whether or not a quintic polynomial is solvable by radicals, but due to the length of the proof we will not give it here. The proof is given in [2, page 135].

This proposition tells us that if we have a polynomial over Q whose Galois group is solvable, then the polynomial is solvable by radicals. Thus, this proposition is very important to us as it implies that what we must do to find a quintic polynomial which is solvable by radicals is to find a quintic whose Galois group is solvable.

Once we know what has to be accomplished we may begin to search for some quintic polynomials that are solvable by radicals. We will need five other very important propositions.

The first proposition is related to the fact that the Galois group $\mathscr{G}(E/Q)$ for any quintic f over Q is a permutation group of the roots $\alpha_1,\alpha_2,\alpha_3,\alpha_4,\alpha_5$ of f and is isomorphic to a subgroup of S_5. This is so, because each $\phi \in \mathscr{G}(E/Q)$ leaves Q fixed, and $\phi(f\alpha_i)=f(\phi\alpha_i)=0$. Hence $\phi\alpha_i$ is again a root of f. Furthermore we also have:

Proposition 10.2: If f is an irreducible polynomial over Q, $\mathscr{G}(E/Q)$ must be a transitive permutation group of the roots of f.

Proof: We must show that given two roots α_i and α_j, there is some $\phi \in \mathscr{G}(E/Q)$, such that $\phi(\alpha_i)=\alpha_j$. If this were not the case, then the polynomial $g(x)=(x-\alpha_1)(x-\alpha')...(x-\alpha'')$, in which $\alpha_1,\alpha',...,\alpha''$ are distinct images of α_1 under $\mathscr{G}(E/Q)$, would be fixed by $\mathscr{G}(E/Q)$ and have coefficients in Q. This means that $g(x)$ would be a proper divisor of f, contradicting the fact that f is irreducible. Thus given two roots α_i and α_j, there is some $\phi \in \mathscr{G}(E/Q)$, such that $\phi(\alpha_i) = \alpha_j$, that is $\mathscr{G}(E/Q)$ must be a transitive permutation group of the roots of f.■

This fact leads us to wonder what are the transitive subgroups of S_5.

Proposition 10.3: The only transitive subgroups of S_5 are Z_5, D_{10}, W, A_5, and all of S_5 itself.

Here W is a group of order 20 known as the Frobenius group, generated by (12345) and (2354), and D_{10} is the set of rotations and reflections of a regular pentagon.

Since Z_5 has order 5, D_{10} has order 10, and W has order 20, each are solvable by Proposition 8.5. On the other hand we have seen that A_5 and S_5 are not solvable by Propositions 9.5 and 9.7 respectively.

Corollary 10.1: A quintic with Galois group isomorphic to Z_5, D_{10} , or W, is solvable by radicals.

Corollary 10.2: A quintic with Galois group isomorphic to A_5 or to S_5 is not solvable by radicals.

In order to help us look at the subgroups of the Galois groups of quintics, we will need the following three results. We will not provide the proof of the first one.

Proposition 10.4: Suppose that f is a monic polynomial over Z and that p is a prime. Let $\bar{f}$ be the corresponding polynomial over Z_p. If f has distinct roots in a splitting field extension L of Q, then the cyclic group $\mathscr{G}(B / Z_p)$ of the roots of $\bar{f}$ is isomorphic to a subgroup of $\mathscr{G}(L / Q)$.

What this proposition does, is that it allows us to mod our quintic into a prime finite field, and then look at the cyclic group of the polynomial over Z_p formed by the roots of $\overline{f}$. That group is isomorphic to a subgroup of the Galois group of the original equation by Proposition 10.4. This will help us determine which one of the transitive subgroups of S_5 is the Galois group.

In order to determine the prime numbers which are useful to mod out by, we use the discriminant.

Definition 10.2: The discriminant, Δ, of a polynomial f over Q is the quantity

$$\delta^2 = \left(\prod_{1 \le i < j \le n} (\alpha_j - \alpha_i) \right)^2 ,$$

where $\alpha_1, \alpha_2, \ldots, \alpha_n$ are the roots of the polynomial f.

The discriminant is easy to find when you know the roots. However, when we are trying to obtain examples of quintics, we usually do not know the roots, and usually can not find them explicitely. Thus, determining the discriminant can be quite a task when the roots cannot be found.

However, one of the goals of this project is to try and find examples of quintics that are solvable by radicals. The following proposition determines the discriminant for a family of polynomials that we will use to generate examples of solvable quintics.

Proposition 10.5: Suppose $f(x) = x^5 + px + q$. Then the discriminant of f, Δ, is equal to $5^5q^4 + 4^4p^5$.

Proof: Let $\alpha_1, \alpha_2, \alpha_3, \alpha_4,$ and α_5 be the roots of the quintic $f(x) = x^5 + px + q$. We know that the discriminant is defined to be:

$$\Delta = \delta^2 = \left(\prod_{1 \le i < j \le n} (\alpha_j - \alpha_i) \right)^2$$

To derive the discriminant for any quintic polynomial it is helpful to observe that $\sqrt{\Delta}$ can be expressed as Vandermonde's determinant:

$$\sqrt{\Delta} = \det \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 & \alpha_5 \\ \alpha_1^{\ 2} & \alpha_2^{\ 2} & \alpha_3^{\ 2} & \alpha_4^{\ 2} & \alpha_5^{\ 2} \\ \alpha_1^{\ 3} & \alpha_2^{\ 3} & \alpha_3^{\ 3} & \alpha_4^{\ 3} & \alpha_5^{\ 3} \\ \alpha_1^{\ 4} & \alpha_2^{\ 4} & \alpha_3^{\ 4} & \alpha_4^{\ 4} & \alpha_5^{\ 4} \end{bmatrix} = \det \begin{bmatrix} 1 & \alpha_1 & \alpha_2^{\ 2} & \alpha_3^{\ 3} & \alpha_4^{\ 4} \\ 1 & \alpha_1 & \alpha_2^{\ 2} & \alpha_3^{\ 3} & \alpha_4^{\ 4} \\ 1 & \alpha_1 & \alpha_2^{\ 2} & \alpha_3^{\ 3} & \alpha_4^{\ 4} \\ 1 & \alpha_1 & \alpha_2^{\ 2} & \alpha_3^{\ 3} & \alpha_4^{\ 4} \\ 1 & \alpha_1 & \alpha_2^{\ 2} & \alpha_3^{\ 3} & \alpha_4^{\ 4} \end{bmatrix} \qquad (10.1)$$

this means that Δ can be expressed as the determinant of the product of the two matrices. This means that:

$$\Delta = \det\begin{bmatrix} \pi_0 & \pi_1 & \pi_2 & \pi_3 & \pi_4 \\ \pi_1 & \pi_2 & \pi_3 & \pi_4 & \pi_5 \\ \pi_2 & \pi_3 & \pi_4 & \pi_5 & \pi_6 \\ \pi_3 & \pi_4 & \pi_5 & \pi_6 & \pi_7 \\ \pi_4 & \pi_5 & \pi_6 & \pi_7 & \pi_8 \end{bmatrix} \qquad (10.2)$$

where $\pi_i = \alpha_1^{\,i} + \alpha_2^{\,i} + \alpha_3^{\,i} + \alpha_4^{\,i} + \alpha_5^{\,i}$. In order to find this determinant we must first find expressions for each π_i in terms of our coefficients.

Since $\alpha_1,\alpha_2,\alpha_3,\alpha_4,$ and α_5 are the roots of the quintic $f(x) = x^5 + px + q$, we can assume that there exists some splitting field E, in which $f(x)$ factors as:

$$f(x) = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)(x-\alpha_4)(x-\alpha_5)$$

expanding this yields:

$$\begin{gathered} x^5 \\ +(\alpha_1+\alpha_2+\alpha_3+\alpha_4+\alpha_5)x^4 \\ +(\alpha_1\alpha_2+\alpha_1\alpha_3+\alpha_1\alpha_4+\alpha_1\alpha_5+\alpha_2\alpha_3+\alpha_2\alpha_4+\alpha_2\alpha_5+\alpha_3\alpha_4+\alpha_3\alpha_5+\alpha_4\alpha_5)x^3 \\ +\begin{pmatrix} \alpha_1\alpha_2\alpha_3+\alpha_1\alpha_2\alpha_4+\alpha_1\alpha_2\alpha_5+\alpha_1\alpha_3\alpha_4+\alpha_1\alpha_3\alpha_5 \\ +\alpha_1\alpha_4\alpha_5+\alpha_2\alpha_3\alpha_4+\alpha_2\alpha_3\alpha_5+\alpha_2\alpha_4\alpha_5+\alpha_3\alpha_4\alpha_5 \end{pmatrix}x^2 \\ +(\alpha_1\alpha_2\alpha_3\alpha_4+\alpha_1\alpha_2\alpha_3\alpha_5+\alpha_1\alpha_2\alpha_4\alpha_5+\alpha_1\alpha_3\alpha_4\alpha_5+\alpha_2\alpha_3\alpha_4\alpha_5)x \\ -\alpha_1\alpha_2\alpha_3\alpha_4\alpha_5 \end{gathered}$$

Recall that in general, the elementary symmetric functions denoted $\sigma_k(x_1,x_2,\ldots,x_n)$ are the sum of all the monomials $x_{i_1}x_{i_2}\ldots x_{i_k}$, where $i_1 < i_2 < \ldots < i_k$. For our purposes we need only to note that:

$$\sigma_1(\alpha_1,\alpha_2,\alpha_3,\alpha_4,\alpha_5) = \alpha_1+\alpha_2+\alpha_3+\alpha_4+\alpha_5,$$

$$\pi_3 = 3\sigma_3 - \sigma_2\pi_1 + 2\sigma_1\pi_2 = 0$$

$$\pi_4 = \sigma_3\pi_1 - \sigma_2\pi_2 + \sigma_1\pi_4 - 4\sigma_4 = -4p$$

$$\pi_5 = 5\sigma_5 - \sigma_4\pi_1 + \sigma_3\pi_2 - \sigma_2\pi_3 + \sigma_1\pi_4 = -5q$$

$$\pi_6 = -\sigma_5\pi_1 + \sigma_4\pi_2 - \sigma_3\pi_3 + \sigma_2\pi_4 - \sigma_1\pi_5 = 0$$

$$\pi_7 = \sigma_5\pi_2 - \sigma_4\pi_3 + \sigma_3\pi_4 - \sigma_2\pi_5 + \sigma_1\pi_6 = 0.$$

Once we have derived these we can then see that

$$\pi_8 = \sigma_5\pi_3 - \sigma_4\pi_4 + \sigma_3\pi_5 - \sigma_2\pi_6 + \sigma_1\pi_7 = 4p^2.$$

Using this we now know that matrix for which we need to calculate the determinant is

$$A = \begin{bmatrix} 5 & 0 & 0 & 0 & -4p \\ 0 & 0 & 0 & -4p & -5q \\ 0 & 0 & -4p & -5q & 0 \\ 0 & -4p & -5q & 0 & 0 \\ -4p & -5q & 0 & 0 & 4p^2 \end{bmatrix}.$$

We can check that the determinant of a matrix B of the form

$$\begin{bmatrix} 5 & 0 & 0 & 0 & a \\ 0 & 0 & 0 & a & b \\ 0 & 0 & a & b & 0 \\ 0 & a & b & 0 & 0 \\ a & b & 0 & 0 & c \end{bmatrix}$$

has determinant $-5a^3c + 5b^4 + a^5$, thus substituting in $a = -4p$, $b = -5q$, and $c = 4p^2$ yields that

$$\det A = 5\left(4^4 p^5\right) + 5^5 q^4 - 4\left(4^4 p^5\right) = 4^4 p^5 + 5^5 q^4.$$

Thus, if $f(x) = x^5 + px + q$ then the discriminant of f, Δ, is equal to $5^5 q^4 + 4^4 p^5$.■

A similar but more lengthy proof will show that if $f(x) = x^5 + nx^2 + px + q$ then the discriminant of f, Δ, is equal to

$$3^3\cdot 5\cdot 11 n^4 p^2 - 2^4\cdot 3^3 n^5 q + 2^6\cdot 5\cdot 13 n p^3 q + 2^5\cdot 3^2\cdot 5^2 n^2 p q^2 + 2^9\cdot 3 p^5 - 2^7\cdot 5 n p^4 + 5^5 q^4 .$$

Proposition 10.5 is helpful because modding out by one of the prime factors of the discriminant will give us a polynomial with zero discriminant in the prime field, Z_p, and therefore no information on the Galois group of the original polynomial. Thus, we should mod out by a prime which is not a factor of the discriminant in order to be able to obtain information about the Galois group of the polynomial.

Proposition 10.7: Assume $f(x)$ is a polynomial over Q and let Δ be the discriminant of $f(x)$, and let E be the splitting field for $f(x)$, then

(i) If $\Delta = 0$, $f(x)$ has a repeated root in E.

(ii) If $\Delta \neq 0$ and Δ has a square root in Q, then $\mathscr{G}(E/Q) \subseteq A_n$.

(iii) If Δ has no square root in Q, then $\mathscr{G}(E/Q) \not\subset A_n$.

Proof: (i) holds since if $\Delta = 0$, then two of our roots are equal, which means $f(x)$ has a repeated root in E.

(ii) Assume $\Delta \neq 0$ and Δ has a square root in Q. Then, $p = \sqrt{\Delta} = \prod_{1 \leq i < j \leq n} (\alpha_j - \alpha_i) \in Q$. Take $\sigma \in \mathscr{G}(E/Q)$, then $\sigma(p) = p$ as p belongs to the fixed field. However, the only way to fix p would be for σ to be an even product of transpositions, otherwise σ would switch an odd number of signs, $\sigma(p) = -p$, and p would not be fixed. Thus, $\sigma \in A_n$. Thus $\mathscr{G}(E/Q) \subseteq A_n$.

(iii) Follows directly from the fact that (ii) is true.■

Propositions 9.8 and 10.1-10.7 will now allow us to give a plethora of examples of quintic polynomials that are and are not solvable by radicals. These examples are given in the next chapter.

CHAPTER ELEVEN

QUINTIC EXAMPLES

AND THE METHOD

To determine whether a quintic is solvable or not, we have devised the following method. Please note that this method will not always allow you to determine whether a quintic is solvable by radicals, but in many of the polynomials we found it has been useful.

This method only applies to irreducible quintics.

Step One: Given a quintic $p(x)$, we first make sure that it is irreducible over Q. Then we determine the types of roots of the quintic, using calculus and elementary Algebra. If $p(x)$ has 3 real roots and 2 complex roots, then you can conclude that the quintic is not solvable by radicals, as follows. In this case, since the Galois group G, must be transitive by Proposition 10.2 and it also contains a transposition, G is isomorphic to S_5 by Proposition 9.8, which is not a solvable group by Proposition 9.7. Thus, $p(x)$ is not solvable by radicals by Proposition 10.1.

If $p(x)$ has all real roots, this research project has not been able to determine a process for whether this quintic is solvable by radicals. If $p(x)$ has 1 real root and 4 complex roots, then move onto step two.

Step Two: Using the discriminant we mod out $p(x)$ into an appropriate prime field, in order to determine the cyclic subgroups of G. These subgroups will allow us to determine whether G is solvable using Proposition 10.7.

This two step method works for a sufficiently large set of quintic polynomials, and it has allowed us here to find examples of quintics that are solvable by radicals. Of course, there are other means, different from our method, of analyzing a quintic polynomial. Examples 11.10 and 11.11 illustrate two other such possibilities.

Example 11.1: $f(x)=x^5-4x-2$ is not solvable by radicals.

First we determine that $f(x)=x^5-4x-2$ is irreducible using the Eisenstein criterion with $p=2$, since 2 divides all the coefficients except the leading one, while 2^2 does not divide 2, the constant term. Now we use calculus to try and determine the number of real roots, since we cannot find out the five roots by hand. Taking the first derivative yields

$f'(x)=5x^4-4$, thus $f'(x)$ has roots at $\pm\sqrt[4]{4/5}$. This means, that $f(x)$ has relative extrema at $\pm\sqrt[4]{4/5}$, which means there could be real roots on either side of both $\pm\sqrt[4]{4/5}$. Now we check by plugging in numbers on both sides of $\pm\sqrt[4]{4/5}$ as shown in Figure 3.

x	-2	-1.5	-1	-.5	0	.5	1	1.5	2
f(x)	-26	-3.59	1	-.031	-2	-3.96	-5	-.406	22
+/-	-	-	+	-	-	-	-	-	+

Figure 3. Roots For Example 11.1

Using the above figure we can see that $f(x)$ has real roots between -1.5 and -1, -1 and -.5, and 1.5 and 2. Thus $f(x)$ has three real roots. This means that $f(x)$ has 2 complex roots. Let the three real roots be α_3, α_4, and α_5, and the two complex roots be α_1 and α_2. Then, the automorphism γ which will carry the complex number $a+bi$ to its complex conjugate will interchange α_1 and α_2, while fixing our three real roots α_3, α_4, and α_5. Thus, γ will be in the Galois group $\mathscr{G}(E/Q)$, where $E = Q(\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5)$. However, we know that $\mathscr{G}(E/Q)$ is isomorphic to a transitive subgroup of S_5, and that it contains the transposition $(1,2)$, our first two roots are permuted, thus by Proposition 9.8, $\mathscr{G}(E/Q)$ is isomorphic to all of S_5, which is a non-solvable group. Thus by Proposition 10.1, the quintic polynomial $f(x) = x^5 - 4x - 2$ is not solvable by radicals.■

The procedure in Example 11.1 can be used to analyze each of the Examples 11.2 to 11.5. In each case we can verify that each polynomial is irreducible using the Eisenstein Criterion, and then apply calculus like in

Example 11.1 to get that each polynomial has three real roots and two complex ones, thus giving us quintics that are not solvable by radicals.

Example 11.2: $f(x)=2x^5-10x+5$ is not solvable by radicals.

Example 11.3: $f(x)=x^5-4x^2+2x-2$ is not solvable by radicals.

Example 11.4: $f(x)=x^5+9x^4-6x^3-3x^2+3x-3$ is not solvable by radicals.

Example 11.5: $f(x)=2x^5-7x^3-7x+7$ is not solvable by radicals.

The past examples were quite easy to characterize because each one had 3 real roots and 2 complex roots. We ask what can be done in the case in which $f(x)$ has 1 real and 4 complex roots. Here is what this research has found.

Example 11.6: $f(x)=x^5+20x+16$ is not solvable by radicals.

First we need to determine whether or not $f(x)=x^5+20x+16$ is irreducible. We will do this by considering $f(x-1)=(x-1)^5+20(x-1)+16=x^5-5x^4+10x^3-10x^2+25x-5$. By the Eisenstein criterion with $p=5$, $f(x-1)$ is irreducible, since 5 divides all the coefficients except the leading one, while 5^2 does not divide -5, the constant term. Now since $f(x-1)$ is irreducible then $f(x)=x^5+20x+16$ is irreducible since $f(x-1)$ is just a linear transformation of $f(x)$.

Now we use calculus to try and determine the number of real roots, since we cannot determine our five roots explicitly. Taking the first derivative yields $f'(x)=5x^4+20$, thus $f'(x)$ has roots at $\pm\sqrt[4]{-4}$, this means that $f'(x)$ has no real roots, thus $f(x)$ has no relative extrema. But $f'(x)>0$, so $f(x)$ is always increasing, and thus $f(x)$ has a real root as shown below in Figure 4.

x	-2	-1.5	-1	-.5	0	.5	1	1.5	2
f(x)	-56	-21.6	-5	5.9	16	26.03	37	n/a	n/a
+/-	-	-	-	+	+	+	+	+	+

Figure 4. Roots For Example 11.6

Using the above figure we can see specifically that $f(x)$ has a real root between -1 and -.5. Thus $f(x)$ has one real root. This means that $f(x)$ has 4 complex roots.

Now we find the discriminant of $f(x)$ using Proposition 10.5. Since $f(x)=x^5+20x+16$ we get $\Delta=5^5q^4+4^4p^5=5^5 16^4+4^4 20^5=5^5 2^{16}+2^8 2^{10}5^5=5^5 2^{16}(1+2^2)=2^{16}5^6$. Thus $\Delta=2^{16}5^6$. Since $\Delta=2^{16}5^6$ is a perfect square we know that by

Proposition 10.7 the Galois group of $f(x)$ must be a subgroup of A_5. We will determine whether it is a proper subgroup or all of A_5. To do this we mod out $f(x) = x^5 + 20x + 16$ into a prime finite field other than 2 or 5, else the polynomial would become unuseful. The lowest prime we have left is 3.

So $f(x) = x^5 + 20x + 16$ mod 3 is $f(x) = x^5 - x + 1$. Checking all the numbers in Z_3, $f(x) = x^5 - x + 1$ is irreducible over Z_3. Thus it does not factor over Q, and we do not get any more information about the Galois group, since this implies that the Galois group has a subgroup of order 5, and all the transitive subgroups of S_5 have subgroups of order five.

The next prime finite field we look at is Z_7. We see that $f(x) = x^5 + 20x + 16$ mod 7 is $\overline{f(x)} = x^5 + 6x + 2$. Using synthetic division we can check that in Z_7, $\overline{f(x)}$ factors as $(x+2)(x+3)(x^3 + 2x^2 - 2x - 2)$. Using synthetic division and checking all the numbers in Z_7, it can be shown that the cubic $(x^3 + 2x^2 - 2x - 2)$ is irreducible in Z_7. This means the roots of $\overline{f(x)}$ form a cyclic group of order three. Using Proposition 10.4 we obtain that the Galois group generated by the roots of $f(x) = x^5 + 20x + 16$ has a subgroup isomorphic to a cyclic group of order 3. However, since we know that the Galois group of $f(x)$ must be a transitive subgroup of A_5 we have A_5, D_{10}, and Z_5 to choose from. But the Galois group of $f(x)$ must also have a subgroup of order 3. Thus the Galois group of $f(x)$ must be isomorphic to A_5 since D_{10}, and Z_5 cannot have subgroups of order 3. Therefore, since A_5 is not a solvable group, the Galois group is not solvable and by Proposition 10.1, $f(x)=x^5+20x+16$ is not solvable by radicals.■

The following two examples show quintics which are not solvable by radicals. The first one having a discriminant that is not a perfect square, the second one having a perfect square discriminant.

Example 11.7: $f(x)=x^5+15x+6$ is not solvable by radicals. In this case $f(x)=x^5+15x+6$ is clearly irreducible by the Eisenstein Criterion. Using calculus we see that there is one real root and 4 complex roots. The discriminant is $2^4 3^4 5^5 7^2$, and thus is not a perfect square. Thus by Proposition 10.7 it must have a Galois group which is not a subgroup of A_5. Hence the Galois group must be S_5 or W. Now our next step is to mod $f(x)$ into an appropriate prime finite field. The prime finite field we look at next is Z_{11}. We see that $f(x)=x^5+15x+6$ mod 11 is $\overline{f(x)}=x^5+4x+6$. Using synthetic division we can check that in Z_{11}, $\overline{f(x)}$ factors as $(x+10)(x+4)(x^3-3x^2+2x+4)$. Using synthetic division and checking all the numbers in Z_{11}, it can be shown that the cubic (x^3-3x^2+2x+4) is irreducible in Z_{11}. That means that the roots of $\overline{f(x)}$ generated a cyclic subgroup of order three. Using Proposition 10.4 we have that the Galois group generated by the roots of $f(x)=x^5+15x+6$ has a subgroup isomorphic to a cyclic group of order 3. However, since we know that the Galois group has to be either S_5 or W and W cannot have a subgroup of order three, the Galois group must be S_5. Thus, $f(x)$ is not solvable by radicals by Proposition 10.1. ■

Example 11.8: $f(x)=x^5+11x+44$ is not solvable by radicals. In this case $f(x)=x^5+11x+44$ is clearly irreducible using the Eisenstein Criterion with $p=11$. After determining that there is one real root and 4 complex roots we find the discriminant is $2^{14}7^2 11^4$, and thus is a perfect square. Thus by Proposition 10.7 it must have a Galois group which is a subgroup of A_5, thus the Galois group must be A_5, D_{10}, or Z_5. Now our next step is to mod $f(x)$ into an appropriate prime finite field. The next lowest prime finite field we can look at is Z_3, but this results in an irreducible polynomial which would be of very little use to us. We then mod out into Z_5. We see that $f(x)=x^5+11x+44$ mod 5 is $\overline{f(x)}=x^5+x+4$. Using synthetic division we can check that in Z_5, $\overline{f(x)}$ factors as $(x-3)(x^4-2x^3-x^2+2x+2)$. Using synthetic division and checking all the numbers in Z_5 we can check that the quartic $\left(x^4-2x^3-x^2+2x+2\right)$ is irreducible in Z_5. Thus the roots of $\overline{f(x)}$ generate a cyclic subgroup of order four. Using Proposition 10.4 we obtain that the Galois group generated by the roots of $f(x)=x^5+11x+44$ has a subgroup isomorphic to a cyclic group of order 4. However, since we know the Galois group has to be either A_5, D_{10}, or Z_5 and D_{10} and Z_5 cannot have a subgroup of order four, the Galois group must be A_5. Thus $f(x)=x^5+11x+44$ is not solvable by radicals, by Proposition 10.1. ■

Now we move onto an example of a solvable quintic.

Example 11.9: $f(x)=x^5-5x+12$ is solvable by radicals.

First we need to check whether or not $f(x)=x^5-5x+12$ is irreducible. We will do this by considering $f(x+2)=(x+3)^5-5(x+3)+12=x^5+15x^4+90x^3-270x^2+390x-78$ which using the Eisenstein criterion with $p=3$, is irreducible, since 3 divides all the coefficients except the leading one, while 3^2 does not divide -78, the constant term. Now since $f(x+3)$ is irreducible, we also have that $f(x)=x^5-5x+12$ is irreducible.

We use calculus to find out the number of real roots, since we cannot determine our five roots. Taking the first derivative yields $f'(x)=5x^4-5$, thus $f'(x)$ has roots at ±1, this means that $f'(x)$ has two real roots, thus $f(x)$ has two relative extrema which means $f(x)$ will have the potential for roots on both sides of ±1. Now we check by plugging in numbers as shown in Figure 5.

x	-2	-1.5	-1	-.5	0	.5	1	1.5	2
f(x)	-10	11.91	16	14.47	12	9.53	8	12.09	34
+/-	-	-	-	+	+	+	+	+	+

Figure 5. Roots For Example 11.9

Using the figure above, we can see that $f(x)$ has a real root between -2 and -1.5. Thus $f(x)$ has one real root. This means that $f(x)$ has 4 complex roots.

Next we find the discriminant of $f(x)$ using Proposition 10.5. We have $f(x) = x^5 - 5x + 12$, so $\Delta = 5^5 q^4 + 4^4 p^5 = 5^5 12^4 + 4^4(-5)^5 = 5^5 2^8 3^4 - 2^8 5^5 = 5^5 2^8 (3^4 - 1) = 2^{12} 5^6$. Thus $\Delta = 2^{12} 5^6$. Now since this discriminant is a perfect square we know that the Galois group is a subgroup of A_5. Now we must determine whether it is all of A_5 or a proper subgroup of A_5. To do this we mod out $f(x) = x^5 - 5x + 12$ by a prime finite field other than 2 or 5, else the polynomial would become trivial. So the lowest prime we have left is 3.

So $f(x)=x^5-5x+12$ mod 3 is $\overline{f(x)}=x^5+x$ which in Z_3, factors as $x(x^2+x-1)(x^2-x-1)$. Thus we know that Galois group has a subgroup isomorphic to Z_2. This fact right away eliminates Z_5 from the picture. So the Galois group must be either A_5 or D_{10}.

The proof of the fact that in this case the Galois group is D_{10} requires the use of a computer. An outline of the proof can be found in [7, page 162]. Since the Galois group is D_{10}, and we know that by Proposition 8.5, D_{10} is a solvable group, Proposition 10.1 yields that $f(x)=x^5-5x+12$ is solvable by radicals.■

The last two examples do not use the method that Example 11.1 through Example 11.9 used and will be handled differently.

Example 11.10: $f(x)=x^5+x^4-4x^3-3x^2+3x+1$ is solvable by radicals.

First we check that $f(x)=x^5+x^4-4x^3-3x^2+3x+1$ is irreducible by using the Eisenstein Criterion $(p=11)$ and the

substitution $x+2$, which yields

$$f(x+2)=(x+2)^5+(x+2)^4-4(x+2)^3-3(x+2)^2+3(x+2)+1$$

$$=x^5+11x^4+44x^3+77x^2+77x+11.$$

This example was not created like the ones before it. In previous examples we started with the polynomial and tested it in various ways to see whether it was solvable by radicals. This one we will show is solvable by working backwards.

Consider an 11th root of unity, say $\alpha = e^{2\pi i/11}$. Reasoning like in Example 6.3 we get that a minimal polynomial for α is $\Phi_p(x) = 1 + x + x^2 + \ldots + x^{10}$, which is irreducible over Q by Example 4.8, and has the cyclic Galois group Z_{10}. This has a subgroup of order 2 and the fixed field of this has Galois group Z_5 by the Fundamental Theorem of Galois Theory. (The Galois group of a fixed field B, between our splitting field E and Q is $\mathscr{G}(B/Q) \approx \mathscr{G}(E/Q)/\mathscr{G}(E/B) = Z_{10}/Z_2 \approx Z_5$.) This fixed field is generated by $\alpha + \alpha^{-1}$, while the minimal polynomial for this is $f(x) = x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1$ (this can be checked by plugging $\alpha + \alpha^{-1}$ into $f(x) = x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1$ which yields zero), thus the Galois group for $f(x) = x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1$ is Z_5, which by Example 8.7 is a solvable group, thus $f(x) = x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1$ is solvable by radicals.■

Example 10.11: $f(x) = x^5 - 2$ is solvable by radicals.

First we note that $f(x) = x^5 - 2$ is irreducible by the Eisenstein Criterion. For this example, we show that the dimension of the splitting field of $f(x)$ over Q is twenty. Thus the Galois group must have order twenty and thus must be solvable by Example 8.9. If the Galois group is solvable, then by Proposition 10.1, $f(x)=x^5-2$ is solvable by radicals.

Proposition 11.1: Let $f(x)=x^5-2$ and let the splitting field of the roots of $f(x)=x^5-2$ be E, then $[E:Q]=20$.

Proof: Clearly, we have one positive real root for $f(x)=x^5-2$, namely $2^{1/5}$, and $f(x)=x^5-2$ is a minimal polynomial for $2^{1/5}$, thus $[Q(2^{1/5}):Q]=5$.

Now let us consider any other root of $f(x)=x^5-2$ in C. Then $(\alpha/2^{1/5})^5=\alpha^5/2=1$, so $\alpha=\omega 2^{1/5}$ where ω is a complex root of $x^5-1=(x-1)(x^4+x^3+x^2+x+1)$. Since $(x^4+x^3+x^2+x+1)$ is irreducible by Example 4.8, we get that $[Q(\omega):Q]=4$. Now notice that the roots of $f(x)=x^5-2$ are $2^{1/5},\omega 2^{1/5},\omega^2 2^{1/5},\omega^3 2^{1/5},\omega^4 2^{1/5}$, so the splitting field of $f(x)$ is $E=Q(2^{1/5},\omega)$. Since $f(x)=x^5-2$ is irreducible over $Q(\omega)$, we also have that $[Q(2^{1/5}):Q(\omega)]=5$.

Now, $[Q(2^{1/5},\omega):Q]=[Q(2^{1/5}):Q(\omega)][Q(\omega):Q]=5\cdot 4=20$ by Proposition 3.1. Hence $[E:Q]=20$. Thus by Proposition 6.1 the Galois group must be group of order twenty and thus an order twenty subgroup of S_5. Therefore it must be solvable by Example 8.9 since it has order 20.■

CHAPTER TWELVE
CONCLUSIONS AND RECOMMENDATIONS

If we look back on the questions that motivated my research: Are there any quintics that are solvable by radicals? If so, can we predict whether a quintic will be solvable or not? What methods can we employ to determine whether a specific quintic is solvable? We can draw the following conclusions based on the work done in this thesis. Predicting whether a quintic is solvable or not can be easy if it has 3 real roots and 2 complex roots, but much more difficult if it has one real root and 4 complex roots, or all real roots. In the first two cases, after some calculations, we were able to find a method to decide whether a quintic of the form $f(x)=x^5+px+q$ is solvable or not.

A topic that can be further investigated, is trying to come up with a reasonable equation for the discriminant of a quintic of any form. This might not necessarily guarantee the generation of a plethora of quintics that are solvable, as we have found it quite difficult to actually find a discriminant which is a perfect square even for a simple quintic of the form $f(x)=x^5+px+q$.

In fact, finding quintics which have discriminants with prime factorizations which are not perfect squares proved to be difficult as well. This means finding the discriminant in terms of the coefficients will not even guarantee generating unsolvable examples. Employing a computer program to help in the search for discriminants that have prime factorization and that are perfect squares may also prove to be useful in furthering the topic of quintics that are solvable by radicals.

In conclusion, maybe as the excitement grew over whether the typical quintic was solvable by radicals, many people discovered just how hard it was to find reasonable examples. Hence, when it was proven that the typical quintic was unsolvable by radicals, questions like those that fueled my research, though important, were considered not worth the time nor hassle they required when there were still other topics waiting to be further developed and discovered.

BIBLIOGRAPHY

[1] Borsuk, K., Szmielew, W. Foundations of Geometry.
North-Holland Publishing Company, Amsterdam, 1960.

[2] Clark, A. Elements of Abstract Algebra.
Dover Publications, New York, 1984.

[3] Dixon, John D. Problems In Group Theory.
Dover Publications, New York, 1973.

[4] Dubinsky, Ed. Learning Abstract Algebra with ISETL.
Springer, New York, 1994.

[5] Dunham, W. Journey Through Genius.
John Wiley and Sons, New York, 1990.

[6] Edwards, H.M. Galois Theory.
Springer-Verlag, New York, 1984.

[7] Garling, D.J.H. A Course In Galois Theory.
Cambridge University Press, New York, 1986.

[8] Kay, D.C. College Geometry: A Discovery Approach.
HarperCollins College Publishers, New York, 1994.

[9] Lyapin, E.S. Exercises in Group Theory.
Plenum Press, New York, 1972.

[10] Martin, G.E. Geometric Constructions.
Springer-Verlag, New York, 1998.