THE SOLVABILITY BY RADICALS OF LINEAR, QUADRATIC, CUBIC, QUARTIC, AND QUINTIC EQUATIONS

A Thesis

Presented to

the Faculty of the Department of Mathematics

Kansas State Teachers College

In Partial Fulfillment

of the Requirements for the Degree

Master of Arts

by

David L. Preston

August 1968

Marion P. Emerson

Approved for the Major Department

Samuel [illegible]

Approved for the Graduate Council

3

Acknowledgements

I would like to sincerely thank Dr. Marion Emerson. Without his help, understanding, and patience (not only on this paper, but throughout my graduate program) this paper would not have been written.

I would also like to thank my wife for her understanding and patience throughout my graduate program.

TABLE OF CONTENTS

LIST OF TABLES

CHAPTER I

INTRODUCTION

The primary purpose of this paper is to prove that the rationals cannot be extended by radicals to include the roots of an irreducible fifth degree polynomial equation. This paper also shows that extensions can be obtained for other polynomial equations of lesser degree. Throughout this paper rational polynomial equations will be referred to as polynomial equations. In Chapter Two, the extension of the rationals to include roots of first and second degree polynomial equations are considered. In Chapter Three, it is shown that the rationals can be extended by radicals to include roots of third degree polynomial equations. In the fourth chapter it is shown that the rationals cannot be extended by radicals to include the roots of an irreducible fifth degree polynomial equation.

Two approaches to the problem of extending the rationals (denoted Ra) by radicals will be used. The approach used in Chapter Two is to consider the set that is obtained by adjoining radicals of the form $\sqrt{i}$, where i is an integer, to the rationals and to prove this set is a field. This is done with integers because $\sqrt{b}$ where $b \in Ra$ can always be expressed as $a\sqrt{i}$ where $a \in Ra$ and $i \in I$. The approach used in Chapter Three is to prove that the rationals can be extended by radicals to include the roots of an irreducible third degree polynomial equation.

It will be presupposed that the reader has completed a course in abstract algebra. Thus, it will be assumed that the reader knows the axioms of a group, ring, integral domain, and field. Also the reader should know the definition and some properties of polynomial rings.

This paper concerns field extensions so a definition is needed:

1.1 Definition: A field K is called a field extension of the field F if and only if F is a subfield of K.

Many examples of field extensions can be given. The real number system is a field extension of the rational number system. The complex number system is a field extension of the real number system.

CHAPTER II

FIRST AND SECOND DEGREE POLYNOMIAL EQUATIONS

Consider the roots of the polynomial equations of the form $ax + b = 0$, where $a \neq 0$. The roots of these equations are of the form $-b/a$, for $a(-b/a) + b = 0$. Since the set of rational numbers is a field, it follows that $-b/a \in Ra$. Therefore, when the roots of $ax + b = 0$ are adjoined to Ra, Ra is obtained. Thus Ra is a field that includes all roots of first degree polynomial equations.

Consider the roots of all second degree polynomial equations over Ra of the form $f(x) = ax^2 + bx + c = 0$. The roots of $f(x)$ are of the form $\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$. Let $D = b^2 - 4ac$ and consider the set Ra $(\sqrt{D})$, where $D \in Ra$. This means that $\sqrt{D}$ has been adjoined to Ra. Since $\sqrt{D}$ can be expressed as $a\sqrt{i}$, where $a \in Ra$ and $i \in I$, elements of the form $\frac{-b + \sqrt{D}}{2a}$ can be obtained by operating on $\sqrt{i}$ with the rationals. Operating on $\sqrt{i}$ with the rationals means that the set Ra $\cup \{\sqrt{i}\}$ is extended so that it is closed under multiplication and addition.

Let F be defined to be the set obtained by adjoining the roots of all quadratics to Ra, and all members obtained by operating on these roots with the rationals and the roots themselves. Intuitively, F can be obtained by a different way. Suppose the rationals are extended by the $\sqrt{2}$, which is a root of a quadratic equation and also the square root of an integer, in the ordinary way. The field Ra $(\sqrt{2})$ is obtained. Then suppose Ra $(\sqrt{2})$ is extended by the square root of another integer in the same way. If this process could be repeated until all the roots of quadratics were adjoined in such a manner, F would be obtained. It is clear then, Ra$\sqrt{b}$, $b \in I$, is a subset of F.

The elements of F are of the form $\sum_{i\in I} b_i\sqrt{i}$, where $b_i \in Ra$. It should be noted that this is a finite sum and no infinite series belongs to F. The definitions of equality, addition and multiplication are:

2.1 Definition: $\sum_{i\in I} b_i\sqrt{i} = \sum_{j\in I} a_j\sqrt{j}$ if and only if $b_i = a_j$ when $i = j$

2.2 Definition: $\forall\, i,j;\ \sum_{i\in I} b_i\sqrt{i} + \sum_{j\in I} a_j\sqrt{j} = \sum_{k\in I}(b_k + a_k)\sqrt{k}$

2.3 Definition:

$$\forall\, i,j \quad \Big(\sum_{j\in I} b_j\sqrt{j}\Big)\Big(\sum_{i\in I} a_i\sqrt{i}\Big) = \left\{\begin{array}{l} \sum_{i,j\in I} -b_i a_j\sqrt{ij} \text{ if } i<0 \text{ and } j<0 \\ \sum_{i,j\in I} b_i a_j\sqrt{ij} \text{ if } i\geq 0 \text{ or } j\geq 0 \end{array}\right\}$$

Now to prove F is a field. The subscripts will now be omitted. Notice that b_i refers to the rational number that is the coefficient of $\sqrt{i}$ in $\sum b_i\sqrt{i}$.

Property I: Closure

Since $\sum b_i\sqrt{i} + \sum a_j\sqrt{j} = \sum(b_i + a_j)\sqrt{i}$ when $i = j$, and the rationals are closed under addition, it follows that $b_i + a_j$ is a rational and $\sum(b_i + a_j)\sqrt{i}$ can be written $\sum c_i\sqrt{i}$. Therefore, F is closed under addition.

Also, since the rationals are closed under multiplication, $b_i a_j$ can be expressed as c_k and $\sqrt{ij}$ as $\sqrt{k}$ making $\sum b_i a_j\sqrt{ij} = \sum c_k\sqrt{k}$. Therefore, F is closed under multiplication.

Property II: Additive Identity

Since 0 is a root of $x^2 = 0$, which is a second degree polynomial equation $0 \in F$. Also, 0 can be written as $\sum 0\sqrt{i}$. Therefore, $\sum b_i\sqrt{i} + \sum 0\sqrt{i} = \sum(b_i + 0)\sqrt{i} = \sum b_i\sqrt{i}$. This follows because 0 is the additive identity for the rationals.

Property III: Multiplicative Identity

Since 1 is a root of $x^2 - 1 = 0$ which is a second degree polynomial equation, $1 \in F$. Also, 1 can be written as $\sum c_k\sqrt{k}$ where $c_k = 1$ when $k = 1$ and $c_k = 0$ when $k \neq 1$. Therefore, $(\sum b_i\sqrt{i})(\sum c_k\sqrt{k}) = \sum b_i c_k\sqrt{ik}$.

This means that each term of $\sum b_i\sqrt{i}$ is multiplied by each term of $\sum c_k\sqrt{k}$. But, there is only one term of $\sum c_k\sqrt{k}$ not equal to zero, and this is $c_1\sqrt{1} = 1$. Therefore, the product of every term of $\sum b_i\sqrt{i}$ with 1 is needed. $(\sum b_i\sqrt{i})(1\sqrt{1}) = \sum b_i\cdot 1\sqrt{i\cdot 1} = \sum b_i\sqrt{i}$, since $b_i\cdot 1 = b_i$ and $i\cdot 1 = i$.

Property IV: Additive Inverse

Consider $\sum b_i\sqrt{i}$ and $\sum -b_i\sqrt{i}$ where $-b_i$ refers to the additive inverse of b_i. Since $b_i \in Ra$, there exists $-b_i \in Ra$ such that $b_i + (-b_i) = 0$. Therefore, $\sum b_i\sqrt{i} + \sum -b_i\sqrt{i} = \sum \left(b_i + (-b_i)\right)\sqrt{i} = \sum 0\sqrt{i} = 0$.

Property V: Multiplicative Inverse

Induction will be used to prove F has inverses. Consider n to be the number of terms in $\sum b_i\sqrt{i}$. If $n = 1$, $\frac{1}{b_r\sqrt{r}}\cdot\frac{\sqrt{r}}{\sqrt{r}} = \frac{\sqrt{r}}{b_r r}$ which is in F. If $n = 2$, $\frac{1}{b_r\sqrt{r} + b_s\sqrt{s}} = \frac{b_r\sqrt{r} - b_s\sqrt{s}}{b_r^2 r + b_s^2 s}$, which is in F. Assume that $\sum b_i\sqrt{i}$ has an inverse if there are k terms and consider the k + 1 case, that is, k + 1 terms. It must be shown that $\sum b_k\sqrt{k} + b_s\sqrt{s}$ has an inverse. $\sum b_k\sqrt{k}$ means $\sum b_k\sqrt{k} \in K$ where K is an extension of Ra by adjoining radicals in the manner described earlier until the elements of K have at most k radicals. Under the induction hypothesis then, $\sum b_k\sqrt{k}$ has an inverse. Consider G to be the extension of K by $\sqrt{s}$ in the usual manner. Elements of G are of the form $\sum b_k\sqrt{k} + b_s\sqrt{s} = g + b_s\sqrt{s}$ where $g, b_s \in K$. $\frac{1}{g + b_s\sqrt{s}} = \frac{g - b_s\sqrt{s}}{g^2 - b_s^2 s} = \frac{g}{g^2 - b_s^2 s} - \frac{b_s\sqrt{s}}{g^2 - b_s^2 s}$. Since the first term of this expression and the coefficient of $\sqrt{s}$ is in G, the entire expression is in G. Therefore, $\sum b_k\sqrt{k} + b_s\sqrt{s}$ has an inverse, and, by induction, every element of F has an inverse.

Property VI: Associative Property of Multiplication

$$\left((\sum b_i\sqrt{i})(\sum a_j\sqrt{j})\right)(\sum c_k\sqrt{k}) = (\sum b_i a_j\sqrt{ij})(\sum c_k\sqrt{k}) = \sum(b_i a_j)c_k\sqrt{(ij)k}.$$

Since the rationals are associative, this becomes: $\sum b_i(a_j c_k)\sqrt{i(jk)} = (\sum b_i\sqrt{i})(\sum a_j c_k\sqrt{jk}) = (\sum b_i\sqrt{i})\left((\sum a_j\sqrt{j})(\sum c_k\sqrt{k})\right)$.

Property VII: Associative Property of Addition

$$(\sum b_j\sqrt{i} + \sum a_j\sqrt{j}) + \sum c_k\sqrt{k} = \sum(b_i + a_j)\sqrt{i} + \sum c_k\sqrt{k} =$$

$\sum\left((b_i + a_j) + c_k\right)\sqrt{i}$. Since the rationals are associative, this becomes: $\sum\left(b_i + (a_j + c_k)\right)\sqrt{i} = \sum b_i\sqrt{i} + \sum(a_j + c_k)\sqrt{j} = \sum b_i\sqrt{i} + (\sum a_j\sqrt{j} + \sum c_k\sqrt{k})$.

Property VIII: Commutative Property of Addition

$\sum b_i\sqrt{i} + \sum a_j\sqrt{j} = \sum(b_i + a_j)\sqrt{i}$. Since the rationals are commutative, this becomes: $\sum(a_j + b_i)\sqrt{i} = \sum a_j\sqrt{j} + \sum b_i\sqrt{i}$.

Property IX: Commutative Property of Multiplication

$(\sum b_i\sqrt{i})(\sum a_j\sqrt{j}) = \sum b_i a_j\sqrt{ij}$. Since the rationals are commutative, this becomes: $\sum a_j b_i\sqrt{ji} = (\sum a_j\sqrt{j})(\sum b_i\sqrt{i})$.

Property X: Distributive Properties

$$\sum b_i\sqrt{i}(\sum a_j\sqrt{j} + \sum c_k\sqrt{k}) = \sum b_i\sqrt{i}\left(\sum(a_j + c_k)\sqrt{j}\right) =$$

$\sum b_i(a_j + c_k)\sqrt{ij}$. Since the rationals are distributive, this becomes: $\sum(b_i a_j + b_i c_k)\sqrt{ij} = \sum b_i a_j\sqrt{ij} + \sum b_i c_k\sqrt{ik} = (\sum b_i\sqrt{i})(\sum a_j\sqrt{j}) + (\sum b_i\sqrt{i})(\sum c_k\sqrt{k})$. The right distributive property can be shown similarly.

F is a field and since $Ra \subset F$, it follows that F is a field extension of the rationals. This means that the rationals have been extended by radicals to the field F, which contains all the roots of all second degree polynomial equations.

CHAPTER THREE

THIRD DEGREE POLYNOMIAL EQUATIONS

Extending the rationals to contain roots of third degree polynomials can be done in at least two ways. One way would be to extend the rationals by adjoining all roots of third degree polynomial equations, finding the general form of an element of this set, and proving this set a field as was done with quadratics in the second chapter. Another way would be to prove that the rationals can be extended by radicals to include roots to third degree polynomial equations.

The roots of the cubic equation $ax^3 + bx^2 + cx + d = 0$ are:

$$x_1 = z_1 - p/3z_1 - b/3$$
$$x_2 = \omega z_1 - \omega^2 p/3z_1 - b/3$$
$$x_3 = \omega^2 z_1 - \omega p/3z - b/3$$

where $\omega = -1/2 + 1/2\sqrt{3i}$ and $\omega^2 = -1/2 + 1/2\sqrt{3i}$ and z_1 is a root of one of the following: $z^3 = -q/2 + \sqrt{R}$, $z^3 = q/2 - \sqrt{R}$ when $R = 1/27\ p^3 + 1/4\ q^2$ and $p = c - b^2/3$, $q = d - bc/3 + 2b^3/27$. [2, pp 244-247]

In order to prove that the rationals can be extended by radicals to include the roots of an irreducible third degree polynomial equation (cubic), Abel's theorem is needed.

3.1 Theorem: "If F is of characteristic zero, then f(x) is solvable by radicals if and only if the Galois group G_0 of f(x) is solvable, that is, there exists a finite chain of subgroups $G_0 \supseteq G_1 \supseteq \supseteq . . . \supseteq G_m = E$ such that G_1 is normal in G_{i-1} and G_{i-1}/G_i is Abelian, i = 1, 2, ... , m." [1, p 186]

If $f(x) = ax^3 + bx^2 + cx + d = 0$ is solvable by radicals, then the rationals can be extended by these radicals as was done for second degree polynomial equations. To prove f(x) is solvable by radicals, each condition of 3.1 will have to be satisfied. Each condition will be taken in order with the necessary definitions given preceding the proof of the condition.

3.2 Definition: "In an arbitrary ring R, if there exists a positive integer n such that $nx = 0$ for every x in R, then the least such positive integer n is called the <u>characteristic</u> of R and R is said to have (positive) <u>characteristic n</u>. If no such integer exists, that is, if $nx = 0$ for all x in R only if $n = 0$, then R is said to have <u>characteristic zero</u>". [1, p 138]

3.3 Theorem: The rationals have characteristic zero.

Proof: It needs to be understood that $nx = 0$ means $x + x + \ldots + x = 0$ with n terms. Suppose that the rationals do not have characteristic zero. This implies that there exists an n, such that, for every $x \in Ra$, $nx = 0$. Suppose $x = 1$. This means $1 + 1 + 1 + \ldots + 1 = 0$. Since $1 + 1 = 2$, $2 + 1 = 3, \ldots, (n - 1) + 1 = 0$. This implies that the natural numbers are finite. But, this is a contradiction because the naturals are not finite. Therefore, the rationals have characteristic zero.

In order to obtain the Galois group of f(x), it is necessary to define this and other terms.

3.4 Definition: "Let K and K' be fields and $A = \{\alpha_i : i \in I\}$ be a set of isomorphisms of K into K'. An element k in K is called <u>fixed</u> for A if $k\alpha_i = k\alpha_j$ for all i and j in I". [1, p 179]

3.5 Definition: "If H is a subgroup of a group G, then a <u>right coset</u> of H is a subset S of G such that there exists $x \in G$ for which $S = Hx$. Left cosets are defined similarly". [3, p 19]

3.6 Definition: "A subgroup H of G is normal in G written $H \triangleleft G$, if and only if $x^{-1} Hx \subset H$ for all $x \in G$". [3, p 19]

3.7 Definition: "If H is a normal subgroup of G, then the set of cosets of H in G form a group under multiplication." This group is then called the factor group of H in G and is denoted G/H. [3, p 38]

3.8 Definition: $[G:H]$ is the notation used to denote the index of G/H. This gives the number of elements of the factor group G/H.

3.9 Definition: An automorphism is a one-to-one mapping of a set onto itself, such that the operations are preserved under the mapping.

3.10 Definition: Let K be a superfield of F. Let G be the set of all automorphisms of K such that F is mapped onto F, i.e., F remains fixed under the mapping $\alpha \in G$. If $[K:F]$ is finite, then K is normal over F and G is called the Galois group of K over F. $[K:F]$ in this definition means that the extension K, of F, as a vector space has finite dimension over F. This dimension is called the degree of K over F.

To find the Galois group of $f(x) = ax^3 + bx^2 + cx + d = 0$, consider the set K, where K is obtained by extending the rationals by adjoining the roots of f(x), namely k_1, k_2, k_3, in the usual manner. That is, K is obtained by operating on k_1, k_2, k_3 by the rationals and k_1, k_2, and k_3. Also, $Ra \subset K$. Consider the automorphisms of K.

3.11 Theorem: If $a \in Ra$, and α is an automorphism of K, the $(a)\alpha = a$.

Proof: Suppose $(a)\alpha \neq a$ and $a \neq 0$. A lemma is needed in the proof of this theorem.

3.11.1 Lemma: Under α, the integers must be mapped onto the integers.

Proof: Suppose $(d)\alpha = e$ where d, e are integers but $d \neq e$. Then one can be subtracted from d (or added as the case may be) and e until one is obtained on the left. The result would be $(1)\alpha = e - k$. But $(1)\alpha = 1$ so $(d)\alpha = d$ and the lemma is proven.

Since integers have to be mapped onto integers, under any automorphism, quotients must be mapped onto quotients and the resulting rational numbers must be mapped onto the rational numbers. Therefore, $(a)\alpha = a$.

Since the rationals must be mapped onto themselves, it suffices to map k_1, k_2, and k_3 onto some elements of K. For once the rationals are mapped onto themselves and k_1, k_2, and k_3 are mapped to some elements, the rest of the mapping will be determined by the mapping of k_1, k_2, and k_3.

3.12 Theorem: Under the automorphism α, roots must be mapped onto themselves.

Proof: If one or all of the roots are rational, then by 3.11, they must be mapped onto themselves and there would be only one automorphism, namely, the identity mapping. Therefore, suppose $(k_i)\alpha = \lambda$ (where $i = 1, 2, 3$) $\lambda \notin Ra$ and $\lambda \epsilon \{k_1, k_2, k_3\}$. Consider $ax^3 + bx^2 + cx + d$ and the following mapping: $(a)\alpha = a$, $(b)\alpha = b$, $(c)\alpha = c$, and $(d)\alpha = d$. Then $(ak_i^3 + bk_i^2 + ck_i + d)\alpha = a\lambda^3 + b\lambda^2 + c\lambda + d$ and since $ak_i^3 + bk_i^2 + ck_i + d = 0$, $(0)\alpha = 0$ and $(0)\alpha = a\lambda^3 + b\lambda^2 + c\lambda + d \neq 0$. This contradicts the hypothesis that α is an automorphism. Therefore, roots must be mapped onto roots.

Under this definition of α, where the rationals are mapped onto themselves and roots are mapped onto themselves, it follows that α is an automorphism.

The elements of K are of the form: $\sum_{i,j,z \epsilon \{0,1,2\}} a_{ijz}\, k_1^i\, k_2^j\, k_3^z$. Again, a finite sum is meant. In order that the next theorem can be proven, and in order to satisfy a condition of Abel's theorem, K must be shown to be a field. Since the roots of f(x) are necessarily complex numbers, it suffices to show that K has inverses. To do this, it is only necessary to show that k_i, $i \epsilon \{0,1,2\}$ has an inverse in K, because a similar proof can be given for other elements in K. Since f(x) and k_1 are relatively prime polynomials, it follows that $1 = r(k_i)\ k_i + h\ (k_i)\ f(k_i)$. Since $f(k_i) = 0$, $1 = r(k_i)k_i$ which means k_i has an inverse in K.

3.13 Theorem: If α is defined by $(\sum a_{ijz}\, k_1^i\, k_2^j\, k_3^z)\alpha = \sum a_{ijz}\, (k_{p(1)})^i\, (k_{p(2)})^j\, (k_{p(3)})^z$ where p(1), p(2), p(3) is a permutation of 1, 2, and 3, then α is an automorphism of k on to K.

Proof: Addition will be defined as follows:

$\sum a_{ijz}\, k_1^i\, k_2^j\, k_3^z + \sum b_{rst}\, k_1^r\, k_2^s\, k_3^t = \sum (a_{ijk} + b_{rst})\, k_1^i\, k_2^j\, k_3^z = \sum (a_{ijz} + b_{ijz})\, k_1^i\, k_2^j\, k_3^z$. In other words, the coefficients of like terms are added together making $a_{ijz} + b_{rst} = a_{ijz} + b_{ijz}$. This operation is preserved under the mapping α since $(\sum a_{ijz}\, k_1^i\, k_2^j\, k_3^z + \sum b_{rst}\, k_1^r\, k_2^s\, k_3^t)\alpha = \left(\sum(a_{ijz} + b_{rst})\, k_1^i\, k_2^j\, k_3^z\right)\alpha = \sum(a_{ijz} + b_{rst})\, k_{p(1)}^i\, k_{p(2)}^j\, k_{p(3)}^z =$

$\sum a_{ijz}\, k_{p(1)}^i\, k_{p(2)}^j\, k_{p(3)}^z + \sum b_{rst}\, k_{p(1)}^r\, k_{p(2)}^s\, k_{p(3)}^t = (\sum a_{ijz}\, k_1^i\, k_2^j\, k_3^z)\alpha + (\sum b_{rst}\, k_1\, k_2\, k_3)\alpha$.

Multiplication is defined as follows:

$(\sum a_{ijz}\, k_1^i\, k_2^j\, k_3^z)(\sum b_{rst}\, k_1^r\, k_2^s\, k_3^t) = \sum a_{ijz}\, b_{rst}\, k_1^{i+r}\, k_2^{j+s}\, k_3^{z+t}$.

In other words, each term of $\sum a_{ijz}\, k_1^i\, k_2^j\, k_3^z$ is multiplied by each term of $\sum b_{rst}\, k_1^r\, k_2^s\, k_3^t$ and the sum of the products is taken. This operation is preserved under the mapping α since, $\left[(\sum a_{ijz}\, k_1^i\, k_2^j\, k_3^z)(\sum b_{rst}\, k_1^r\, k_2^s\, k_3^t\right]\alpha =$
$(\sum a_{ijz}\, b_{rst}\, k_1^{i+r}\, k_2^{j+s}\, k_3^{z+t})\alpha = \sum a_{ijz}\, b_{rst}\, k_{p(1)}^{i+r}\, k_{p(2)}^{j+s}\, k_{p(3)}^{z+t} =$
$(\sum a_{ijz}\, k_{p(1)}^i\, k_{p(2)}^j\, k_{p(3)}^z) \cdot (\sum b_{rst}\, k_{p(1)}^r\, k_{p(2)}^s\, k_{p(3)}^t) =$
$(\sum a_{ijz}\, k_1^i\, k_2^j\, k_3^z)\alpha \cdot (\sum b_{rst}\, k_1^r\, k_2^s\, k_3^t)\alpha$.

From the definition of α, when i, j, k, = 0, $(a)\alpha = a$ and when $a_{ijk} = 1$, $(k_1)\alpha = k_{p(1)}$ thereby satisfying the two previous theorems that the rationals must be mapped onto themselves and roots must be mapped onto roots.

It is clear that α is an onto mapping. For every $\sum a_{ijz}\, k_1^i\, k_2^j\, k_3^z$ of K, there exists an image in K, namely $\sum a_{ijz}\, k_{p(1)}^i\, k_{p(2)}^j\, k_{p(3)}^z$. For every $\sum a_{ijz} k^i_{p(1)} k^j_{p(2)} k^z_{p(3)}$ there exists a preimage in K, namely $\sum a_{ijz} k_1^i k_2^j k_3^z$.

To prove α is a one-to-one mapping, suppose $(\sum a_{ijz} k_1^i k_2^j k_3^z)\alpha = \sum a_{ijz} k^i_{p(1)} k^j_{p(2)} k^z_{p(3)}$ and $(\sum b_{rst} k_1^r k_2^s k_3^t)\alpha = \sum a_{ijz} k^i_{p(1)} k^j_{p(2)} k^z_{p(3)}$. It follows that $(\sum a_{ijz} k_1^i k_2^j k_3^z + \sum b_{rst} k_1^r k_2^s k_3^t)\alpha = \sum a_{ijz} k^i_{p(1)} k^j_{p(2)} k^z_{p(3)} + \sum -a_{ijz} k^i_{p(1)} k^j_{p(2)} k^z_{p(3)} = 0$. Since α is an automorphism, (0) = 0 making $\sum a_{ijz} k_1^i k_2^j k_3^z + \sum -b_{rst} k_1^r k_2^s k_3^t = 0$. Since K is a field, $\sum a_{ijz} k_1^i k_2^j k_3^z = \sum b_{rst} k_1^r k_2^s k_3^t$. Therefore α is one-to-one and α is an automorphism.

Since α maps roots onto roots, and there are three roots, there are at most six such automorphisms. Consider the following set S of automorphisms, $\{\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5; \alpha_6\}$ where α_i is defined as follows:

α_1	α_2	α_3	α_4	α_5	α_6
$k_1 \rightarrow k_1$	$k_1 \rightarrow k_1$	$k_1 \rightarrow k_2$	$k_1 \rightarrow k_3$	$k_1 \rightarrow k_2$	$k_1 \rightarrow k_3$
$k_2 \rightarrow k_2$	$k_2 \rightarrow k_3$	$k_2 \rightarrow k_1$	$k_2 \rightarrow k_2$	$k_2 \rightarrow k_3$	$k_2 \rightarrow k_1$
$k_3 \rightarrow k_3$	$k_3 \rightarrow k_2$	$k_3 \rightarrow k_3$	$k_3 \rightarrow k_1$	$k_3 \rightarrow k_1$	$k_3 \rightarrow k_2$

TABLE I

GROUP TABLE FOR S

	α_1	α_2	α_3	α_4	α_5	α_6
α_1	α_1	α_2	α_3	α_4	α_5	α_6
α_2	α_2	α_1	α_5	α_6	α_3	α_4
α_3	α_3	α_6	α_1	α_5	α_4	α_2
α_4	α_4	α_5	α_6	α_1	α_2	α_3
α_5	α_5	α_4	α_2	α_3	α_6	α_1
α_6	α_6	α_3	α_4	α_2	α_1	α_5

From the way the elements of S are defined, S is the symmetric group of order six. In fact, S is the Galois group for f(x).

3.14 Theorem: S is the Galois group for $f(x) = ax^3 + bx^2 + cx + d = 0$.

1. K is the superfield of Ra as proven earlier.

2. S is the set of all automorphisms of K and Ra $\subset$ K by the definition of K and because Ra has to be mapped onto itself (3.11), Ra is the fixed field for K (3.4).

3. To prove the following a theorem will be used from a reference and no proof will be given.

4.14.1 Lemma: "Let K_A be the fixed field of the field K for the group $A = \{\alpha_1 = e, \alpha_2, \alpha_3, \ . \ . \ . \ , \alpha_n\}$ of automorphisms of K. Then $[K:K_A] = n$". [1, p 180]. In this case $[K:Ra] = [K:K_A] = 6$. Therefore, by 3.10, S is the Galois group of f(x) and K is normal over Ra. To show that f(x) is solvable by radicals, it must be shown that there exists a finite chain of subgroups $G_o \geq G_1 \geq . \ . \ . \geq G_m = \{e\}$ such that G_1 is normal in G_{i-1} and G_{i-1}/G_i is Abelian.

Consider the following finite chain of subgroups:

$$M_o = \{\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6\}$$
$$M_1 = \{\alpha_1, \alpha_5, \alpha_6\}$$
$$M_2 = \{\alpha_1\}$$

From the definition of a normal subgroup $M_o \lhd M_1 \lhd M_2$. Since $[M_1:M_2] = 3$ and $[M_o:M_1] = 2$, and any group of order 1, 2, or 3 is Abelian, M_1/M_o and M_2/M_1 are Abelian.

Therefore, S is the Galois group for f(x) and is solvable, and by Abel's theorem, f(x) is solvable by radicals.

Since f(x) is solvable by radicals, Ra can be extended by these radicals to include all the roots of all cubic equations. This can be done in a manner similar to the way the rationals were extended by all the roots of all quadratics in Chapter Two. This extension contains radicals, sums and products of these radicals with themselves and the rational numbers, and the rationals. It can be shown that this extension is a subfield of the complex number field.

CHAPTER IV

FOURTH AND FIFTH DEGREE POLYNOMIAL EQUATIONS

In Chapter Three, it was proven that the Galois group for a cubic is a subgroup of the symmetric group of order six (denoted S_3). For a quartic, the Galois group is a subgroup of the symmetric group S_4. The next polynomial equation to be considered is the one of fifth degree.

To prove that an irreducible fifth degree polynomial equation cannot be solved by radicals, it suffices to show that the Galois group, S_5, does not satisfy Abel's theorem. One of the conditions of Abel's theorem makes it necessary to find a finite chain of normal subgroups of S_5 such that the factor groups are not Abelian. It will be proven that no such chain of subgroups exists, that is, it will be proven that the alternating subgroup, A_5, is the only non-trivial normal subgroup of S_5 and every non-trivial normal subgroup of A_5 is A_5. Thus, the only finite chain possible is $\{e\} \lhd A_5 \lhd S_5$. Then it will be proven that the factor group, S_5/A_5 is not Abelian.

4.11 Theorem: If $\pi \in A_5$, then π can be written as a product of the 3-cycles (123), (124), and (125).

Proof: Any pair of 2-cycles can be written as a 3-cycle, or as a product of 3-cycles. To show this, two cases need to be considered. The first case is when π = (ab)(cd) or the two 2-cycles are disjoint. Then π can be written, π = (ab)(cd) = (acd)(acb). The second case is when the two 2-cycles are not disjoint. Then π can be written, π = (ab)(ad) = (abd).

To show that this product of 3-cycles can be written as a product of the 3-cycles (123), (124), and (125), consider the case where one belongs to the 3-cycle. This 3-cycle can be rewritten with the one first. For example, (214) = (142). If this 3-cycle has a two adjacent to the one, the 3-cycle has been rewritten as desired. Suppose then the two does not follow the one. To rearrange the letters of a 3-cycle, all that is necessary is to multiply the 3-cycle be itself and its inverse. For example, (132) = (132)(132)(123) = (123)(123). This puts the 3-cycle in the form desired. Suppose there isn't a two in the 3-cycle, such as (134). Since (134) = (213)(241), by using the previous procedure, (134) = (213)(241) = (132)(124) = (123)(123)(124). In general, suppose (1cd) needs to be rewritten where c,d $\neq$ 2. Then (1cd) = (21c)(2d1) and follow the previous procedure. Suppose that the 3-cycle contains no one or two. Then, in general, (cde) = (1cd)(1ec) and since no two appears here apply the above procedure. For example, (345) = (134)(153) = (213)(241)(215)(231) = (132)(124)(152)(123) = (132)(132)(123)(124)(152)(152)(125)(123) = (123)(123)(124)(125)(125)(123). Thus, any element of A_5 can be written as a product of the 3-cycles (123)(124) and (125).

4.12 Theorem. If $K \lhd A_5$, $K \neq \{e\}$, and K contains a 3-cycle, then $K = A_5$.

Proof: First it needs to be shown that K containing a 3-cycle implies that $(123) \in K$. Let (abc) be the three cycle. If a, b, and c, are the digits 1, 2, 3, then K contains the necessary 3-cycle. Suppose (abc) = (12c) where c $\neq$ 3. Then $[(12)(3c)]^{-1}$ (12c) $[(12)(3c)]$ = $(132) \in K$ which means $(132)^{-1} = (123) \in K$. Suppose (abc) = (1bc), where b,c $\neq$ 2. Then $[(1b)(2c)]^{-1}$ (1bc) $[(1b)(2c)]$ = $(12b) \in K$. But (12b) can be transformed by using the method above into the desired element. Suppose $(abc) \in K$ but a, b, c, $\neq$ 1.

Then $\left[(1a)(bc)\right]^{-1}$ (abc) $\left[(1a)(bc)\right]$ = (1cb)$\in$K. By using the above procedures (1cb) can be transformed to the desired element. Therefore, (123)$\in$K.

Since (123)$\in$K, (213)$\in$K, because K is a group. Since K$\triangleleft$A$_5$, for every element $\pi \in A_5$, π^{-1} (213)$\pi \in$ K. Let π = (12)(3k) where k $>$3. Then π^{-1} (213)π= (12k)$\in$ K. But by (4.11), (123) and (12k) generate A$_5$ making K = A$_5$.

4.13 Theorem: If K$\triangleleft$A$_5$ and K$\neq\{e\}$, then K contains a 3-cycle. (Thereby making K = A$_5$ by 4.12)

Proof: Suppose there exists a nonidentity element $\pi \in$K, such that π leaves fixed as many digits as possible. π Leaving a digit fixed means that under the permutation π, this digit is mapped onto itself. It suffices to prove this by considering cases.

Case I: Suppose that π leaves exactly all of the digits fixed. This, of course, is the identity element. Since it was assumed that $\pi \neq$ e, π cannot leave all the digits fixed.

Case II: Suppose that π leaves exactly one digit fixed. The result would be a 4-cycle or an element of the form, (ab)(cd). Suppose π is a 4-cycle (abcd), then (abcd) = (ab)(ac)(ad) is an odd permutation making $\pi \notin$ K. If π = (ab)(cd), then for every $\alpha \in A_5$, $\alpha^{-1}\pi\alpha \in$K. Let α = (cde). (cde)$^{-1}$ π(cde) = (ab)(de). π^{-1} = (ab)(cd) so (ab)(de)π^{-1} $\in$ K. But, (ab)(de)π^{-1} = (dec) which means π leaves two elements fixed. This is contrary to the definition of π. Therefore, π cannot leave exactly one digit fixed.

Case III: Suppose π leaves exactly two digits fixed. But this is what is being proven. It will be proven that this can be the only case.

Case IV: Suppose π leaves exactly three digits fixed. The result would be a 2-cycle. But a 2-cycle is an odd permutation making $\pi \in K$. Therefore, π cannot leave exactly three digits fixed.

Case V: Suppose π leaves exactly four digits fixed. This is impossible because this would leave the remaining digit fixed thereby making $\pi = e$. Therefore, π cannot leave exactly four digits fixed.

Case VI: Suppose π leaves none of the digits fixed. π could be of the form (abcde) or (abc)(de). But (abc)(de) is an odd permutation so $\pi = (abcde)$. Since $\pi^{-1} = (edcba)$ and $(cde) \in A_5$, $(cde)^{-1} \pi (cde) \in K$. But $(cde)^{-1}$ $\pi (cde) = (abdec)$ and $(edcba)(abdec) = (acd)$ meaning π leaves two elements fixed contrary to the definition of π. Therefore, π must leave at least one digit fixed. Therefore, K contains a 3-cycle making $K = A_5$.

4.13 Theorem: If $K \triangleleft S_5$, then $K = A_5$.

Proof: Suppose $K \triangleleft S_5$ but $K \neq \{e\}$, A_5 or S_5. Let $K \cap A_5 = H$. $H \neq \emptyset$, $H \triangleleft S_5$, and $H \subset A_5$. Since $H \triangleleft S_5$, for every $\alpha \in S_5$, $\alpha^{-1} h \alpha \in H$. This means that $\forall \pi \in A_5$, $\pi^{-1} h \pi \in H$ which means $H \triangleleft A_5$. But by the previous theorems, $H = A_5$. Similarly, $H \triangleleft K$.

Since $A_5 = H$, $K \cap A_5 = A_5$, making $A_5 \in K$, and $A_5 \neq K$ (by the hypothesis). It follows that there exists a $\pi \in K$ such that π is an odd permutation and $\pi \neq e$. Now to show that $K = S_5$. It is obvious that $K \subset S_5$. Suppose $\sigma \in S_5$. If σ is an even permutation, then $\sigma \in K$, so let σ be an odd permutation. Pick any $\delta \in A_5$, then $\delta^{-1} \sigma \delta = k \in K$. But this makes $\sigma = \delta k \delta^{-1}$ and because $\delta, k, \delta^{-1} \in K$, it follows that $\sigma \in K$. Therefore, $S_5 \subset K$. This makes $K = S_5$.

Since there are only two normal subgroups of S_5, namely $\{e\}$, and A_5, to prove that S_5 is not solvable it is necessary to show that the factor group $A_5/\{e\}$ is not Abelian.

4.14 Theorem: $A_5 \{e\}$ is not Abelian.

Proof: This follows easily by considering an example. (abc)(cde) $\neq$ (cde)(abc). Therefore, $A_5/\{e\}$ is not Abelian.

Therefore, there does not exist for S_5 a finite chain of subgroups for which the factor groups are Abelian. Therefore, an irreducible quintic is not solvable by radicals making it impossible to extend the rationals by radicals to include the roots of an irreducible quintic.

This procedure can be followed to prove S_n, $n > 5$, is not solvable. In fact, a general proof can be given.

CHAPTER V

CONCLUSION

The problem of determining the solvability of a polynomial equation by radicals by considering the solvability of its Galois group seems to be unrelated. But, as stated in Abel's theorem, this is the key as to whether or not a polynomial equation is solvable by radicals.

In Chapter Two, the set that is obtained by adjoining the square roots of integers was proven a field. This approach of extending the rationals by radicals may have been used for extending the rationals with roots from polynomial equations of degree greater than two. The problem with using this approach is making sure the roots of all the polynomials being considered are included in the set.

In Chapter Three, a different approach was used. Proving that the rationals could be extended by radicals to include the roots of a cubic involved the use of Abel's theorem. This theorem was not proven because the proof is beyond the scope of this paper. Showing what the theorem means and how it can be used is more in line as to the purpose of this paper.

In Chapter Four, it was proven that the rationals could not be extended by radicals to include the roots of fifth degree polynomial equations. This involved doing quite a bit of formularization of the elements of S_5 and A_5 which could be of use to someone studying permutation groups.

Although this paper only considered roots of polynomial equations of degree five or less, the conclusion arrived at in Chapter Four can be generalized. That is, it can be proven that the Galois group of an n^{th} degree polynomial equation $(n \geq 5)$, is not solvable.

BIBLIOGRAPHY

BIBLIOGRAPHY

1. Barnes, Wilfred E., Introduction to Abstract Algebra, (D. C. Heath and Company; 1963).

2. Miller, Earle B and Thall, Robert M., College Algebra, (Ronald Press Company; 1950).

3. Scott, W. R., Group Theory, (Prentice-Hall, Inc.; 1964).

4. VanDer Waerden, B. L. , Modern Algebra, (Frederich Ungar Publishing Co.; 1931).