GALOIS THEORY

by

CLARA DOROTHY SCHIEFERECKE

B. S., Marymount College, 1964

A MASTER'S REPORT

submitted in partial fulfillment of the

requirements for the degree

MASTER OF SCIENCE

Department of Mathematics

KANSAS STATE UNIVERSITY
Manhattan, Kansas

1966

Approved by:

Charles F. Koch

Major Professor

TABLE OF CONTENTS

INTRODUCTION

The discovery of the algebraic solution of the general quadratic equation is attributed to the Hindus. Tartaglia obtained the solution of the general cubic by radicals in the 16^{th} century and about the same time, Ferrari solved the general quartic by radicals. In the following years, mathematicians attempted to solve the general polynomial equation of degree greater than four by radicals. In 1824, N. H. Abel proved that such solutions cannot exist.

Early in the 19^{th} century, E. Galois (1811 - 1832) proved that an equation is solvable if and only if its group is a solvable group. By showing that the group of the general polynomial of degree n is the permutation group on n letters, Galois proved that the general polynomial of degree greater than four is not solvable by radicals. Galois' work had particular significance in the fact that his was the first attempt to utilize group theory as a tool.

A discussion of the development of his theory and its application to the general solution of polynomial equations is included in this report.

The theorems on commutator subgroups and solvable groups from group theory are introduced when needed. All other basic ideas from group theory and ring theory have been assumed.

It should be noted in this report that unless otherwise stated, all fields are assumed to have characteristic zero. This insures that every irreducible polynomial in a field of characteristic zero will be seperable. It should also be noted that following modern usage, polynomials are solvable and have roots.

Definition 1: A field F is a set of elements on which are defined two binary operations (called + and x for simplicity) which satisfy the following postulates:

Postulate 1: F is closed under + and x.

Postulate 2: + and x are commutative and associative.

Postulate 3: The set contains an identity element e_o for + and e_1 for x.

Postulate 4: x is distributive over +.

Postulate 5: Every element has an inverse with respect to + and x except e_o, which does not have an inverse with respect to x.

Suppose E and F are two fields on which the same two operations are defined. If every element of F is an element of E, then F is a subfield of E, denoted by $F \subset E$. If $F \subset E$, E is called an extension of F.

Definition 2: A non-empty set V is said to be a vector space over a field F if V is an abelian group under an operation denoted by +, and if for every $a \in F$, $v \in V$, there is defined an element, written as av, in V subject to

(1) $a(v + w) = av + aw$

(2) $(a + b)v = av + bv$

(3) $a(bv) = (ab)v$

(4) $1v = v$

for all $a,b \in F$, $v,w \in V$ (where the 1 represents the unit element of F under multiplication.)

The following two examples attempt to clarify the concept of a vector space.

Example 1: Let K be a field and let F be a subfield of K. Then K is a vector space over F. Let the + of the vector space be the addition of the elements of K. Define av, for $a \in F$, $v \in K$, to be the product of a and v as elements in the field K. Axioms (1), (2), and (3) are then consequences of the right-distributive, left-distributive, and associative laws, respectively, which hold since K is a field.

Example 2: Let F be any field and let V = F[x], the set of polynomials in x over F. F[x] is obviously an abelian group under +. It is also true that a polynomial can always be multiplied by an element of F. With these natural operations, F[x] is a vector space over F.

Definition 3: If $F \subset E$, the degree of E over F is the dimension of the vector space E over F where the dimension of E over F is the number of vectors in a basis. This will be denoted by (E:F). If (E:F) is finite, E will be called a finite extension of F.

Theorem 1: If F, B, and E are three fields such that $F \subset B \subset E$, then (E:F) = (E:B)(B:F).

Proof: Let w_i, i: 1,...,m, form a basis for E over B and u_i, i: 1,...,n, form a basis for B over F. Then for any $x \in E$, x can be represented as a linear combination of $w_1, \ldots, w_m$, i.e.:

(1) $x = \sum_{j=1}^{m} r_j w_j$, r_j B.

Similarly

(2) $r_j = \sum_{i=1}^{n} a_{ij} u_i$, a_{ij} F.

Substituting (2) into (1), an expression for x is obtained

(3) $x = \sum_{j=1}^{m} \sum_{i=1}^{n} a_{ij}(u_i w_j)$

Suppose x = 0. Then (1) implies that all $r_j = 0$, j: 1,...,m. If all $r_j = 0$, (2) implies that all $a_{ij} = 0$, j: 1,...,m, i: 1,...,n. But this implies that the m·n elements in (3) are linearly independant with respect to F. Hence (E:F) = m·n.

But (B:F) = n and (E:B) = m.

Hence (E:F) = (E:B)(B:F).

Corollary: If $F_1,\ldots,F_n$ are n fields such that $F_1 \subset F_2 \subset \cdots \subset F_n$, then $(F_n:F_1) = (F_2:F_1)(F_3:F_2)\ldots(F_n:F_{n-1})$.

Proof: The proof is obtained by extending the same technique used in proving the preceeding theorem.

An expression of the form $a_0x^n + a_1x^{n-1} + \ldots + a_n$ is called a polynomial in F of degree n if the coefficients $a_0,\ldots,a_n$ are elements of a field F and $a_0 = 0$. A polynomial in F is called reducible in F if it is equal to the product of two polynomials in F each of degree at least 1. Polynomials which are not reducible in F are called reducible. If f(x), g(x), and h(x) are polynomials in a field such that f(x) = g(x) h(x), then g(x) divides f(x) in F or g(x) is a factor of f(x). Certainly the degree of f(x) is equal to the sum of the degrees of g(x) and h(x), so that if neither g(x) nor h(x) is a constant then each has degree less than f(x). Hence by a finite number of factorizations, a polynomial can always be expressed as a product of irreducible polynomials in a field F.

Definition 4: Let E be an extension field of a field F. Let $a \in E$. If there exist polynomials with coefficients in F which have a as a root, a is called algebraic with respect to F.

Let $F \subset K$, and let $a \in K$. Let M be the collection of all subfields of K which contain both F and a. M is nonempty since $K \in M$. Now consider the intersection of all subfields of K which are elements of M. This intersection is again a subfield of K and will be denoted by F(a). Some properties of F(a) are:

1. F(a) contains both a and F.

2. Every subfield of K in M contains F(a), yet F(a) is itself in M. Thus F(a) is the smallest subfield of K containing both F and a. F(a) is the subfield obtained by adjoining a to F.

At this point a more constructive description of F(a) is considered. Consider all elements in K which can be expressed in the form $B_0 + B_1 a + \dots + B_s a^s$, where the B's range freely over F and s can be any non negative integer. As elements in K, one such element can be divided be another excluding division by zero. Let U be the set of all such quotients. U can be shown to be a subfield of K. Certainly $F \subset U$ and $a \in U$. Hence $F(a) \subset U$. Any subfield of K which contains both F and a by virtue of closure under addition and multiplication, must contain all elements $B_0 + B_1 a + \dots + B_s a^s$, $B_i \in F$. Hence F(a) must contain all these elements; being a subfield of K, F(a) must contain all quotients of such elements. Hence $U \subset F(a)$.

$$\left.\begin{array}{l}\text{But } U \subset F(a) \\ F(a) \subset U\end{array}\right\} \Longrightarrow \quad U = F(a)$$

Hence an internal construction of F(a) is obtained, namely U.

<u>Theorem 2</u>: The element $a \in K$ is algebraic over F if and only if F(a) is a finite extension.

Proof: Assume F(a) is a finite extension of K and let $(F(a):F) = m$. Consider $1, a, a^2, \dots, a^m \in F(a)$. These elements are linearly dependant over F. Therefore, there are elements $b_0, b_1, \ldots, b_m \in F$, not all zero such that $b_0 1 + b_1 a + \ldots + b_m a^m = 0$. Hence a is algebraic over F.

Let $p(x) \in F[x]$ be a monic polynomial of lowest positive degree satisfied by a. Let deg $p(x) = n$. $p(x) = x^n + b_1 x^{n-1} + \ldots + b_n$, $b_i \in F$. Certainly $a^n + b_1 a^{n-1} + \ldots + b_n = 0$.

Hence $a^n = -b_1 a^{n-1} - \ldots - b_n$.

Consider a^{n+1}, $a^{n+1} = -b_1 a^n - b_2 a^{n-1} - \ldots - b_n a$

$$= -b_1(-b_1 a^{n-1} - \ldots - b_n) - b_2 a^{n-1} - \ldots - b_n a.$$

Hence a^{n+1} is a linear combination of the elements $1, a, a^2, \ldots, a^{n-1}$ over F. Continuing this process for $k \geq 0$, a^{n+k} can be shown to be a linear combination over F. Now consider $T = \{B_0 + \ldots + B_{n-1} a^{n-1}\}$ where $B_i \in F$. Clearly T is closed under addition and multiplication. Hence T is a ring. Certainly $a \in T$ and $F \subset T$. That T is also a field is shown by the following: let $0 \neq u = B_0 + \ldots + B_{n-1} a^{n-1} \in T$ and let $h(x) = B_0 + \ldots + B_{n-1} x^{n-1} \in F[x]$. Since $u \neq 0$, and $u = h(a)$, $h(a) \neq 0$, then $p(x)$ does not divide $h(x)$. Hence $p(x)$ and $h(x)$ are relatively prime. Since this is true, there exists polynomials $s(x)$ and $t(x) \in F[x]$ such that $p(x)\, s(x) + h(x)\, t(x) = 1$ which implies that $1 = p(a)\, s(a) + h(a)\, t(a)$. But $p(a) = 0$. Hence $1 = h(a)\, t(a)$ or $1 = u\, t(a)$. Therefore $u^{-1} = t(a)$. In $t(a)$ all powers of a higher than n-1 can be replaced by a linear combination of $1, a, \ldots, a^{n-1}$ over F, hence $t(a) \in T$. Thus every non zero element of T has an inverse in T and T is a field.

Clearly $T \subset F(a)$, yet F and a are both contained in T. Therefore $T = F(a)$. Hence $F(a) = \{x \mid x = B_0 + \ldots + B_{n-1} a^{n-1}\}$. T is spanned over F by the elements $1, a, \ldots, a^{n-1}$. Hence $(T:F) \leq n$.

Consider $b_0 + b_1 + \ldots + b_{n-1}a^{n-1} = 0$ where $b_i \in F$, and not all $b_i = 0$. This would imply that a satisfies a polynomial of degree less than n which contradicts the original choice of p(x) as the monic polynomial of lowest degree. Hence $1, a, \ldots, a^{n-1}$ are linearly independant over F and form a basis of T over F. Hence $(T:F) = n$. Since $T = F(a)$, $(F(a):F) = n$ and F(a) is then a finite extension of F.

In the previous paragraphs algebraic elements in a given extension K of F were discussed, that is, elements which satisfy polynomials in F[x]. The following paragraphs discuss the problem of finding an extension of F in which a given polynomial has a root. The problem reduces to actually constructing the field.

Definition 5: If $p(x) \in F[x]$, then an element a lying in some extension field of F is called a root of p(x) if $p(a) = 0$.

Theorem 3: (Kronecker) If p(x) is a polynomial in F[x] of degree $n \geq 1$ and is irreducible over F, then there is an extension E of F such that $(E:F) = n$, in which p(x) has a root.

Proof: Let $E = \frac{F[x]}{(p(x))}$. Since p(x) is irreducible, E is a field.[1] Let $\bar{F} = \{a + (p(x)) \mid a \in F\}$. Let T be the mapping from F[x] into $\frac{F[x]}{(p(x))}$ such that $f(x)T = f(x) + (p(x))$. Consider the mapping T of F onto $\bar{F}$. Clearly F is isomorphic to $\bar{F}$. Since $F \subset F[x]$, $\bar{F} \subset E$. E is an extension of $\bar{F}$ and since $\bar{F} \cong F$, E can be considered an extension of F. Consider the dimension of E over F. The elements $1 + (p(x)), \ldots, x^{n-1} + (p(x))$ form a basis of E over F. Hence the degree of E over F equals the

[1]For a proof, refer to Elements of Modern Abstract Algebra, Miller, page 83.

degree of $p(x)$. For convenience of notation, let the element $xT = x + (p(x))$ in the field E be denoted as a. For $f(x) \in F[x]$, consider the element $f(x)T$ where $f(x) = B_0 + \dots + B_k x^k$. Then $f(x)T = B_0T + (B_1T)(xT) + \dots + (B_kT)(xT)^k$. But $xT = a$ and $B_0T = B_0$.

Hence
$$\begin{aligned} f(x)T &= B_0T + (B_1T)a + \dots + (B_kT)a^k \\ &= B_0 + B_1a + \dots + B_ka^k \\ &= f(a) \end{aligned}$$

Certainly $p(x) \in (p(x))$, hence $p(x)T = 0$. But $p(x)T = p(a)$. Hence the element $a = xT$ in E is a root of $p(x)$.

Corollary: If $f(x) \in F[x]$ then there is a finite extension E of F in which $f(x)$ has a root. Moreover, $(E:F) \leq \deg f(x)$.

Proof: Let $p(x)$ be an irreducible factor of $f(x)$; any root of $p(x)$ is a root of $f(x)$. By the preceeding theorem there is an extension E of F with $(E:F) = \deg p(x) \leq \deg f(x)$ in which $p(x)$ and so $f(x)$ has a root.

Theorem 4: Let $f(x) \in F[x]$ be of degree $n \geq 1$. Then there is an extension E of F of degree at most $n!$ in which $f(x)$ has n roots.

Proof: A root of multiplicity m is counted as m roots. By the preceeding corollary, there is an extension E_0 of F with $(E_0:F) \leq n$ in which $f(x)$ has a root α. Hence in $E_0[x]$, $f(x) = (x-\alpha)\, q(x)$ where the degree of $q(x) = n-1$. Continuing the above process, there is an extension E of E_0 of degree at most $(n-1)!$ in which $q(x)$ has n-1 roots. Now every root of $f(x)$ is either α or a root of $q(x)$, hence all n roots of $f(x)$ have been obtained. Then $(E:F) = (E:E_0)(E_0:F) \leq (n-1)!n = n!$

Definition 6: Let $f(x) \in F[x]$. A splitting field over F for $f(x)$ is a finite extension E of F if over E, but not over any proper subfield of E, $f(x)$ can be factored as a product of linear factors.

Theorem 4 guarantees the existence of a splitting field. Given a polynomial of degree n over F, the splitting field for this polynomial is a finite extension of F of degree at most n! over F. Given a splitting field of $f(x)$, this splitting field will be the minimal extension of F in which the polynomial $f(x)$ has n roots where n equals the degree of $f(x)$.

Consider now any two splitting fields for a polynomial over a field F. The following theorems will prove that a splitting field is unique up to an isomorphism.

Lemma 1: Let F and F' be two fields and let T be an isomorphism of F onto F' such that $aT = a'$ for $a \in F$ and $a' \in F'$. Let T_1 be a mapping from $F[x]$ to $F'[t]$ such that $f(x)T_1 = (a_0x^n + \dots + a_n)T_1 = a_0't^n + \dots + a_n'$. Then T_1 is an isomorphism.

Proof: $f(x)T_1 + g(x)T_1 = (a_0't^n + \dots + a_n') + b_0't^n + \dots + b_n'$ $= (a_0' + b_0')t^n + (a_1' + b_1')t^{n-1} + \dots + (a_n' + b_n') = (f(x) + g(x))T_1$. Similarly for multiplication. Hence T_1 is operation preserving. Clearly T_1 is one-to-one and onto since T is one-to-one and onto. Hence T_1 is an isomorphism.

Lemma 2: There is an isomorphism T_2 of $\dfrac{F[x]}{(f(x))}$ onto $\dfrac{F'[t]}{(f'(t))}$ with the property that for every $a \in F$, $aT_2 = a'$, where $a' \in F'$.

Proof: Let T_2 be defined by $(g(x) + (f(x)))T_2 = g'(t) + (f'(t))$. The proof follows.

Theorem 5: If $p(x)$ is irreducible in $F[x]$ and if v is a root of $p(x)$, then $F(v)$ is isomorphic to $F'(w)$ where w is a root of $p'(t)$;

moreover, this isomorphism T can be so chosen that

1. $vT = w$

2. $aT = a'$ for every $a \in F$.

Proof: Let v be a root of p(x) lying in some extension K of F. Let $M = \{ f(x) \in F[x] \mid f(v) = 0 \}$. Trivially M is an ideal of F[x], and $M \neq F[x]$. Hence $M = (p(x))$. Let T_1 be a mapping such that: $q(x)T_1 = q(v)$ for all $q(x) \in F[x]$. The kernel of T_1 is p(x). By the fundamental homorphism theorem for rings, $\frac{F[x]}{(p(x))} \cong F(v)$. Let this isomorphism be denoted by T_2. Clearly for every $a \in F$, $aT_1 = a$. Under this isomorphism every element of F remains fixed and $v = (x + p(x))T_2$. p(x) irreducible implies that p'(t) is irreducible in F'[t]. Again there exists an isomorphism T_3 of $\frac{F'[t]}{(p'(t))}$ onto F'(w) such that T_3 leaves every element of F' fixed and $(t + (p'(t)))T_3 = w$. By Lemma 2, $\frac{F[x]}{(p(x))} \cong \frac{F'[t]}{(p'(t))}$. Hence $F(v) \cong \frac{F[x]}{(p(x))} \cong \frac{F'[t]}{(p'(t))} \cong F'(w)$.

Then $v \longrightarrow x + (p(x)) \longrightarrow t + (p'(t)) \longrightarrow w$ and $vT = w$, where $T = T_1T_2T_3$. For $a \in F$, $a \longrightarrow a + (p(x)) \longrightarrow a' + (p'(t)) \longrightarrow a'$. Hence $aT = a'$.

Theorem 6: Any two splitting fields E and E' of the polynomial $f(x) \in F[x]$ and $f'(t) \in F'[t]$, respectively, are isomorphic by an isomorphism T_1 with the property that $aT_1 = a'$ for every $a \in F$.

Proof: Let $(E:F) = 1$. Then $E = F$. By Lemma 1, f'(t) splits over F' into a product of linear factors which implies that $E' = F'$. Then $T_1 = T$ will be the required automorphism where $f(x)T = (a_0x^n + \dots + a_n)T = a_0't^n + \dots + a_n'$.

Assume the result to be true for any field F_0 and any polynomial $f(x) \in F[x]$ provided the degree of some splitting field E_0 of f'(x) has degree less than n over F_0, that is, $(E_0:F_0) < n$. Let $(E:F) = n > 1$. Since $n > 1$, f(x) has an irreducible factor p(x) of degree $r > 1$. But E splits f(x), hence E must split p(x). This implies the existence of an $a \in E$ such that $p(a) = 0$. Bu Theorem 3, $(F(v):F) = r$. Similarly there exists a $w \in E$ such that $p'(w) = 0$. By Theorem 5, $F(v) \cong F(w)$. Now $(F(v):F) = r > 1$. Hence $(E:F(v)) = \frac{(E:F)}{(F(v):F)} = \frac{n}{r} < n$. E is a splitting field for f(x) considered as a polynomial over $F_0 = F(v)$, for no subfield of E, containing F_0 and hence F, can split f(x), since E was assumed to be a splitting field for f(x). Likewise E' is a splitting field for f'(t) over $F_0' = F'(w)$. Bu the induction hypothesis there is an isomorphism T_1 of E onto E' such that $aT_1 = aT$ for all $a \in F_0$. Since $F \subset F_0$, $aT_1 = aT = a'$.

<u>Corollary</u>: If p(x) is a polynomial in a field F, then any two splitting fields for p(x) are isomorphic.

Proof: Let E = F' and T be the identity mapping. Then the corollary follows from Theorem 6.

By an automorphism of a field K is meant a mapping from K onto itself such that this mapping is operation preserving and one-to-one. Two automorphisms T_1 and T_2 of K are said to be distinct if $T_1(a) \neq T_2(a)$ for some element a K.

<u>Theorem 7</u>: Let K be a field. If $T_1, \ldots, T_n$ are n distinct automorphisms of K, then it is impossible to find elements $a_1, \ldots, a_n$, not all zero, in K such that $a_1T_1(u) + \ldots + a_nT_n(u) = 0$ for all $u \in K$.

Proof: Assume that there exists a set of elements, $a_1, \ldots, a_n \in K$, not all zero, such that $a_1T_1(u) + a_2T_2(u) + \ldots + a_nT_n(u) = 0$ for all $u \in K$. Then there exists a minimal relation:

(1) $a_1T_1(u) + \ldots + a_mT_m(u) = 0$, where $a_i \neq 0$.

Let $m = 1$, then $a_1T_1(u) = 0$ for all $u \in K$ implies $a_1 = 0$. Hence $m > 1$. Since these automorphisms are distinct, there exists a $c \in K$ such that $T_1(c) \neq T_m(c)$. Consider $a_1T_1(cu) + \ldots + a_mT_m(cu) = 0$. This must hold true since $cu \in K$. But T_i is an automorphism. Hence

(2) $a_1T_1(c)T_1(u) + \ldots + a_mT_m(c)T_m(u) = 0.$

Multiply (1) by $T_1(c)$ and subtract from (2). This results in

(3) $a_2(T_2(c) - T_1(c))T_2(u) + \ldots + a_m(T_m(c) - T_1(c)) = 0.$

Let $b_i = a_i(T_i(c) - T_1(c))$ for i: $2,\ldots,m$; $b_m = a_m(T_m(c) - T_1(c)) \neq 0$, since $a_m \neq 0$ and $T_m \neq T_1(c)$. But (3) is then a sum of fewer terms than the original relation wich was assumed to be minimal. Hence the theorem is proved.

Corollary: If E and E' are two fields, and $T_1,\ldots,T_n$ are n mutually distinct isomorphisms mapping E into E', then $T_1,\ldots,T_n$ are independant.

Definition 7: If G is a group of automorphisms of K, then the fixed field of G is the set of all elements $a \in K$ such that $T(a) = a$ for all $T \in G$.

Lemma 3: The fixed field of G is a subfield of K.

Proof: Let a,b be in the fixed field of G. The fixed field is non empty since $T(1) = 1$ for all $T \in G$.

$T(a-b) = T(a) + T(-b) = T(a) - T(b) = a - b$

$T(ab^{-1}) = T(a)T(b^{-1}) = T(a)(T(b))^{-1} = ab^{-1}$

Hence the fixed field of G is a subfield of K.

Theorem 8: If $T_1,\ldots,T_n$ are n mutually distinct isomorphisms of a field E into E', and if F is the fixed field of E, then $(E:F) \geq n$.

Proof: Assume $(E:F) = r < n$. Let $w_1,\ldots,w_r$ be a generating system of E over F.

Consider the homogeneous linear equqtions:

(1) $T_1(w_1)x_1 + T_2(w_1)x_2 + \dots + T_n(w_1)x_n = 0$

(2) $T_1(w_2)x_1 + T_2(w_2)x_2 + \dots + T_n(w_2)x_n = 0$

. . . .

(r) $T_1(w_r)x_1 + T_2(w_r)x_2 + \dots + T_n(w_r)x_n = 0.$

Since there are more unknowns than equqtions, there exists a non-trivial solution. Let the non trivial solution be denoted by $x_1,\dots,x_n$.
For any $\alpha \in E$, $\alpha = a_1w_1 + \dots + a_rw_r$, $a_i \in F$. Multiply equation (1) by $T_1(a_1)$, equation (2) by $T_2(a_2)$, equation (r) by $T_r(a_r)$. Since $a_i \in F$, $T_1(a_i) = T_j(a_i)$. Also $T_j(a_i)T_j(w_i) = T_u(a_iw_i)$.
Now $T_i(a_1w_1)x_1 + \dots + T_n(a_1w_1)x_n = 0$

. . . .

$T_1(a_rw_r)x_1 + \dots + T_n(a_rw_r)x_n = 0.$

Consider the sum of these equations. It is true that
$T_i(a_1w_1) + T_i(a_2w_2) + \dots + T_i(a_rw_r) = T_i(a_1w_1 + \dots + a_rw_r) = T_i(\alpha)$.
Hence a non-trivial dependance relation $T_1(\alpha)x_1 + \dots + T_n(\alpha)x_n = 0$ is obtained. By the corollary to Theorem 7, this is impossible.
Hence $(E:F) \geq n$.

Corollary: If $T_1,\dots,T_n$ are automorphisms of the field E, and if F is the fixed field, then $(E:F) \geq n$.

Definition 8: An extension field E of a field F is called a normal extension of F if E is a finite extension of F such that F is the fixed field of G(E,F) where G(E,F) is the group of automorphisms of E that leave F fixed.

Certainly it is true that the field F may be smaller than the fixed field of G(E,F) since there may be some elements in E that remain fixed by every automorphism in G(E,F).

Theorem 9: If $T_1,\dots,T_n$ is a group of automorphisms of a field E and if F is the fixed field of $T_1,\dots,T_n$, then $(E:F) = n$.

Proof: Let the identity of $T_1,\dots,T_n$ be T_1. Assume that $(E:F) > n$. Then there exist α_i, i: $1,\dots,(n+1)$, $\in E$ which are linearly independant with respect to F. There exists a non-trivial solution in E to the system of equations:

$$x_1T_1(\alpha_1) + x_2T_1(\alpha_2) + \dots + x_{n+1}T_1(\alpha_{n+1}) = 0$$

$$\dots\dots\dots\dots\dots\dots\dots\dots\dots$$

$$x_1T_n(\alpha_1) + x_2T_n(\alpha_2) + \dots + x_{n+1}T_n(\alpha_{n+1}) = 0.$$

The solution cannot lie in F, otherwise the first equation would be a dependance between $\alpha_1,\dots,\alpha_{n+1}$. Let $a_1,\dots,a_r,0,\dots,0$ be the nontrivial solution with the least number of elements different from zero. $r \neq 1$ since $a_1T_1(\alpha_1) = 0$ implies $a_1 = 0$. Assume that $\alpha_r = 1$. Then:

(1) $a_1T_i(\alpha_1) + \dots + a_{r-1}T_i(\alpha_{r-1}) + T_i(\alpha_r) = 0$

for i: $1,\dots,n$. Now $a_1,\dots,a_{r-1}$ cannot all be elements of F. Let $a_1 \in E$, $a_1 \notin F$. Let T_k be the automorphism for which $T_k(a_1) \neq a_1$. Consider $T_kT_1,\dots,T_kT_n$. This is a permutation of $T_1,\dots,T_n$. Apply T_k to (1):

$$T_k(a_1)T_kT_j(\alpha_1) + \dots + T_k(a_{r-1})T_kT_j(\alpha_{r-1}) + T_kT_j(\alpha_r) = 0$$

for j: $1,\dots,r$, so that from $T_kT_j = T_i$

(2) $T_k(a_1)T_i(\alpha_1) + \dots + T_k(a_{r-1})T_i(\alpha_{r-1}) + T_i(a_r) = 0$

Subtract (2) from (1).

(3) $(a_1 - T_k(a_1))T_i(a_1) + \dots + (a_{r-1} - T_k(a_{r-1}))T_i(a_{r-1}) = 0.$

(3) is a non trivial solution to the system having fewer than r elements different from 0, contrary to the choice of r. Hence $(E:F) = n$.

Corollary 1: If F is the fixed field for the finite group G, then each automorphism T that leaves F fixed must belong to G.

Proof: Let $(E:F)$ = order of $G = n$. Let T be an automorphism not in G. Then F would remain fixed under the $(n+1)$ elements; T and the elements in G. Hence $(E:F) = (n+1)$ which contradicts Theorem 9.

Corollary 2: There are no two finite groups G_1 and G_2 with the same fixed field.

Definition 9: Let $f(x)$ be a polynomial in F, then $f(x)$ is called separable if its irreducible factors do not have repeated roots. An element $a \in E$ where E is an extension of F is called separable if it is a root of a separable polynomial $f(x)$ in F. E is a separable extension if each element of E is separable.

Lemma 4: Let K be the splitting field of $f(x)$ in $F[x]$ and let $p(x)$ be an irreducible factor of $f(x)$ in $F[x]$. If the roots of $p(x)$ are $a_1, \ldots, a_n$, then for each i there exists an automorphism $T_i \in G(K,F)$ such that $T_1(a_1) = a_1$.

Proof: Let a_1, a_i be any two roots of $p(x)$. Consider $F_1 = F(a_1)$ and $F_1' = F(a_i)$, by Theorem 5, $F_1 \cong F_1'$. This automorphism maps a_1 onto a_i and leaves every element of F fixed. K is the splitting field for $f(x)$ over F_1 and F_1'. Hence there exists an automorphism T_i of K such that $T_i(a_1) = T(a_1) = a_i$, where T is the automorphism of F_1 onto F_1' and T_i leaves every element of F fixed.

Theorem 10: K is a normal extension of F if and only if K is the splitting field of some polynomial over F.

Proof: Assume that K is a normal extension of F. Consider $K = F(a)$, and $p(x) = (x - T_1(a)) \ldots (x - T_n(a))$ where $p(x)$ is a polynomial over K and $T_i \in G(K,F)$. Then $p(x) = x^n - \ldots + (-1)^n b_n$ where the b_i are the elementary symmetric functions in $a = T_1(a), \ldots, T_n(a)$.

But then $b_1, \ldots, b_n$ are each invariant with respect to every $T \in G(K,F)$. Since K is normal over F, each b_i must be in F. Hence K splits the polynomial into a product of linear factors. It has been shown that F(a) is the minimal subfield containing F and a, hence K is the splitting field of p(x) over F.

Assume that K is the splitting field of some polynomial over F. The proof is by induction: assume that for any pair of fields K_1, F_1 of degree less than (K:F) that whenever K_1 is the splitting field over F_1 of a polynomial in $F_1[x]$, then K_1 is normal over F_1.

If f(x) over F splits into linear factors over F, then F = K. Hence K is a normal extension. Let p(x) be an irreducible factor of degree $r > 1$. Now $a_1, \ldots, a_r \in K$. Certainly K is the splitting field of f(x) considered as a polynomial over $F(a_1)$. Now $(K:F(a_1) = \frac{(K:F)}{(F(a_1):F)} = \frac{n}{r} < n$. Hence K is a normal extension of $F(a_1)$. Let u K be left fixed by every T_i G(K,F). Certainly every $T_i \in G(K,F(a_1))$ leaves F fixed, hence leaves u fixed. This implies that $u \in F(a_1)$. Thus $u = B_0 + \ldots + B_{r-1}a_1^{r-1}$ where $B_i \in F$. By Lemma 4, there exists a $T_i \in G(K,F)$ such that $T_i(a_1) = a_i$. But T_i leaves u and B_i fixed. Now apply T_i to u. $u = B_0 + \ldots + B_{r-1}a_i^{r-1}$ for i: 1,...,r. Consider $q(x) = (B_0 - u) + B_1x + \ldots + B_{r-1}x^{r-1}$ in K[x]. q(x) has degree at most r-1 but has r roots. Hence all coefficients must be zero and $u = B_0$. Hence $u \in F$ and K is normal over F.

Definition 11: Let f(x) be a polynomial in F[x] and let K be its splitting field over F. The Galois group of f(x) is the group of all automorphisms of K leaving every element of F fixed. This group will be denoted by G(K,F).

The following theorem gives the relation between the structure of a splitting field and its group of automorphisms. It is known as the fundamental theorem of Galois Theory.

Theorem 11: If $p(x)$ is a separable polynomial in a field F, and G the group of the equation $p(x) = 0$ where E is the splitting field of $p(x)$, then

(1) Each intermediate field, B, is the fixed field for a subgroup G_B of G and distinct subgroups have distinct fixed fields.

(2) The intermediate field B is a normal extension of F if and only if the subgroup G_B is a normal subgroup of G. In this case the group of automorphisms of B which leaves F fixed is isomorphic to the factor group (G/G_B).

(3) For each intermediate field B, $(B:F)$ = index of G_B and $(E:B)$ = order of G_B.

Proof: (1) Let $p(x)$ lie in any intermediate field. Then E is the splitting field for $p(x)$. Hence, E is a normal extension of each intermediate field B; then B is the fixed field of the subgroup of G consisting of the automorphisms which leave B fixed. By Corollary 2, Theorem 9, distinct subgroups have distinct fixed fields.

(3) Let $F \subset B \subset E$. Since B is the fixed field for G_B of G, $(E:B)$ = order of G_B. (Theorem 9) Let $o(G)$ = order of the group G, and $i(G)$ = index of G. $o(G) = o(G_B)\, i(G_B)$. But $(E:F) = o(G)$ and $(E:F) = (E:B)(B:F)$ together with $o(G) = o(G_B)(B:F)$ imply that $(B:F) = i(G_B)$.

(2) Let G_B be a subgroup of G. Let $T_1, T_2 \in G_B$. Then for any $a \in B$, $T_1(a) = a = T_2(a)$. Let TT_1, $TT_2 \in G_B$. Then for any $a \in B$,

$TT_1(a) = T(a) = TT_2(a)$. Hence the elements of G in any one left coset of G_B map B in the same way. Let $T_1T \in T_1G_B$ and $T_2T \in T_2G_B$ where $T_1, T_2 \in G$. Now $T_1T(a) = T_1(a)$ and $T_2T(a) = T_2(a)$ for all $a \in B$. Suppose $T_1(a) = T_2(a)$. This implies $T_2^{-1}T_1(a) = a$ which implies that $T_2^{-1}T_1$ is an element of G_B. Let $T_2^{-1}T_1 = T_3 \in G_B$. Then $T_1 = T_2T_3$ which implies that $T_1G_B = T_2T_3G_B = T_2G_B$. Hence elements of different cosets give different isomorphisms. The number of distinct isomorphisms is equal to the index of G_B in G.

Each isomorphism of B which is the identity on F is given by an automorphism belonging to G, i.e., it maps B isomorphically into some other subfield B' of E and is the identity on F. Let $T \in G$, $T \notin G_B$. Let $b \in B$, $b' \in B'$ and $T(b) = b'$. Let G_B be the group of B. Then $TG_BT^{-1}(b') = TG_BT^{-1}T(b) = TG_B(b) = T(b) = b'$. Hence the group TG_BT^{-1} leaves every element $b' \in B'$ unaltered. Hence the isomorphisms are identical to the automorphisms if and only if G_B is a normal subgroup of G, if and only if $G_B = TG_BT^{-1}$. Hence the number of automorphisms of B is equal to the index of G_B in G and equal to (B:F) if and only if G_B is a normal subgroup of G. But B is a normal extension of F if and only if the number of automorphisms of B is (B:F).

<u>Definition 12</u>: A group G is said to be solvable if there exists a finite chain of subgroups $G = N_0 \subset N_1 \subset \dots \subset N_k = (e)$ where each N_i is a normal subgroup of N_{i-1} and such that every factor group N_{i-1}/N_i is abelian.

The symmetric group on three letters is a solvable group. Let $N_1 = \{(e), (1,2,3), (1,3,2)\}$, N_1 is a normal subgroup of S_3 and $N_1/(e)$ and S_3/N_1 are both abelian of orders 3 and 2 respectively.

Given the group G and $a, b \in G$, then the commutator of a and b is the element $a^{-1}b^{-1}ab$. The commutator subgroup, G', is the subgroup generated by all the commutators in G. G' is a normal subgroup of G. Let $\alpha_1, \ldots, \alpha_n \in G'$. Then $x^{-1}\alpha_1, \ldots, \alpha_n \in G'$. Let $\alpha_1 = a^{-1}b^{-1}ab$. $x^{-1}a^{-1}b^{-1}abxx^{-1}\alpha_2 \ldots \alpha_n x = (x^{-1}a^{-1}xx^{-1}b^{-1}xx^{-1}axx^{-1}bx)(x^{-1}\alpha_2 \ldots \alpha_n x)$ $= (x^{-1}ax)^{-1}(x^{-1}bx)^{-1}(x^{-1}ax)(x^{-1}bx)(x^{-1}\alpha_2 \ldots \alpha_n x)$. But $(x^{-1}ax)^{-1}(x^{-1}bx)^{-1}(x^{-1}ax)(x^{-1}bx)$ is a commutator and hence is an element of G'. Continuing this process, $x^{-1}\alpha_1 \ldots \alpha_n x$ can be shown to be a product of commutators. Hence $x^{-1}G'x = G'$ and G' is a normal subgroup of G. G/ G' is abelian: for let $a, b \in G$, $(aG')(bG') = (ab)G'$ $= ab(b^{-1}a^{-1}ba)G' = (ba)G' = (bG')(aG')$.

Let M be a normal subgroup of G such that G/M is abelian. Then $G' \subset M$. Let $a, b \in G$, then $(aM)(bM) = (bM)(aM)$. $(ab)M = (ba)M$ implies $a^{-1}b^{-1}abM = M$ which implies that $a^{-1}b^{-1}ab$ M. Hence M contains all commutators and thus contains the group these generate.

Consider $G^{(2)} = (G')'$. $G^{(2)}$ is the subgroup of G generated by all elements $(a')^{-1}(b')^{-1}a'b'$ where $a', b' \in G'$. The proof that $G^{(2)}$ is a normal subgroup of G' and G is similar to the proof that G' is a normal subgroup of G. Define $G^{(m)} = G^{(m-1)'}$.

<u>Lemma 5</u>: G is solvable if and only if $G^k = (e)$ for some integer k.

Proof: If $G^k = (e)$, let $N_0 = G$, $N_1 = G'$, $N_2 = G^{(2)}, \ldots, N_k = G^{(k)} = (e)$. Then $G = N_0 \supset N_1 \supset \ldots \supset N_k = (e)$. Each N_i is normal in G, hence each N_i is normal in N_{i-1}. Now $N_{i-1}/N_i = G^{i-1}/G^i = G^{i-1}/(G^{i-1})'$. Hence G^{i-1}/G^i is abelian. Hence G is solvable.

If G is a solvable group, then $G = N_0 \supset N_1 \supset \ldots \supset N_k = (e)$. Hence the commutator subgroup N'_{i-1} of N_{i-1} must be contained in N_i.

Hence $N_1 \supset N_0' = G'$, $N_2 \supset N_1' \supset (G')' = G^{(2)}$, $N_3 \supset N_2' \supset N_2' \supset (G^2)' = G^3$, $, \ldots, N_i \supset G^i$, $(e) = N_k \supset G^k$. Hence $G^{(k)} = (e)$.

Corollary: If G is a solvable group and if $\overline{G}$ is a homomorphic image of G, then $\overline{G}$ is a solvable group.

Proof: Since $\overline{G}$ is a homomorphic image of G, $(\overline{G})^k$ is the image of $G^{(k)}$. Since $G^k = (e)$ for some k, $(\overline{G})^k = (e)$ for the same k, hence by Lemma 5, $\overline{G}$ is solvable.

Lemma 6: Let $G = S_n$, where $n \geq 5$, then G^k for k: 1,2,..., contains every 3-cycle of S_n.

Proof: If N is a normal subgroup, then N' must also be a normal subgroup. Now if N is a normal subgroup of $G = S_n$, where $n \geq 5$, which contains every 3-cycle, then N' must also contain every 3-cycle. Let $a = (1,2,3)$, $b = (1,4,5) \in N$. Then $a^{-1}b^{-1}ab =$ $(3,2,1)(5,4,1)(1,2,3)(1,4,5) = (1,4,2)$ must be in N'. Since N' is a normal subgroup of G, for any $\pi \in S_n$, $\pi^{-1}(1,4,2)\pi \in N$. Choose a $\pi \in S_n$ such that $\pi(1) = i_1$, $\pi(4) = i_2$, and $\pi(2) = i_3$, where i_1, i_2, i_3, are any distinct integers in the range from 1 to n; then $\pi^{-1}(1,4,2)\pi = (i_1, i_2, i_3)$ is in N'. Hence N' contains all 3-cycles.

Now let N = G. G is normal in G and G' contains all 3-cycles; since G' is normal in G, $G^{(2)}$ contains all 3-cycles; since $G^{(2)}$ is normal in G, $G^{(3)}$ contains all 3-cycles. Continuing this process, G^k contains all 3-cycles for arbitrary k.

Theorem 12: S_n is not solvable for $n \geq 5$.

Proof: If $G = S_n$ by Lemma 6, G^k contains all 3-cycles in S_n for every k. Therefore $G^k \neq (e)$ for any k, hence G cannot be solvable.

Theorem 13: Let F be a field and let $F(x_1, \ldots, x_n)$ be the field of rational functions in $x_1,\ldots,x_n$ over F. Let S be the field of symmetric rational functions: then

(1) $(F(x_1,\ldots,x_n):S) = n!$

(2) $G(F(x_1,\ldots,x_n),S) = S_n$, the symmetric group of degree n.

(3) If $a_1,\ldots,a_n$ are the elementary symmetric functions in $x_1,\ldots,x_n$, then $S = F(a_1,\ldots,a_n)$.

(4) $F(x_1,\ldots,x_n)$ is the splitting field of the polynomial $t^n - a_1t^{n-1} + \ldots + (-1)^n a_n$ over $F(a_1,\ldots,a_n) = S$.

Proof: Let S_n be the symmetric group of degree n: for $\sigma \in S_n$ Let $\sigma(i)$ be the image of i under σ for $1 \leq i \leq n$. For $\sigma \in S_n$, and $r(x_1,\ldots,x_n) \in F(x_1,\ldots,x_n)$, define the mapping which takes $r(x_1,\ldots,x_n)$ onto $r(x_{\sigma(1)},\ldots,x_{\sigma(n)})$. Certainly the elements of S_n define automorphisms of $F(x_1,\ldots,x_n)$. The fixed field of $F(x_1,\ldots,x_n)$ with respect to S_n will consist of all rational functions $r(x_1,\ldots,x_n)$ such that $r(x_1,\ldots,x_n) = r(x_{\sigma(1)},\ldots,x_{\sigma(n)})$ for all $\sigma \in S_n$. But this fixed field then consists of elements in F known as the symmetric rational functions, hence the fixed field is S. Since S_n is a group of automorphisms of $F(x_1,\ldots,x_n)$ leaving S fixed, $S_n \subset G(F(x_1,\ldots,x_n),S)$ Hence $(F(x_1,\ldots,x_n):S) \geq o(G(F(x_1,\ldots,x_n),S)) \geq o(S_n) = n!$ Consider the field $F(a_1,\ldots,a_n)$ obtained by adjoining $a_1,\ldots,a_n$ to F where $a_1 = \sum_{i=1}^{n} x_i$, $a_2 = \sum_{i\ j} x_ix_j$,..., $a_n = x_1x_2\ldots x_n$. Since $a_i \in S$, and the a_i represent the elementary symmetric functions, the field $F(a_1,\ldots,a_n) \subset S$. Now consider the polynomial $p(t) = t^n - a_1t^{n-1} + \ldots + (-1)^n a_n$ where $a_i \in F(a_1,\ldots,a_n)$. p(t) factors over $F(x_1,\ldots,x_n)$ as $p(t) = (t-x_1)(t-x_2)\ldots(t-x_n)$. Hence p(t) splits as a product of linear factors over $F(x_1,\ldots,x_n)$. Suppose $p(t)$ splits over a proper subfield K of $F(x_1,\ldots,x_n)$. K would contain F and all the roots of $p(t)$, hence $K = F(x_1,\ldots,x_n)$. Therefore $F(x_1,\ldots,x_n)$ is the splitting field of $p(t)$. But $p(t)$ has degree n, hence $(F(x_1,\ldots,x_n):F(a_1,\ldots,a_n))$ is less than or equal to n! Now

$n! \geq (F(x_1,\ldots,x_n):F(a_1,\ldots,a_n)) = (F(x_1,\ldots,x_n):S)(S:F(a_1,\ldots,a_n)) \geq n!$

But this implies that $(F(x_1,\ldots,x_n):S) = n!$, hence $(S:F(a_1,\ldots,a_n)) = 1$, which implies that $S = F(a_1,\ldots,a_n)$. $n! \geq o(G(F(x_1,\ldots,x_n),S)) \geq o(S_n) = n!$ and $S_n \subset G(F(x_1,\ldots,x_n),S)$, implies $G(F(x_1,\ldots,x_n),S) = S_n$.

Definition 13: Given a field F and a polynomial $p(x)$ F x , $p(x)$ is solvable by radicals over F if there exists a finite sequence of fields, $F_1 = F(w_1)$, $F_2 = F_1(w_2),\ldots,F_k = F_{k-1}(w_k)$ such that $w_1^{r_1} \in F$, $w_2^{r_2} \in F_1,\ldots,w_k^{r_k} \in F_{k-1}$ such that the roots of $p(x)$ all lie in F_k.

Example: Consider the polynomial $x^4 + 3x^3 + 5x^2 + 3x + 14$ over the field of rational numbers. The roots of the polynomial are $\frac{-3 \pm \sqrt{-7}}{2}$ and $\pm\sqrt{-1}$. Let $F_1 = F(\sqrt{-7})$, $(\sqrt{-7})^2 \in F$, $F_2 = F_1(\sqrt{-1})$, $(\sqrt{-1})^2 \in F_1$. The extension field F_2 contains all the roots of the given polynomial. The sequence of fields is finite, hence $p(x)$ is solvable by radicals over F.

Definition 14: Let $F(a_1,\ldots,a_n)$ be the field of rational functions in the n variables $a_1,\ldots,a_n$ over F. The general polynomial of degree n over F, $p(x) = x^n + b_1x^{n-1} + \ldots + b_n$ can be considered as the particular polynomial $p(x) = x^n - a_1x^{n-1} + \ldots + (-1)^n a_n$ over the field $F(a_1,\ldots,a_n)$. $p(x)$ is solvable by radicals if it is solvable by radicals over $F(a_1,\ldots,a_n)$.

Lemma 7: Let F be a field containing all n^{th} roots of unity for some n. Let $a \neq 0 \in F$. Let $x^n - a \in F[x]$ and let K be its splitting field over F. Then:

(1) $K = F(u)$ where u is any root of $x^n - a$.

(2) The Galois group of $x^n - a$ is abelian.

Proof: Since F contains all n^{th} roots of unity, it contains $w = e^{\frac{2\pi i}{n}}$. Certainly $w^n = 1$. Let $u \in K$ be any root of $x^n - a$, then $u, wu, w^2u, \ldots, w^{n-1}u$ are distinct roots of $x^n - a$. Suppose the roots are not distinct: $w^iu = w^ju$, $0 \leq i < j < n$, then $(w^i - w^j)u = 0$, $u \neq 0$, implies $w^i = w^j$. Dividing both sides of the equation by w^i yields $w^{j-i} = 1$. But $0 < j-i < n$. Hence $w^{j-i} \neq 1$, $w^j \neq w^i$ and the roots are distinct.

Since $w \in F$, $u, wu, \ldots, w^{n-1}u \in F(u)$. Hence $F(u)$ splits $x^n - a$. $F(u)$ is the smallest subfield containing F and u. Hence $F(u) = K$.

Let $T_1, T_2 \in G(F(u), F)$. Since u is a root of $x^n - a$, $T_1(u)$ and $T_2(u)$ are roots of $x^n - a$ and $T_1(u) = w^iu$, $T_2(u) = w^ju$ for some i and j. Thus $T_1T_2(u) = T_1(w^ju) = T_1(w^j)T_1(u) = w^jT_1(u) = w^jw^iu = w^{i+j}u$. Similarly $T_2T_1(u) = w^{j+i}u$. Therefore T_1T_2 and T_2T_1 agree on u and F, hence they agree on $F(u)$. But this implies that $T_1T_2 = T_2T_1$. Hence the Galois group is abelian.

Theorem 14: If $p(x) \in F[x]$ is solvable by radicals over F, then the Galois group of $p(x)$ is a solvable group.

Proof: Let the Galois group of $p(x)$ over F be $G(K,F)$. Let K be the splitting field of F. Since $p(x)$ is solvable by radicals, there exists a sequence of fields:

$F \subset F_1 = F(w_1) \subset F_2 = F_1(w_2) \subset \dots \subset F_k = F_{k-1}(w_k)$ where $w_1^{r_1} \in F$, $w_2^{r_2} \in F_1, \dots, w_k^{r_k} \in F_{k-1}$ and $K \subset F_k$. Certainly F_k can be assumed to be a normal extension of F, F_k is a normal extension of any intermediate field, or F_k is a normal extension of each F_i. By Lemma 7, each F_i is a normal extension of F_{i-1}, now since F_k is normal over F_{i-1}, by the Fundamental Theorem, $G(F_k,F_i)$ is a normal subgroup of $G(F_k,F_{i-1})$. Consider:

$(e) \subset G(F_k,F_{k-1}) \subset \dots \subset G(F_k,F_2) \subset G(F_k,F_1) \subset G(F_k,F)$. Then:

$G(F_i,F_{i-1}) \cong \dfrac{G(F_k,F_{i-1})}{G(F_k,F_i)}$. By Lemma 7, $G(F_i,F_{i-1})$ is an abelian group, hence $\dfrac{G(F_k,F_{i-1})}{G(F_k,F_i)}$ is abelian. Hence $G(F_k,F)$ is solvable.

Now $K \subset F_k$ and since K is a splitting field, K is normal over F. By the fundamental theorem, $G(F_k,K)$ is a normal subgroup of $G(F_k,F)$ and $G(K,F) \cong \dfrac{G(F_k,F)}{G(F_k,K)}$. By the corollary to Lemma 5, the homomorphic image of a solvable group is solvable. $G(K,F)$ is then a solvable group.

Hence if $p(x)$ is solvable by radicals, the Galois group is a solvable group. And equivalently, if the Galois group is not a solvable group, then $p(x)$ is not solvable by radicals. The latter form is the one used in proving Abel' Theorem. The preceeding theorem directly relates the solvability by radicals of $p(x)$ to the solvability of the Galois group.

<u>Theorem 15:</u> The general polynomial of degree $n \geq 5$ is not solvable by radicals.

Proof: The general polynomial of degree n can be considered as the particular polynomial over the field of rational functions of the roots. By Theorem 13, the Galois group of the polynomial is S_n. By Theorem 12, S_n is not solvable for $n \geq 5$. Hence the general polynomial of degree $n \geq 5$ is not solvable by radicals.

ACKNOWLEDGMENT

The author wishes to express her sincere thanks and appreciation to Dr. Charles Koch for his helpful suggestions and assistance with the preparation of this report.

REFERENCES

Artin, Emil.
Galois Theory. Notre Dame Mathematical Lectures. Number 2, Second Edition. Notre Dame, Indiana, 1944.

Birkoff and Maclane.
A Survey of Modern Algebra. New York, The Macmillan Company, Revised Edition 1953.

Herstein, I. N.
Topics in Algebra. New York, Blaisdell Publishing Company, Second Printing, 1964.

Lieber, Lillian R.
Galois and the Theory of Groups. The Science Press Printing Company, New York, 1932.

Miller, Kenneth S.
Elements of Modern Abstract Algebra. New York, Harper and Row, 1958.

Benner, Newhouse, Rader, Yates.
Topics in Modern Algebra. Harper and Brothers, New York, 1962.

GALOIS THEORY

by

CLARA DOROTHY SCHIEFERECKE

B. S., Marymount College, 1964

AN ABSTRACT OF A MASTER'S REPORT

submitted in partial fulfillment of the

requirements for the degree

MASTER OF SCIENCE

Department of Mathematics

KANSAS STATE UNIVERSITY
Manhattan, Kansas

1966

The purpose of this report is a study of Galois' application of group theory to the general solution of polynomial equations culminating in the proof that general polynomial equations of degree greater than four are not solvable by radicals.

Basic properties of fields, vector spaces, and extension fields are introduced first. Some properties of polynomial equations are taken into consideration. The Kronecker Theorem insures that for every irreducible polynomial over a field, there exists an extension field in which this polynomial has a root. A direct application of this theorem is the existence and structure of the root field of a polynomial. Automorphisms of such a field are considered. These automorphisms give meaning to the Galois group of a polynomial. The fundamental theorem of Galois theory gives the relation between the structure of a splitting field and its group of automorphisms. This theorem and some definitions and theorems concerning solvable groups contribute further to the basic theory needed to determine necessary conditions for the solvability of a polynomial equation by radicals.

One of the main objectives of Galois theory is to determine the solvability of a polynomial equation. Possibly the most important case of this is the proof that the general polynomial equation of degree greater than four is not solvable by radicals.