GALOIS THEORY

BY

H. K. HUANG

B. S., NATIONAL TAIWAN UNIVERSITY
TAIPEI, TAIWAN, CHINA, 1961

A MASTER'S REPORT

submitted in partial fulfillment of the

requirement for the degree

MASTER OF SCIENCE

Department of Mathematics

KANSAS STATE UNIVERSITY
Manhattan, Kansas

1963

Approved by :

A. L. Yates

Major Professor

TABLE OF CONTENTS

INTRODUCTION

It is common knowledge that one of the important function of mathematics is to solve equation. A polynomial equation of the first degree $ax + b = 0$ can be solved. The solution here is $x = -b/a$. A polynomial equation of the second degree $ax^2 + bx + c = 0$ also can be solved and the solution is $x = (-b \pm \sqrt{b^2 - 4ac})/2a$. As the degree increases, however, the solution becomes rapidly more difficult, and it is well-known that mathematicians cannot solve by radicals polynomial equations of degree higher than four.[1] Galois (1811-1832), however, showed that an equation is solvable by radicals if and only if its group, for a field containing its coefficients, is a solvable group. That is to say, one can determine whether it is possible or impossible to solve a high order equation by radicals by applying the theory of groups. However, it is important to make clear at this point just what is meant by possible or impossible. Whether a problem can or cannot be solved depends upon the conditions imposed upon the solution. Thus, $x + 2 = 3$ can be solved if positive integers are permitted. On the contrary, it cannot be solved if

1. Including addition, subtraction, multiplication and division.

only negative integers are permitted. A polynomial may be reducible or irreducible depending upon the field in which the factoring is to be done. Thus, $x^2 - 2$ is irreducible in the field of rational numbers but reducible in the field of irrational numbers. Hence it would be absurd to say whether a polynomial is reducible or irreducible without specifying the field.

To use the relationship between roots and the coefficients of an equation to solve the equation itself is a common method for solving an equation. For instance, having given a quadratic equation, say $x^2 + bx + c = 0$, then by the theory of equations, $x_1 + x_2 = -b$ and $x_1x_2 = c$, where x_1 and x_2 are two roots of the quadratic equation. If this pair of equations is solved for x_1 and x_2, then one quickly discovers that this method does not work because one is only led back to the original equation. However, if it were possible to obtain a pair of equations both of which were linear, then one could find the values of x_1 and x_2 from them. The same argument also holds for equations of higher degree.

These are the ideas upon which Galois based his solution of an equation by the theory of groups. The development of his theory and its application to the solution of an equation will be discussed in the following sections.

GROUPS

Definition. A group G is a set of elements with a binary operation o which satisfies the following postulates:

Postulate 1. o is closed on the set.

Postulate 2. o is associative on the set.

Postulate 3. There exists an identity element in the set for the operation o.

Postulate 4. For every element in the set there exists in the set an inverse with respect to o.

For example, the set of four elements $S = \{1,-1,i,-i\}$ under multiplication forms a group. Multiplication is closed on the set because the product of any two elements in S is again in S. Multiplication is associative on the complex number system. 1 is the identity element under multiplication. 1 is its own inverse and so is -1; i is the inverse of -i and -i is the inverse of i. Thus this set of elements satisfies all the four postulates and hence it forms a group.

Definition. If the set of elements which constitutes G is finite, then G is called a finite group.

For example, the set $S = \{1,-1,i,-i\}$ forms a finite group under multiplication because the set S is a finite set.

Definition. An Abelian group is a group with the additional postulate:

Postulate 5. o is commutative on the set.

Again, the set $S = \{1,-1,i,-i\}$ is an Abelian group because multiplication is commutative on the complex number system.

Definition. The order of a finite group G is the number of elements in G.

Definition. A subset S of a group G is called a subgroup of G if S itself is a group with respect to the binary operation of G.

In any group G the set consisting of the identity e alone is a subgroup of G. The whole group G is also a subgroup of G itself. Both of these are called improper subgroups.

Theorem 1. The order of a finite group G is a multiple of the order of every one of its subgroups.[1]

Definition. The order of an element a of a finite group is the least postive integer m such that $a^m = e$, where e is the identity of the finite group.

Theorem. 2 The order of a finite group G is a multiple of the order of any of the elements of G.

Proof; The proof is obvious by using the preceding theorem and definition.

1. For a proof, refer to p.94 in Benner, Newhouse, Rader Yates: Topics In Modern Algebra.

Definition. A cyclic group is one which contains a particular element, called the generator of thegroup, such that the order of this element is equal to the order of the group.

Theorem 3. There exists a cyclic group for any order.

Proof: Let n be any arbitrary positive integer. The group made up of the elements $b, b^2, \ldots, b^{n-1}, b^n = e$ under multiplication is a cyclic group of order n. This proves the theorem.

Definition. Let G and H be two sets of elements each with a particular operation. If the mapping $G \to H$ has the property that for $g_1, g_2 \in G$ and $h_1, h_2 \in H$, $g_1 \to h_1, g_2 \to h_2$ implies $g_1 g_2 \to h_1 h_2^1$, then the mapping is a homomorphism.

Definition. Let G and H be two sets of elements each with a particular operation. If the mapping $G \to H$ is one-to-one, and if for $g_1, g_2 \in G$, $h_1, h_2 \in H$, $g_1 \to h_1$ and $g_2 \to h_2$ implies $g_1 g_2 \to h_1 h_2$, then the mapping is an isomorphism.

Definition. If the two systems in the preceding definition are the same system, then the mapping is an automorphism.

Theorem 4. Two cyclic groups of the same order are isomorphic.

Proof: Let the two cyclic groups be G_1 and G_2. Let a be a generator of G_1 and b be a generator of G_2; also let $a^i \to b^i$ and $a^j \to b^j$. Since G_1 and G_2 have the same order, this is a one-to-one correspondence between G_1 and G_2

1. From now on, juxtaposition will be used instead

of operation 0.

$a^i \rightarrow b^i$ and $a^j \rightarrow b^j$. Since G_1 and G_2 have the same order, this is a one-to-one correspondence between G_1 and G_2. Then since $a^i a^j = a^{i+j}$ and $b^i b^j = b^{i+j}$, $a^{i+j} \leftrightarrow b^{i+j}$. Thus G_1 and G_2 are isomorphic.

Definition. If all properties of the elements of a group are abstracted except those of its multiplication table, then this group so formed is an abstracted group.

Theorem.5. If p is a prime, the cyclic group is the only abstract group of order p.

Proof: If G is of order p, then it contains an element b which differs from e. Since p is a prime, it follows from Theorem 2 that the order of b is p; hence G is cyclic. Since two cyclic groups of the same order are isomorphic, the cyclic group is the only abstract group of order p.

Definition. A permutation group on a set of symbols is a group with permutations on a given (finite) set of symbols as its elements and multiplication of permutations as its operation.

For example, the set of permutations $\{1, (ab)(cd), (ac)(bd), (ad)(bc)\}$ forms a permutation group.

Let P be the set of all permutations on n letters. If there exists a maximum subset of P such that when all the elements of this subset are applied to a function

individually and if the value of this function remains unaltered, then this subset of P forms a group.[1] It is said to be the group under which the function is invariant. As an illustration, if one applies the permutations 1 and (ab) to the function a + b individually, then the value of this function remains unchanged. Thus $\{1, (ab)\}$ forms a group.

Definition. The total set of permutations on n letters $b_1, b_2, \ldots, b_n$ contains n! permutations. This set of elements forms a group of order n!/2. which is a symmetric group.

Definition. The total set of even permutations on n letters $b_1, b_2, \ldots, b_n$ forms a group of order n!/2. This group is an alternating group.

Definition. A transitive group is a permutation group with the additional property that it contains a permutation which replaces any given one of its elements by any other given one.

The group consisting of the permutations 1, (ab)(cd), (ac)(bd), (ad)(bc) is a transitive group because these elements in order replace a by a,b,c,d, b by b,a,d,c and so on. The following five definitions play an important role in dealing with the solution of equations by using Galois theory, as one will see later.

1. For a proof, refer to p. 21 in Carmichael: Introduction to the Theory of Groups of Finite order.

Definition. A transform of an element b is $a^{-1}ba$, where $a,b \in G$.

Definition. A group T is a normal subgroup of G if it remains unchanged when all of its elements are transformed by all the elements of G.

Definition. For $H \subseteq G$ and fixed $x \in G$, $\{hx \mid h \in H\}$ is a left coset of H, denoted by Hx, and $\{xh \mid h \in H\}$ is a right coset of H denoted by xH.

Definition. If G is a group and T is a normal subgroup of G, then the set H containing all distinct xT, for all $x \in G$, is the factor group of G with respect to T, designated by H=G/T.

Definition. Let G be a group. If it contains a sequence of subgroups $G = G_0 \supset G_1 \supset G_2 \supset \ldots \supset G_s = 1$, each a normal subgroup of the preceding, and with G_{i-1}/G_i Abelian, then G is a solvable group.

Theorem 6. A homomorphic image of a solvable group is solvable.

Proof: Let G be a solvable group; i.e., $G \supset G_1 \supset G_2 \supset \ldots \supset G_s = 1$, each a normal subgroup of the preceding and with G_{i-1}/G_i Abelian. Let T be a homomorphism of the group G on the group G'. Hence there exist G_i' such that T is a homomorphism of G_i on G_i', where G_i are normal subgroups of G, and G_i' are normal subgroups of G', and $G' \supset G_1' \supset G_2' \supset \ldots \supset G_s' = 1$. However, G_{i-1}/G_i is isomorphic to G_{i-1}'/G_i'[1]. This implies that G_{i-1}'/G_i' is Abelian. Therefore G' is solvable.

1. For a proof, refer to p. 28 in Hall: The Theory of Groups.

Definition. If p = (123...n) denotes a permutation on k letters $b_1, b_2, \ldots, b_k$, and if (123...n) has n letters ($k \geq n$), then p is an n-cycle.

Theorem 7. If G is a symmetric group on n letters ($n > 4$), if H is a subgroup of G containing every 3-cycle, and if H_1 is a normal subgroup of H such that H/H_1 is Abelian, then H_1 contains every 3-cycle.

Proof: Let x = (ijk) and y = (krs) be two elements of H, where i,j,k,r and s are five distinct letters. Let $H \to H/H_1$ be a homomorphism. If $x \to x'$, $y \to y'$, where x',y' are two elements of H/H_1, then $x^{-1}y^{-1}xy \to x'^{-1}y'^{-1}x'y' = 1$. ($H/H_1$ is Abelian). Hence $x^{-1}y^{-1}xy \in H_1$. However, $x^{-1}y^{-1}xy = (kji)(srk)(ijk)(krs) = (ikr)$. Therefore, for each i,k,r, the 3-cycle $(ikr) \in H_1$.

Theorem 8. The symmetric group G on n letters is not solvable for $n > 4$.

Proof: Suppose the symmetric group G is solvable. Then by definition there exists an expression $G = G_0 \supset G_1 \supset G_2 \supset \cdots \supset G_r = 1$ such that each G_i is a normal subgroup of the preceding one, and G_{i-1}/G_i is Abelian. As one can observe from the preceding theorem, G contains every 3-cycle. Since G_r is a normal subgroup of G, G_r contains a 3-cycle. Hence $G_r \neq 1$. This contradicts the fact that G is a solvable group.

FIELD THEORY

Definition. A field F is a set of elements with two closed operations ① and ② which satisfies the following postulates:

Postulate 1. ① and ② are both commutative.

Postulate 2. ① and ② are both associative.

Postulate 3. The set contains an identity element e_0 for ① and an identity element e_1 for ②.

Postulate 4. Every element has an inverse with respect to ① and ② except e_0, which does not have an inverse with respect to ②.

Postulate 5. ② is distributive with respect to ①.

If E and F are two fields with the same operations, and if every element in F is also in E, then F is called a subfield of E, and E is called an extension of F. This is designated by $F \subset E$. Suppose E' is the additive group of the field E and F is a field. If for each $A \in E'$ and $a \in F$, one defines a particular operation o which is the same as operation ② defined above such that $A \circ a$ is again an element in E', then E can be considered as a vector space over F. This is because all the vector space postulates are satisfied by the properties of an additive Abelian group and this particular operation. Hence one can consider the degree of E over F, denoted as (E/F), as the dimension of the vector space of E over F. In case this value is finite, E is a a finite extension of F.

Theorem 9. If F, B, E, are three finite fields such that $F \subset B \subset E$, then $(E/F) = (B/F)(E/B)$.

Proof: Let the distinct elements $w_1,\ldots,w_m$ form a basis for E over B and $u_1,\ldots,u_n$ form a basis for B over F. For any element $x \in E$, x can be represented as a linear combination of $w_1,\ldots,w_m$, i.e.;

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

One can use the same argument to show that

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

Substituting (2) into (1), one obtains

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

Suppose x = 0. Then (1) implies that all $r_j = 0$, $j = 1,\ldots,m$. If all $r_j = 0$, (2) implies that all $a_{ij} = 0$, $j = 1,\ldots,m, i = 1,\ldots,n$. It follows that the m·n elements in (3) are linearly independent with respect to F. Thus, they form an extension E of F. Since (E/F) is m·n, (B/F) is n and (E/B) is m, the statement (E/F)=(B/F)(E/B) is true.

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

Proof: One can extend the same technique used in proving the preceding theorem to show that the corollary is true.

A polynomial of degree n in F is an expression $a_0x^n + a_1x^{n-1} + \ldots + a_n$ such that all $a_i \in F$ with $a_0 \neq 0$. A polynomial P is called irreducible in F if it cannot be expressed as a product of two polynomials of degree at least one in F; otherwise P is called reducible.

Theorem 10. If $f(x)$ is an irreducible polynomial of degree n in F, then it cannot divide the product of any two polynomials $g_n(x)$ and $h(x)$ of degree less than n in F.

Proof: Let $h(x)$ be a polynomial in F of degree less than n. Suppose there exist some $g_i(x)$, $i = 1,\ldots,k$ in F of degree less than n such that $g_i(x)\cdot h(x)$ is divisible by $f(x)$. Then one can select one, say $g_1(x)$ such that the degree of $g_1(x)$ is the least among all $g_i(x)$ and form the equality $k(x)\cdot f(x) = g_1(x)\cdot h(x)$, where $k(x)$ is any polynomial that satisfies this condition. Using the Euclidean Algorithm, one obtains $f(x) = g_1(x)q(x) + r(x)$, where $r(x)$ is the remainder of degree less than $g_1(x)$. Since $f(x)$ is irreducible, $r(x) \neq 0$. Moreover,

$$h(x)f(x) = h(x)g_1(x)q(x) + h(x)r(x),$$

$$r(x)h(x) = h(x)f(x) - h(x)g_1(x)q(x) = h(x)f(x) - k(x)f(x)q(x)$$
$$= f(x)(h(x) - k(x)q(x)).$$

This implies that $r(x)h(x)$ is divisible by $f(x)$, which leads to a contradiction in selecting $g_1(x)$ as the g_i of least degree. This proves the theorem.

If F $\subset$ E, and a $\in$ E, then a is called algebraic with respect to F if there exist polynomials in F such that these polynomials in F have a as a root.

Theorem 11. If $g(x)$ is a polynomial among all the polynomials in F having a as a root such that $g(x)$ is of the least degree and the coefficient of the highest degree term of $g(x)$ is one, then $g(x)$ is unique and irreducible in F and is a divisor of all the said polynomials.

Proof: That $g(x)$ is irreducible follows directly from the choice of $g(x)$. Let $f(x)$ be a polynomial in F such that $f(a) = 0$. Applying the division algorithm, one obtains $f(x) = g(x)q(x) + r(x)$ and $f(a) = 0 = 0 + r(0) = r(0)$. The statement that $r(x)$ is of degree less than $g(x)$ but has a as its root is a contradiction to the choice of $g(x)$. Therefore, $r(x) = 0$. This shows that $f(x)$ is divisible by $g(x)$ and $g(x)$ is unique.

Theorem 12. If F is a finite field of n elements, then the fieldf all polynomials in F of degree less than n forms a field E with n^n distinct elements.

Proof: Let $f(x)$ be irreducible polynomial in F of degreen. Let the general form of the polynomials in F of degree less than n be $g_i(x) = c_0 + c_1x + c_2x^2 + \ldots + c_{n-1}x^{n-1}$. Define ① as the addition and ② as the particular multiplication such that $g_j(x)g_k(x) = g_r(x) \pmod{f(x)}$. By using a theorem in congruences modulo a polynomial that the remainder of the product of two remainders of two polynomials is the remainder of the product of these two polynomials, one observes that ② is closed. Also every $g_i(x)$ has an inverse with respect to ② except the zero polynomial because $g_i(x) \neq 0$ and $g_i(x)g_j(x) = 0$ implies that $g_j(x) = 0$. Hence, they form a field E.

Since if $g_i(x) = c_0 + c_1x + c_2x^2 + \ldots + c_{n-1}x^{n-1}$, and if F contains n distinct elements, then each of the n independent coefficients c_i may have any one of n values. This proves the existence of n^n distinct elements in E.

Theorem 13. (Kronecker) If $f(x)$ is a polynomial in a field F, there exists an extension E of F in which $f(x)$ has a root.

Proof: Case 1. If $f(x)$ has a root in F, then the theorem is proved.

Case 2. If $f(x)$ does not have a root in F, one can construct an extension E of F in which an irreducible factor of $f(x)$ has a root. The procedure is as follows:

Let $f(x) = x^n + b_{n-1}x^{n-1} + \ldots + b_o$ be irreducible in F. Let E be the set of all polynomials $g(a) = c_o + c_1a + \ldots + c_{n-1}a^{n-1}$ of degree less than n with $c_i \in F$. Define ① as addition and ② as the particular multiplication such that $g_j(a)g_l(a) = g_r(a) \pmod{f(a)}$. Then E is an additive group. Since a is a particular element of E, if one performs operation ② on a itself n times, then one will obtain a remainder of the polynomial a^n. This remainder is

(1) $\quad a^n - f(a) = -b_{n-1}a^{n-1} - b_{n-2}a^{n-2} - \ldots - b_o$

On the other hand, instead of computing a^n and then reducing it to an element in E, one can compute this remainder using operations ① and ② with respect in E avoiding the appearance of the a^n power. This remainder, however, must again be equal to a^n, i.e.;

(2) $\quad a^n = -b_{n-1}a^{n-1} - b_{n-2}a^{n-2} - \ldots - b_o$.

Equating (1) and (2) yields $f(a) = 0$ in E. Hence contains F as subfield and a satisfies the equation $f(a) = 0$.

Let $h(a) = \sum_{i=0}^{n-1} b_i a^i$ and $g(a) \neq 0$ be two elements

in E. Then there exists an element $X(a) = \sum x_i a^i \in E$ such that $g(a)X(a) = h(a)$. Computing the left hand product, one obtains an expression $L_0 + L_1 a + \ldots + L_{n-1} a^{n-1}$, where L_i is a linear combination of x_i with coefficients in F. Hence $L_i = b_i, i = 0,1,\ldots,n-1$. This set of simultaneous linear equations has a solution if and only if the rank of the augmented matrix is equal to the rank of the coefficient matrix. This is equivalent to saying that $L_i = b_i$ has a solution if the corresponding set of homogeneous equations $L_i = 0$, $i = 0,1,\ldots,n-1$ has only the trivial solution.[1] The homogeneous case would occur if $X(a)$ satisfies the condition $g(a)X(a) = 0$. This implires that $g(a)X(a)$ is divisible by $f(a)$. According to Theorem 10, this is only possible for $X(a) = 0$. Hence E is a field.

Definition. If F, B and E are three fields having the relation that $F \subset B \subset E$, then B is an intermediate field.

Definition. A splitting (root) field E is an extension of a field F with the property that $f(x)$ (a polynomial in F) can be decomposed into linear factors in E but but cannot be so factored in any intermediate field.

1. Refer to pp 45-47 in Perlis : Theory of Matrices.

Theorem 14. There exists a root field E of $f(x)$, where $f(x)$ is a polynomial in a field F.

Proof: Case 1. If $f(x)$ can be factored into linear factors in F, then F is a root field of $f(x)$.

Case 2. If $f(x)$ cannot be factored into linear factors in F, then one can express $f(x) = f_1(x)f_2(x) \ldots f_r(x)$, where $f_1(x),\ldots,f_r(x)$ are irreducible non-linear factors of $f(x)$ in F. It is true that there exists an extension E_1 of F in which $f_1(x),\ldots,f_r(x)$ into irreducible factors in E_1 and proceed as before. Since the degree of $f(x)$ is finite, one will finally arrive at a field such that $f(x)$ can be decomposed into linear factors.

Theorem 15. A polynomial $f(x)$ in F can be decomposed into unique factors belonging to and irreducible in F in just one way.

Proof: Let $f(x) = p_1(x)\cdot p_2(x)\ldots p_r(x) = q_1(x)\cdot q_2(x)\ldots q_s(x)$, where the leading coefficients of $p_i(x)$ and $q_i(x)$ are one. Let F(a) be an extension of F in which $p_1(a) = 0$. Then $f(a) = 0 = p_1(a)\ldots p_r(a) = q_1(a)\ldots q_s(a)$. This implies that there must be one factor $q_i(a)$, say $q_1(a)$, which equals zero. Hence $p_1(x) = q_1(x)$ (Theorem 11); i.e.,

$p_1(x)(p_2(x)\ldots p_r(x) - q_2(x)\ldots q_s(x)) = 0$,

$p_2(x)\ldots p_r(x) = q_2(x)\ldots q_s(x)$.

If one repeats this procedure r times, one obtains $p_i(x) = q_i(x)$, $i = 1,2,\ldots,r$. Using the fact that a polynomial equation of degree n can have only n roots, it follows that $r = s$.

Definition. Let $S = \{T_1, T_2, \ldots, T_n\}$ be a set of isomorphisms of a field E onto a field E'. Then an element a of E with the property that $T_1(a) = T_2(a) = \ldots T_n(a)$ is a fixed point of E under $T_1, T_2, \ldots, T_n$.

In case S is a set of automorphisms, and T_1 is the identity, one obtains $T_1(x) = x$. If x is a fixed point, then $T_i(x) = x$, $i = 1,2,\ldots,n$.

Theorem 16. The set of all fixed points of E forms a fixed (invariant) field which is a subfield of E.

Proof: Let a and b be two fixed points $\in$ E. Then $T_i(a + b) = T_i(a) + T_i(b) = T_j(a) + T_j(b) = T_j(a + b)$, $T_i(a \cdot b) = T_i(a) \cdot T_i(b) = T_j(a) \cdot T_j(b) = T_j(a \cdot b)$, $(T_i(a))^{-1} = (T_j(a))^{-1} = T_i(a^{-1}) = T_j(a^{-1})$ and $-T_i(a) = T_i(-a)$ etc. Hence, this set forms a field. Since every element in this set is also an element in E, this field is a subfield of E.

Theorem 17. If $T_1, \ldots, T_n$ are n mutually distinct isomorphisms of a field E onto a field E', and if F is the fixed field of E, then $(E/F) \geq n$.

Proof: Let $(E/F) = r < n$. Let $w_1, \ldots, w_r$ be a set of generators of E over F. Consider the set of homogeneous linear equations.

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

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

$\ldots \qquad\qquad \ldots$

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

Since $r < n$, this set of homogeneous linear equations has more unknowns than equations. It follows that there exists a non-trivial solution $x_1,\ldots,x_n$. Multiply (1) by $T_1(a_1)$,..., (r) by $T_1(a_r)$, where $a_i \in F$, $i = 1,\ldots,r$. Since $T_1(a_i) = \ldots = T_n(a_i)$ and $T_1(a_i)\cdot T_1(w_i) = T_1(a_i w_i)$,

$T_1(a_1w_1)x_1 + \ldots + T_n(a_1w_1)x_n = 0$

$\ldots \qquad\qquad \ldots$

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

For any $c \in E$, it is true that

$c = a_1w_1 + \ldots + a_rw_r$, where $a_i \in F$, $i = 1,2,\ldots,r$. Thus, $T_1(c)x_1 + T_2(c)x_2 + \ldots + T_n(c)x_n = 0$. Since not all $x_i = 0$, $i = 1,2,\ldots,n$, $T_i(c)$, $i = 1,2,\ldots,n$ are not mutually distinct. This contradiction arises from $r < n$. Therefore, $(E/F) \geq n$.

Corollary. If $T_1,T_2,\ldots,T_n$ are distinct automorphisms of the field E, and F is the fixed field, then $(E/F) \geq n$.

Theorem 18. If E is an extension field of F, the set G of all automorphisms which leave F fixed is a group G.

Proof: Let $T_1,\ldots,T_n$ be the set G. Since $T_1(T_2(a)) = a = T_1T_2(a) = T_3(a)$, $T_1^{-1}(a) = T_1^{-1}(T_1(a)) = T_1T_1^{-1}(a) = a$, the

set forms a group

It is necessary to point out the fact that the group G does not need to have F as its fixed field, since G may also leave invariant some elements $b \in E$, but $b \notin F$. Hence, the dimension of the fixed field of G over E may be larger than the dimension of F over E.

Definition. If E is a finite extension of F, and if the group of automorphisms of E which leave F invariant has F for its invariant field, then E is a normal extension.

Theorem 19. If E is a normal extension of F, then $(E/F) = n$.

Proof: Let $T_i \in G$ for $i = 1,\ldots,n$. Let $(E/F) > n$. Then there exist $n + 1$ independent elements $b_i \in E$, $i = 1,\ldots,n+1$ with respect to F. The system of homogeneous equations

$$\begin{aligned} &x_1T_1(b_1) + \ldots + x_{n+1}T_1(b_{n+1}) = 0 \\ (1)\quad &x_1T_2(b_1) + \ldots + x_{n+1}T_2(b_{n+1}) = 0 \\ &\cdots \qquad\qquad \cdots \\ &x_1T_n(b_1) + \ldots + x_{n+1}T_n(b_{n+1}) = 0 \end{aligned}$$

has a non-trivial solution in E. If this non-trivial solution is in F, then the first equation of (1) leads to a dependence among the elements $b_1,\ldots,b_{n+1}$, which violates the assumption.

Let $a_1,\ldots,a_{r-1},1,0,\ldots,0$, where $a_i \neq 0$, $i = 1,\ldots,r-1$, be a particular non-trivial solution with the least number of elements different from zero. It is true that $r \neq 1$. Since $T_1(b_1) = b_1 \neq 0$, $a_1T_1(b_1) = 0$ would imply $a_1 = 0$. Thus, one obtains

$$a_1T_1(b_1) + \dots + a_{r-1}T_1(b_{r-1}) + T_1(b_r) = 0$$

(2) $\cdots \qquad \cdots$

$$a_1T_n(b_1) + \dots + a_{r-1}T_n(b_{r-1}) + T_n(b_r) = 0.$$

Suppose $a_1 \in E$ but $a_1 \notin F$. This implies that there exists a $T_k \in G$ such that $T_k(a_1) \neq a_1$. Multiplying (2) by T_k, one obtains

$$T_k(a_1T_1(b_1)) + T_k(a_2T_1(b_2)) + \dots + T_k(a_{r-1}T_1(b_{r-1})) + T_k(T_1(b_r)) = 0$$

(2') $\cdots \qquad \cdots$

$$T_k(a_1T_n(b_1)) + T_k(a_2T_n(b_2)) + \dots + T_k(a_{r-1}T_n(b_{r-1})) + T_k(T_n(b_r)) = 0.$$

$$T_k(a_1)T_kT_1(b_1) + \dots + T_k(a_{r-1})T_kT_1(b_{r-1}) + T_kT_1(b_r) = 0$$

(3) $\cdots \qquad \cdots$

$$T_k(a_1)T_kT_n(b_1) + \dots + T_k(a_{r-1})\,T_kT_n(b_{r-1}) + T_kT_n(b_r) = 0.$$

Since $T_kT_j = T_i$, $1 \leq i,j,k \leq n$, $n = 1,\dots,n$, if one makes some suitable rearrangement of the order of the equations in (3) and performs (2)-(3), one obtains

$$(a_1 - T_k(a_1))T_1(b_1) + \dots + (a_{r-1} - T_k(a_{r-1}))T_1(b_{r-1}) = 0$$

(4) $\cdots \qquad \cdots$

$$(a_1 - T_k(a_1))T_n(b_1) + \dots + (a_{r-1} - T_k(a_{r-1}))T_n(b_{r-1}) = 0,$$

which is also a non-trivial solution of (1). The fact that this solution has fewer than r elements different from zero leads to a contradiction in the choosing of r. This proves the theorem.

Corollary. If E is a normal extension of F, then every automorphism that leaves F fixed belonge to G.

Proof: It is true that (E/F) = order of G = n. Let T_{n+1} be an automorphism that leaves F fixed but not in G. Then F would remain fixed for all T_i, i = 1,...,n+1. This implies that (E/F) $\geq$ n + 1.(Corollary to Theorem 17). But the last statement is a contradiction to (E/F) = n. Thus, T_{n+1} must be in G.

Corollary. No two distinct finite groups G_1 and G_2 have the same fixed field.

Definition. A polynomial $f(x)$ of degree n is separable over a field F if it has n distinct roots in its root (splitting) field E; otherwise $f(x)$ is inseparable. E is called a separable extension of F.

Let $f(x) = a_0 + a_1x + \ldots + a_nx^n$ be a given polynomial of degree n. The polynomial $f'(x) = a_1 + (2a_2)x + \ldots + (na_n)x^{n-1}$ is defined as the formal derivative $f'(x)$ of $f(x)$. If the coefficients of $f(x)$ are in the field of real numbers, this formal derivative is the same as the ordinary derivative in cauculus.

Theorem 20. A polynomial $f(x)$ is separable when factored over E if and only if $f(x)$ and $f'(x)$ are relatively prime.

Proof: Factoring $f(x)$ into powers of distinct linear factors over any root field, one obtains

(1) $\quad f(x) = a_n(x-u_1)^{e_1} \cdot \ldots \cdot (x-u_k)^{e_k} \quad . \quad (a_n \neq 0)$

The formal derivative of (1) would be an expression which is the sum of $(k - 1)$ terms each of which contains $(x - u_1)^{e_1}$ as a factor and one term $a_n e_1(x - u_1)^{e_1-1}(x - u_2)^{e_2}\ldots(x - u_k)^{e_k}$. If $f(x)$ is separable, then $e_1 = e_2 = \ldots = e_k = 1$. Hence, $(f(x),f'(x)) = 1$. If $(f(x),f'(x)) = 1$, then $f(x)$ and $f(x)$ have no factor in common except 1. This implies that $e_1 = 1$; otherwise $f(x)$ and $f'(x)$ would have a factor $(x - u_1)$ in common. The same argument can be used to prove to prove $e_2 = e_3 = \ldots = e_k = 1$. Thus, $f(x) = a_n(x - u_1)\ldots(x - u_k)$.

Definition. If $E = F(u_1,\ldots,u_n)$ is the root field of a polynomial $f(x) = (x - u_1)\ldots(x - u_n)$, then the group G of the automorphisms of E over F is (1) the Galois group or (2) the group of the equation $f(x) = 0$ or (3) the Galois group of the field E over F.

Theorem 21. B is a normal extension of F if and only if the number of automorphism of B is (B/F).

Proof: If B is a normal extension of F, the number of distinct automorphisms of B which leave F fixed is (B/F). (Theorem 19 and its corollary). Let the number of distinct automorphisms of B which leave F fixed be (B/F). Let F' be an intermediate field of all these automorphisms; i.e., $F \subset F' \subset B$. By Theorem 9 and Theorem 19, one has $(B/F') = (B/F)$, $(F'/F) = 1$ or $F = F'$. Thus, B is a normal extension of F.

Theorem 22. E is a normal extension of F if and only if E is the root field of a separable polynomial $f(x)$ in F.[1]

The following theorem which is known as the fundamental theorem of Galois theory gives the relation between the structure of a root field E of a polynomial $f(x)$ in F and its group of automorphisms G.

Theorem 23. If G is the Galois group for the root field E of a separable polynomial $f(x)$ over F, then:
(1) Each intermediate field B is the fixed field for a subgroup G_B of G, and distinct subgroups have distinct fixed fields. One says B and G_B belong to each other.

1. For a proof, refer to pp.44-46 in Artin: Galois Theory.

(2) For each intermediate field B, (E/B) is the order of G_B and (B/F) is the index of G_B in G.

Proof: (1) It is true that the root field E of f(x) in F is also the root field of f(x) in B, where B is an intermediate field. It is also true that E is a normal extension of B. Therefore, there exists a subgroup G_B of G such that G_B leaves B invariant. The same argument can be extended to prove the case when there is more than one intermediate field. Since no two distinct finite groups G_1 and G_2 have the same fixed field, this proves that distinct subgroups have distinct fixed fields.

(2) The index of G_B in G is defined as the order of G divided by the order of G_B. Since G_B has B as its fixed field, by Theorem 19 one has (E/B) = order of G_B and (E/F) = order of G. By definition, order of G = index of G_B in G times order of G_B. Since (E/F) = (B/F)(E/B), the index of G_B = (B/F).

Theorem 24. The intermediate field B is a normal extension of F if and only if the subgroup G_B is a normal subgroup of G.

Proof: Let G be a subgroup of G. Then for any two elements $T_1, T_2 \in G_B$ and any $a \in B$ it is true that $T_1(a) = a = T_2(a)$. If one lets TT_1, TT_2 be two distinct elements in TG_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 and S be two distinct isomorphisms such that T(a) = S(a) for any $a \in B$.

Then $T^{-1}S(a) = a$ or $T_3 = T^{-1}S$, where T_3 is an isomorphism in G_B. This implies that $S = TT_3$ and $SG_B = TT_3G_B = TG_B$. Hence elements of different cosets give different isomorphisms. But the index of G_B in G is equal to the number of left cosets of G_B, therefore the number of 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 automorphis, belonging to G; i.e., it maps B isomorphically into some other subfield B' of E and is the identity on F. Suppose $T \in G$ but $T \notin G_B$. Let $b \in B$, $b \notin B'$ and $T(b) = b'$. Let G_B be the group of B. Then $TG_BT^{-1}(b') = TG_BT^{-1}(T(b)) = TG_B(b) = T(b) = b'$. This implies that 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; i.e., 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;i.e., equal (B/F) if and only if G_B is a normal subgroup of G. But by Theorem 21 B is a normal extension of F if and only if the number of automorphisms of B is (B/F). This completes the proof.

Let $u_0, u_1, u_2, \ldots, u_{s-1}$ be a set of s distinct elements. If this set of elements forms an Abelian group of order s under addition and also forms an Abelian group of order s-1 under multiplication by deleting u_0, and if the distributive law

holds, that is $u_i(u_j + u_k) = u_iu_j + u_iu_k = (u_j + u_k)u_i$ for $1 \leq i,j,k \leq s-1$, then this set of elements forms a finite field of order s. In general, the elements u_o and u_1 have the properties of zero and unity respectively. If one defines $n \cdot a$ to be an element in F which is obtained by adding a to itself n times for any $a \in F$, then if there exists a positive integer p such that $p \cdot a = 0$, and if p is the least positve integer with this property, then p is called the characteristic of the field.

Theorem 25. The characteristic p of a field is a prime number.

Proof: Let $p = r \cdot s$, $r \leq p$, $s < p$, and $a \neq 0$. Clearly $p \cdot a = (r \cdot s)a = r(s \cdot a) = 0$ implies that $r \nless p$, $s < p$, then $p \cdot a \neq 0$ contrary to $p \cdot a = 0$. Hence $r(s \cdot a) = 0$ implies that $r = p$, $s = 1$.

Corollary. If $na = 0$ for $a \neq 0$, then p divides n.

Proof: Let $n = qp + r$ with $0 \leq r \leq p$. Then $na = qpa + ra$, implies $0 = 0 + ra$. Hence $ra = 0$. Since $a \neq 0$, $r = 0$.

Theorem 26. The number of elements in any finite field F is a power of its characteristic.

Proof: Let v_1 be any element of the field different from u_o. Let $r_1 = 0,1,\ldots,p-1$. Then r_1v_1 gives p distinct elements of the field. If these p distinct elements exhaust the total elements of F, then the theorem is true.

If there are some elements in the field not

in the preceding set, then one can pick out one, say v_2 , and perform the same procedure. Then $r_1v_1 + r_2v_2$ $(r_1,r_2 = 0,1,\ldots,p-1)$ would give p^2 distinct elements of the field. One may continue similarly until all the elements are exhibited in the following form:

$r_1v_1 + r_2v_2 + \ldots + r_nv_n$. $(r_i = 0,1,2,\ldots,p-1,\ i = 1,2,\ldots,n.)$ However, this form gives exactly p^n distinct elements.

Theorem 27.(Fermat) Every element of a field F of order p^n satisfies the equation $x^{p^n} - x = 0$.

Proof: Let the number of elements of F be $p^n=q$. Then all the elements except u_o form a multiplication group of order q-1. The order of any element in this group is a factor of the order of the group. Hence every element in this group satisfies the equation $x^{p^n-1} = 1$, or $x^{p^n} - x = 0$. Moreover, $u_o^{p^n} - u_o = 0$. Thus all u_i, $i = 0,1,\ldots,q-1$ satisfy the equation.

Corollary. $x^q - x = (x - u_o)\ldots(x - u_{q-1})$.

Proof: Since all elements of F satisfy $x^q - x = 0$. and the order of every element in the multiplication group is a divisor of $q - 1$, $(x - u_o)\ldots(x - u_{q-1})$ is a divisor of $x^q - x$. But $(x - u_o),\ldots,(x - u_{q-1})$ are relatively prime polynomials each of which divides $x^q - x$. The polynomial obtained by performing this product is monic and of degree q. Therefore $x^q - x = (x - u_o)\ldots(x - u_{q-1}) = \prod_{i=0}^{q-1} (x - u_i)$.

Theorem 26. If the fields F(u) and F(w) are algebraic extensions of the same field F, generated respectively by roots u and w of the same polynomial f(x) irreducible over F, then F(u) and F(w) are isomorphic.

Proof: Let $f(u) = a_0 + a_1u + \dots + a_ku^k$, and

$f(w) = a_0 + a_1w + \dots + a_kw^k$, $a_i \in F, i=0,1,\dots,k$.

If one considers the correspondence $f(u) \leftrightarrow f(w)$, then it is obvious that this correspondence preserves sums and products.

Suppose $f(u) = g(u)$, then $f(u) - g(u) = 0$. It is true that an element u which is algebraic over a field F is the root of one and only one monic polynomial p(x) irreducible in the domain F(x) of all polynomial forms over F. The element u is a root of another polynomial $g_1(x)$ with coefficients in F if and only if $g_1(x)$ is a multiple of p(x) in the domain F(x).[1] Using this fact, one obtains $p(x) \mid (f(x) - g(x))$. Since w also satifies $p(x) = 0$, $f(w) = g(w)$. One can easily reverse the order of the last proof and conclude that $f(u) = g(u)$ if and only if $f(w) = g(w)$. Therefore this correspondence is one-to-one and F(u) and F(w) are isomorphic.

1. For a proof, refer to p. 396 in Birkhoff and MacLane: A Survey of Modern Algebra.

Corollary. If an isomorphism S between fields F and F" carries the coefficients of an irreducible polynomial f(x) into the corresponding coefficients of a polynomial f"(x) over F", and if F(u) and F"(u") are algebraic extensions generated respectively by roots u and u" of these polynomials, then S can be extended to an isomorphism S* of F(u) to F"(u"), in which uS* = u".

Proof: Let $f(x) = a_o + a_1x + \ldots + a_kx^k$, $a_i \in F$

$f"(x) = b_o + b_1x + \ldots + b_kx^k$, $b_i \in F"$ $\quad i=0,1,\ldots,k.$

Since $uS^* = u"$, and $a_iS^* = a_iS = b_i$, $i=0,1,\ldots,k$,

$$(a_o + a_1u + \ldots + a_ku^k)S^* = a_oS^* + (a_1S^*)u" + \ldots + (a_kS^*)(u")^k$$
$$= a_oS + (a_1S)u" + \ldots + (a_kS)(u")^k$$
$$= b_o + b_1u" + \ldots + b_ku"^k .$$

After this correspondence has been determined, one can follow the same procedure used in proving the preceding theorem to show that F(u) and F"(u") are isomorphic.

Theorem 29. If an isomorphism S of F to F" carries f(x) into a polynomial f"(x) and if $E \geq F$ and $E" \geq F"$ are, respectively, root fields of f(x) and f"(x), the isomorphism S can be extended to an isomorphism of E to E".

Proof: One can use the induction method to prove the theorem is true.

Let $n = (E/F)$. For $n = 1$, the case is trivial. Suppose it is true for all root fields E of degree less than n over some F. Since $n > 1$, there exists at least one irreducible

factor $p(x)$ of degree $d>1$ of $f(x)$ in F. Let u be a root of $p(x)$ in E, and let $p^*(x)$ be the factor of $f^*(x)$ corresponding to $p(x)$ under S. Then E^* contains a root u^* of $p^*(x)$. Using the preceding corollary, S can be extended to S^*, and the following properties hold:
$(F(u))S^* = F^*(u^*)$, $uS^* = u^*$, $p(u) = 0$, $p^*(u^*) = 0$.
Since $F(u)$ is larger than F, E is the root field of $f(x)$ over F, and E is certainly the root field of $f(x)$ over $F(u)$ with a degree $(E/F(u)) = m/d<m$.

Using the assumption just made, S^* can be extended from $F(u)$ to E^*. This proves the theorem.

Corollary. Any two root fields E and E' of a given polynomial $f(x)$ over F are isomorphic.

Proof: The proof is immediate by using the theorem.

Theorem 30. Any two finite fields with the same number of elements are isomorphic.

Proof: Let E and E' be two finite fields with the same number of elements $q = p^n$. By Theorem 27 and the preceding corollary both E and E' are the root fields of the polynomial $x^q - x$ over F^1, and hence E and E' are isomorphic.

1. At this stage, one can say that F is actually equal to J_p, the field of integers modulo p, where p is a prime number.

Corollary. For any prime p and any positive integer n there exists a finite field with $p^n = q$ distinct elements.

Theorem 31. In any finite F of $q = p$ distinct elements, the set of all non-zero elements forms a cyclic group under multiplication.

Proof: That this set is an Abelian group is obvious. Each of these elements satisfies the equation $x^{q-1} = 1$. Now $q - 1$ can be written as $q - 1 = p^n - 1 = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$, where $p_1, p_2, \ldots, p_k$ are the distinct prime factors of $p^n - 1$. Then the equation $x^{p_1^{a_1}} - 1 = 0$ has $p_1^{a_1}$ roots, and the equation $x^{p_1^{a_1-1}} - 1 = 0$ has $p_1^{a_1-1}$ roots because an equation of the form $x^d - 1 = 0$ has exactly d roots. This implies that there exist $(p_1^{a_1} - p_1^{a_1-1}) > 1$ elements of order $p_1^{a_1}$. The same argument can be used to prove that there exist elements of order $p_i^{a_i}$, $i = 2, \ldots, k$. Since $p_1, p_2, \ldots, p_k$ are distinct prime factors of $p^n - 1$, there exists at least one element, say c, which is of order $p_1^{a_1} \cdots p_k^{a_k} = p^n - 1$. This proves that c is a generator of the Abelian group.

By the preceding theorems, one can conclude that there is one and essentially only one field with p^n elements. This field is called the Galois field $GF[p^n]$ of order p^n. Hence a particular Galois field is completely determined by its order if only its abstract properties are considered.

Definition. If F is a field with p^n distinct elements, and if a, an element of F, is of order $p^n - 1$, then a is a primitive of the field.

Theorem 32. Any element u of a finite field F of order p^n satisfies an equation of the form $c_k x^k + c_{k-1}x^{k-1} + \ldots + c_1 x + c_o = 0$, where $k \leq n$ and $c_i \in F$, $i = 0,1,\ldots,k$, and $c_k \neq 0$.

Proof: Let u be any element of F. Then one can form the n + 1 distinct elements $u^0, u^1, u^2, \ldots, u^n$. Only n of these elements can be linearly independent over F. Hence these n + 1 elements are linearly dependent over F. Hence there must exist some $c_i \in F$, not all $c_i = 0$, $i = 0,1,\ldots,n$ such that the expression $\sum_{i=0}^{n} c_i u^i = 0$ holds. When $c_n \neq 0$, $n = k$. When $c_n = 0$, $k < n$. This proves the theorem.

Theorem 33. A primitive w of a finite field F of order p^n satisfies an equation of the form $x^n + c_1 x^{n-1} + \ldots + c_n = 0$, where $c_i \in F$. $i = 1,\ldots,n$.

Proof: Let w be any primitive of a finite field F. By the preceding theorem, it is true that w satisfies $\sum_{i=0}^{k} c_i x^i = 0$, where $k \leq n$ and $c_i \in F$, $i = 0,1,\ldots,k$. Hence

(1) $w^k = \sum_{i=0}^{k-1} a_i w^i$, where $a_i \in F$, $i = 0,1,\ldots,k-1$.

If one multiplies (1) by $w, w^2, \ldots, w^{p^k-1}$ individually and reduces the degree of w^k by (1), then one obtains $p^k - 1$ distinct expressions on the right hand side with respect to $w, w^2, \ldots, w^{p^k-1}$ on the left. However, w is a primitive of F and it is of order $p^n - 1$. Thus $n = k$.

APPLICATIONS

Let p be a characteristic of F, and let E be the root field of the polynomial $x^n - 1$ where $(n,p) = 1$. Then E is called the field generated from F by the adjunction of a primitive n^{th} root of unity.

Definition. If F contains a primitive n^{th} root of unity, then the root field E of a polynomial $(x^n - a_1)(x^n - a_2)\ldots(x^n - a_r)$ where $a_i \in F$ for $i = 1,2,\ldots,r$, is the Kummer Field.

Theorem 33. If E is a Kummer field, then (1) E is a normal extension of F, and (2) the Galois group of E over F is Abelian.

Proof: (1) Let p be the characteristic of F. Then $(y - 1)^p = y^p - py^{p-1} + p(p-1)/2!y^{p-1} - \ldots - 1 = y^p - 1$. Suppose n is a multiple of p; i.e., $n = qp$. Then $x^n - 1 = (x^q)^p - 1 = (x^q - 1)^p$. This implies that $x^n - 1$ cannot have more than q distinct roots. Since E is a Kummer field, F contains a primitive w, an n^{th} root of unity. Therefore $x^n - 1$ would have $1,w,w^2,\ldots,w^{n-1}$ as distinwt roots. It follows that $n \neq qp$. Given a Kummer field E, none of the factors $x^n - a_i$, $a_i \neq 0$ has repeated roots because $x^n - a_i$ and nx^{n-1} are relatively prime polynomials. Thus $\prod_{i=1}^{r} (x^n - a_i)$ is separable and hence E is a normal extension of F.

(2) Let $w_1,w_2,\ldots,w_n$ be the n distinct n^{th} roots of unity in F, and let b_1 be a root of $x^n - a_1$ in E.

Then $b_1w_1, b_1w_2, \ldots, b_1w_n$ will be the n distinct roots of $x^n - a_i$. The same argument is also valid for the other $(x^n - a_i)$ factors. Hence $E = F(b_1, b_2, \ldots, b_r)$. Let T_1 and T_2 be two automorphisms in the Galois group G. Then T_1 and T_2 would map b_i on some other root of $(x^n - a_i)$; i.e., $T_1(b_i) = w_{iT_1} \cdot b$, and $T_2(b_i) = w_{iT_2} \cdot b_i$, where w_{iT_1} and w_{iT_2} are two elements in F. Since $T_1(T_2(b_i)) = T_1(w_{iT_2}(b_i)) = w_{iT_2}T_1(b_i) = w_{iT_2}w_{iT_1}b_i = T_2(T_1(b_i))$, T_1 and T_2 are commutative over the generators of E. Thus G is Abelian.

Definition. Suppose E is an extension of F, and $B_1, B_2, \ldots, B_r = E$ are intermediate fields such that $B_i = B_{i-1}(b_i)$, where b_i is a root of an equation of the form $x^{n_i} - a_i = 0$, $a_i \in B_{i-1}$. Then E is called an extension by radicals of F.

A polynomial f(x) in F is said to be solvable by radicals if and only if its root field is in E, an extension by radicals of F.

Theorem 34. The polynomial f(x) is solvable by radicals if and only if its group is solvable.

Proof: Suppose it is true that f(x) is solvable by radicals. Let E be a normal extension of F by radicals containing the root field B of f(x). Let G be the group of E over F. Let B_i be the intermediate fields, i = 1,...,r. Then it is true that B_i is a Kummer extension of B_{i-1} for i = 2,3,...,r. Hence the group of B_i over B_{i-1} is Abelian; i.e., $G_{B_{i-1}}/G_{B_i}$

is Abelian. Since B_i is a normal extension of B_{i-1}, there exists the sequence of groups $G = G_{B_0} \supset G_{B_1} \supset \ldots \supset G_{B_r} = 1$ each a normal subgroup of the preceding. All these imply that G is solvable. Since G_B is a normal subgroup of G, G/G_B is the group of B over F or the group of the polynomial f(x). However, G/G_B is a homomorphic image of the solvable group G. Then by Theorem 6, G/G_B is solvable.

Suppose the Galois group G_f of f(x) is solvable. Let E be the root field. Then $G = G_0 \supset G_1 \supset G_2 \supset \ldots \supset G_r = 1$ is a sequence of normal groups with the groups G_{i-1}/G_i Abelian, where $i = 1,\ldots,r$. Let B_i be the fixed field corresponding to G_i. Then using Theorem 24, B_i is a normal extension over B_{i-1}. Since G_{i-1}/G_i is Abelian, B_i is a Kummer extension of B_{i-1}. This implies that B_i is the root field of a polynomial of the form $\prod_{i=1}^{s} (x^n - a_i)$. Hence it is true that B_r is an extension of B_{i-1} by radicals. Therefore E is an extension by radicals.

Let the polynomial f(x) have the form $f(x) = x^n - u_1x^{n-1} + u_2x^{n-2} - \ldots + (-1)^n u_n$, then f(x) is known as the general equation of degree n over $F(u_1,\ldots,u_n)$.

If E is the root field of $f(x)$ over $F(u_1,\ldots,u_n)$, and if $v_1,v_2,\ldots,v_n$ are the root of $f(x)$ in E, then the following expressions will hold: $u = v_1 + v_2 + \ldots + v_n$, $u_2 = v_1v_2 + v_1v_3 + \ldots + v_{n-1}v_n,\ldots$, $u_n = v_1v_2\ldots v_n$.

Theorem 35. The group of the general equation of degree n is the symmetric group on n letters.

Proof: Let $F(x_1,\ldots,x_n)$ be the field generated by the variables $x_1,\ldots,x_n$. Let $a_1,\ldots,a_n$ be a set of symmetric functions such that $a_1 = x_1 + x_2 + \ldots + x_n$, $a_2 = x_1x_2 + x_1x_3 + \ldots + x_{n-1}x_n,\ldots$ $a_n = x_1x_2\ldots x_n$. Then $(x - x_1)(x-x_2)\ldots(x - x_n)$ $= x^n - a_1x^{n-1} + \ldots + (-1)^n a_n = f^*(x)$. Let $g(a_1,a_2,\ldots,a_n)$ be a polynomial in $a_1, a_2,\ldots,a_n$. Let the v_i defined above replace the x_i. Then $g(a_1,a_2,\ldots,a_n) = g(\sum x_i, \sum x_ix_j,\ldots)$ $= g(\sum v_i, \sum v_iv_j,\ldots,) = g(u_1,u_2,\ldots,u_n)$. Hence $g(a_1,a_2,\ldots,a_n) = 0$ implies that g is identically zero.

Now consider the subfield $F(a_1,\ldots,a_n)$ of $F(x_1,\ldots,x_n)$ and the field $F(u_1,u_2,\ldots,u_n)$. For convenience sake, let (u) denote $(u_1,u_2,\ldots,u_n)$, (a) denoted $(a_1,a_2,\ldots,a_n)$ and so on. One can always set up the correspondence $f(u)/g(u) \longrightarrow f(a)/g(a)$, where $f(u)/g(u) \in F(u)$ and $f(a)/g(a) \in F(a)$. This is clearly a mapping of f(u) on all of F(a). If $f(a)/g(a) = f_1(a)/g_1(a)$, then $f(a)g_1(a) - g(a)f_1(a) = 0$. This implies that $f(u)g_1(u) - g(u)f_1(u) = 0$; i.e., $f(u)/g(u) = f_1(u)/g_1(u)$. Therefore this mapping is an isomorphism. However, this correspondence is actually the correspondence between f(x) and f*(x). By

Theorem 29, this isomorphism can be extended to an isomorphism between E and $F(x)$. This implies that the group of E over $F(u_1,u_2,\ldots,u_n)$ is isomorphic to the group of $F(x_1,x_2,\ldots,x_n)$ over $F(a_1,a_2,\ldots,a_n)$.

Since each permutation of $x_1,x_2,\ldots,x_n$ leaves $a_1,a_2,\ldots,a_n$ fixed, it induces an automorphism of $F(x_1,x_2,\ldots,x_n)$ which leaves $F(a_1,a_2,\ldots,a_n)$ fixed. On the other hand, each automorphism of $F(x_1,x_2,\ldots,x_n)$ which leaves $F(a_1,\ldots,a_n)$ fixed must permute the roots $x_1,x_2,\ldots,x_n$ of $f^*(x)$, and this automorphism is completely determined by the permutation it effects on $x_1,x_2,\ldots,x_n$. This implies that the group of $F(x_1,x_2,\ldots,x_n)$ over $F(a_1,a_2,\ldots,a_n)$ is symmetric group on n letters. Therefore, the group of E over $F(u_1,u_2,\ldots,u_n)$ is also a symmetric group.

Theorem 36. The general equation of degre greater than four is not solvable by radicals.

Proof: Since the Galois group of the general equation is the symmetric group on n letters, and since the symmetric group for $n>4$ is not solvable, the general equation of degree greater than four is not solvable.

ACKNOWLEDGMENT

The author is very grateful for the suggestions and criticisms of Dr. Richard L. Yates in the preparation of this manuscript. Dr. Yates was very generous in letting the author prepare most of the report in absentia.

REFERENCES

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

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

Carmichael, Robert D.
Introduction To The Theory of Groups of Finite Order. Boston, Ginn and Company, 1937.

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

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

Perlis, Sam.
Theory of Matrices. Cambridge, Addison-Wesley Publishing Company, Inc. 1958.

GALOIS THEORY

BY

H. K. HUANG

B. S., NATIONAL TAIWAN UNIVERSITY
TAIPEI, TAIWAN, CHINA, 1961

AN ABSTRACT FOR 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

1963

This report is a discussion of the existence of the root field of a polynomial equation by applying Galois Theory. Some basic definitions and properties of a group are introduced first. Then some particular theorems which are needed in developing Galois Field are proved. Among them, the theorems concerning the solvable group are of utmost importance because these theorems will determine whether or not an equation is solvable by radicals.

The first step in developing the Field Theory is to define what is meant by a field. Then some properties of polynomial equations are taken into consideration. The Kronecker Theorem assures that if $f(x)$ is a polynomial in a field F, then there exists an extension field E of F in which $f(x)$ has a root. This fundamental theorem contributes to the further development of the Field Theory, especially in establishing the root field of a polynomial equation. The combination of the root field of a polynomial equation and the definition of automorphisms of a field gives meaning to the Galois Group and the Galois Field which are the main idea of this report. Some more properties of Galois Fields are considered which are useful for the purpose of application.

One of the main objects of Galois Theory is to determine the solvability of a polynomial equation. A few theorems necessary for this are introduced. The theorem that the general equation of degree greater than four is not solvable by radicals, which is one of the most important results of Galois Theory, is the last theorem of this report.