SOLVABILITY OF EQUATIONS BY RADICALS

by

ROBERT WALLACE BROWN, SR.

A THESIS

submitted to

OREGON STATE COLLEGE

in partial fulfillment of
the requirements for the
degree of

MASTER OF SCIENCE

June 1952

APPROVED:

Signature redacted for privacy.

Professor of Mathematics

In Charge of Major

Signature redacted for privacy.

Head of Department of Mathematics

Signature redacted for privacy.

Chairman of School Graduate Committee

Signature redacted for privacy.

Dean of Graduate School

Date thesis is presented April 25, 1952

Typed by Doris Brown

TABLE OF CONTENTS

ACKNOWLEDGEMENT

The author wishes to express his gratitude to Dr. A. R. Poole for his guidance and patience during the preparation of this thesis.

SOLVABILITY OF EQUATIONS BY RADICALS

INTRODUCTION

It is well known that an algebraic equation of degree 2, 3, or 4 is solvable in terms of radicals of numbers which lie in its coefficient field, while, in general, equations of degree $n > 4$ cannot be so solved. By employing the ideas of groups of substitutions and adjunctions to fields it is possible to prove the above statement as well as to consider the solvability by radicals of any algebraic equation, whether its coefficients are constants or depend on one or more variables. This is what is known as the Galois Theory of Equations.

The theory is simplified to some extent by the more modern approach of considering groups of automorphisms on the roots instead of the substitution groups. That the two groups are isomorphic is proved by Albert (1, pp.183-184). It is this approach by means of automorphism groups that MacDuffee uses (3, pp.100-112), and the purpose here is to attempt to clarify some of the points on which MacDuffee is a little vague.

Some of the results used in this section are given without proof since they are discussed in full by such authors as Albert (1, pp.146-165), Dickson (2, pp.150-163), MacDuffee (3, pp.91-99), and others.

Throughout this thesis F is used to denote a field which is a subfield of the complex field. Let $p(x) = 0$ be a polynomial equation of degree n with coefficients in F. It follows from the Fundamental Theorem of Algebra that $p(x) = 0$ has exactly n roots, which are in general not in F. A root ρ of $p(x) = 0$ which is not in F is said to be algebraic relative to F.

Let $p(x)$ be irreducible in its coefficient field F and let ρ be a root of the equation $p(x) = 0$. Let $g(x)$ be a polynomial function of x.

THEOREM 1. If $g(\rho) = 0$, then $p(x) \mid g(x)$ (3, p.91).

It follows immediately that the irreducible equation $p(x) = 0$ satisfied by ρ is unique, and that the number ρ satisfies no equation of degree $< n$.

THEOREM 2. The set of all rational functions of ρ with coefficients in F form a field $F(\rho)$, called the stem field of $p(x) = 0$ (3, p.92).

This process of obtaining $F(\rho)$ is called the adjunction of ρ to F.

THEOREM 3. The numbers of $F(\rho)$ are uniquely expressible in the form

$$\alpha = a_0 + a_1 \rho + a_2 \rho^2 + \dots + a_{n-1} \rho^{n-1}$$

where the a's are in F(3, p.92).

The roots $\rho, \rho', \rho'', \dots, \rho^{(n-1)}$ of $p(x) = 0$ are called the conjugates of ρ. Each of the conjugates $\rho^{(i)}$ determines a field $F(\rho^{(i)})$. The fields $F(\rho)$, $F(\rho')$, ..., $F(\rho^{(n-1)})$ are called a set of conjugate fields, and they are all isomorphic. They may all be distinct, or they may all be equal, or they may fall into sets of equal fields. If they are all equal, the field $F(\rho)$ is called normal.

The numbers

$$\begin{aligned} \alpha &= a_0 + a_1\rho + a_2\rho^2 + \ldots + a_{n-1}\rho^{n-1}, \\ \alpha' &= a_0 + a_1\rho' + a_2\rho'^2 + \ldots + a_{n-1}\rho'^{n-1}, \\ \alpha'' &= a_0 + a_1\rho'' + a_2\rho''^2 + \ldots + a_{n-1}\rho''^{n-1}, \\ &\cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot , \end{aligned}$$

are called the conjugates of α. The number $\alpha^{(i)}$ lies in the field $F(\rho^{(i)})$, and the number $\alpha^{(j)}$ lies in the field $F(\rho^{(j)})$, so that, in general, the conjugates of α lie in different fields.

THEOREM 4. Every number α of $F(\rho)$ satisfies an equation $f(x)=0$ of degree n with coefficients in F, whose n roots are the n conjugates of α (3, p.93).

This equation

$$\begin{aligned} f(x) &= (x-\alpha)(x-\alpha')\ldots(x-\alpha^{(n-1)}) \\ &= x^n + f_{n-1}x^{n-1} + \ldots + f_0 = 0 \end{aligned}$$

is called the principal equation of α.

THEOREM 5. The n conjugates α, α', ..., $\alpha^{(n-1)}$ are either all distinct or else they fall into h systems, each system containing k equal numbers. In the first case, f(x) is irreducible; in the second case, f(x) is the kth power of an irreducible polynomial of degree h (3, p.94).

If the principal equation $f(x)=0$ is irreducible, α is called a primitive number of $F(\rho)$.

THEOREM 6. If ω is a primitive number of $F(\rho)$, then $F(\omega)=F(\rho)$ (3, p.95).

THEOREM 7. Every imprimitive number of $F(\rho)$ defines a subfield of $F(\rho)$ (3, p.96).

The root field of $p(x) = 0$ is defined to be the field $R = F(\rho, \rho', \ldots, \rho^{(n-1)})$, obtained by adjoining to F all the roots of $p(x) = 0$. That the order of adjunction is immaterial follows from Theorem 8.

THEOREM 8. If ρ_1 and ρ_2 are two numbers algebraic relative to F, the adjunction of ρ_2 to $F(\rho_1)$ gives the same field $F(\rho_1, \rho_2)$ as the adjunction of ρ_1 to $F(\rho_2)$. There exists a single number ρ, algebraic relative to F, such that $F(\rho_1, \rho_2) = F(\rho)$ (3, p.96).

Thus the root field of $p(x) = 0$ is the stem field of at least one number ω. An irreducible equation satisfied by such a number ω is called a resolvent of $p(x) = 0$.

An equation $p(x) = 0$ without a multiple root is called separable. Evidently this is a weaker condition on $p(x)$ than the condition that it be irreducible, for the latter implies the former, while an equation which is separable is not necessarily irreducible.

THEOREM 9. If the separable equation $p(x) = 0$ is of degree n, the degree of the resolvent of its root field is $\leq n!$ (3, p.98).

If $p(x) = 0$ is irreducible in F, but is completely reducible into linear factors in any of its stem fields, it is called a normal equation. That is, all the numbers of the stem field of a normal equation can be written as polynomials in any other root.

An automorphism of $F(\rho)$ is defined to be a correspondence $\alpha \longleftrightarrow \beta$ of the numbers of $F(\rho)$ provided it is an automorphism of both the addition and multiplication groups of $F(\rho)$. The automorphism is said to be relative to F_1, a subfield of $F(\rho)$, if every number of F_1 corresponds to itself under the automorphism.

A set of numbers u_0, u_1, ..., u_{n-1} of $F(\rho)$ such that every number α of $F(\rho)$ is uniquely expressible in the form

$$\alpha = a_0 u_0 + a_1 u_1 + \dots + a_{n-1} u_{n-1}, \qquad a_i \in F,$$

is said to form a basis for $F(\rho)$. By Theorem 3 one such basis is $1, \rho, \rho^2, \dots, \rho^{n-1}$. If these numbers do form a basis for $F(\rho)$, every automorphism of $F(\rho)$ relative to F can be defined by stating the correspondence $\rho \longleftrightarrow \rho'$ of ρ with the number ρ'. For, if

$$\alpha = a_0 + a_1 \rho + a_2 \rho^2 + \dots + a_{n-1} \rho^{n-1}$$

is any number of $F(\rho)$, then

$$\alpha \longleftrightarrow \alpha' = a_0 + a_1 \rho' + a_2 \rho'^2 + \dots + a_{n-1} \rho'^{n-1}.$$

THEOREM 10. If $\rho \longleftrightarrow \rho'$ is an automorphism of $F(\rho)$ relative to F, then ρ' is one of the conjugates of ρ (3, p.99).

THEOREM 11. If ρ' is a conjugate of ρ, then $\rho \longleftrightarrow \rho'$ is an automorphism of $F(\rho)$ relative to F if and only if $F(\rho') = F(\rho)$ (3, p.99).

Thus, since the conjugate fields of a normal equation are all equal, a normal equation of degree n with coefficients in F has exactly n automorphisms relative to F.

THEOREM 12. The automorphisms of $F(\rho)$ relative to F form a group (3, p.99).

THE GALOIS GROUP

Let N be the root field of the separable equation $p(x) = 0$ with coefficients in F, and let G be the group of automorphisms of N relative to F. Let F_1 be a field such that $F \subseteq F_1 \subseteq N$. Then the totality of elements of G which leave numbers of F_1 invariant form a subgroup G_1 of G called the Galois group of N relative to F_1 . Thus G is the Galois group of N relative to F, and the identity automorphism I is the Galois group of N relative to itself.

THEOREM 1. Let N be a normal field of order n over F with Galois group G relative to F, and let $F \subset F_1 \subset N$. Then, if F_1 is normal, the Galois group G_1 of N relative to F_1 is an invariant subgroup of G.

Proof. Since F_1 is normal, every element $g \epsilon G$ carries each number $\alpha \epsilon F_1$ into some number $\alpha' \epsilon F_1$. Thus gG_1g^{-1} carries α into itself so that $gG_1g^{-1} \subseteq G_1$. Similarly, $g^{-1}G_1g \subseteq G_1$. Hence, $gG_1g^{-1} = G_1$ so that G_1 is an invariant subgroup of G.

THEOREM 2. If N_1 is a proper subfield of the field $N = F(\rho)$, there exists some number $\beta \epsilon N_1$ such that $N_1 = F(\beta)$.

Proof. The field N_1 consists of numbers in N all of which are imprimitive in N. For suppose $\omega \epsilon N_1$ is a primitive number of N. Then $F(\omega) = F(\rho)$ is in N_1, which is a contradiction.

Among the numbers of N_1 there is at least one which satisfies an irreducible equation of highest degree $k < n$. Say β is such a number. Then $F(\beta) \subseteq N_1$. Assume there is some number α which is in

N_1 but not in $F(\beta)$. By adjoining α to the field $F(\beta)$, the field $F(\beta,\alpha) = F(\sigma)$ is obtained, where $\sigma \in N_1$. Then, $F(\beta) \subseteq F(\beta,\alpha) = F(\sigma) \subseteq N_1$. But $F(\sigma)$ is of degree k by hypothesis, so that β is a primitive number in $F(\sigma)$. Hence, $F(\beta,\alpha) = F(\beta)$ for all numbers α in N_1 so that $F(\beta) = N_1$.

THEOREM 3. If N and N_1 are normal fields, $F \subset N_1 \subset N$, and if G and H are the Galois groups of N relative to F and N_1, respectively, then G/H is the Galois group of N_1 relative to F.

Proof. The Galois group of $N_1 = F(\beta)$ relative to F is the group K of k automorphisms

$$\beta \longleftrightarrow \beta,\ \beta \longleftrightarrow \beta',\ \dots,\ \beta \longleftrightarrow \beta^{(k-1)}.$$

Or, in terms of ρ, K consists of the automorphisms

$$\rho \longleftrightarrow \rho,\ \rho \longleftrightarrow \rho',\ \dots,\ \rho \longleftrightarrow \rho^{(k-1)}.$$

Now, H consists of the automorphisms of G which leave the elements of N_1 invariant, and the elements g_0, g_1, ..., g_{k-1} of K are distinct modulo H. Thus, the Galois group of N_1 relative to F is the quotient group G/H which contains the elements H, g_1H, ..., $g_{k-1}H$.

THEOREM 4. If H is a subset of G, all the elements of N which correspond to themselves under the automorphisms H form a subfield F_1 of N.

This is Theorem 43.1 (3, p.100) and is proved there.

Thus, H determines a unique subfield F_1 of N. Now consider the Galois group G_1 of N relative to F_1. Since every subset of G_1 leaves every element of F_1 invariant, one such subset could possibly determine F_1 uniquely. Hence, although a subset H will determine a unique subfield F_1, the group determined by F_1, namely its Galois group G_1, might contain H as a proper subset.

THEOREM 5. If H is an invariant subgroup of G, all the elements of N which correspond to themselves under H form a normal subfield F_1 of N.

Proof. Some element g in G carries F_1 into the conjugate field F_1'. Then gHg^{-1} carries all the elements of F_1' into themselves. But H is an invariant subgroup so that H leaves F_1' invariant. Since F_1 is the totality of numbers of N left invariant by H, $F_1' \subseteq F_1$. However, if F_1' is a proper subfield of F_1 then, by Theorem 2, F_1' is of degree less than h. But this is impossible, since all the conjugates of F_1 are of degree h. Hence, $F_1' = F_1$ so that F_1 is normal.

THEOREM 6. If H is a maximal invariant subgroup of the Galois group G of N relative to F, then there exists a normal field N_1, $F \subset N_1 \subset N$, such that the Galois group of N relative to N_1 is H.

Proof. Since H is invariant, it determines a normal subfield N_1 in the sense of Theorem 5. Now, in general, N_1 determines G_1, the Galois group of N relative to N_1, where $G \supset G_1 \supseteq H$. However, N_1 is normal so that G_1 would be invariant by Theorem 1. But H is a maximal invariant subgroup of G so that $G_1 = H$, or H is the Galois group of N relative to N_1.

THEOREM 7. If $f(x) = 0$ is a normal equation of degree n (defining the normal field N) with the Galois group G relative to F, and if G contains an invariant subgroup H of order h (defining the normal subfield N_1), then f(x) factors into k factors, each of degree h with coefficients in N_1 (3, p.103).

Then $f(x) = f_1(x)f_2(x)\cdots f_k(x)$ with each $f_i(x)$ of degree h. Suppose $f_1(x)$ is the factor which has ρ as a zero. Then, $f_1(x)$ is irreducible in N_1; for, suppose $f_1(x)$ has an irreducible factor $g_1(x)$ of degree $m < h$ with coefficients in N_1, where $g_1(\rho) = 0$. Now, it is evident that $N = N_1(\rho)$ since $N_1(\rho) = F(\beta,\rho) = F(\rho,\beta) = F(\rho)$, so that $g_1(x) = 0$ is a normal equation defining N. Then the numbers $1, \rho, \rho^2, \ldots, \rho^{m-1}$ form a basis for N over N_1. Also, there exist numbers $1, \beta, \beta^2, \ldots, \beta^{k-1}$ which form a basis for $N_1 = F(\beta)$ over F.

Now, the products $\beta^i\rho^j$ ($i = 0, 1, \ldots, k-1$; $j = 0, 1, \ldots, m-1$) form a basis of N over F if they are linearly independent. Assume that they are linearly dependent. Then there exists a relation

$$c_0 + c_1\beta + c_2\beta^2 + \cdots + c_{k-1}\beta^{k-1} + c_k\rho + c_{k+1}\beta\rho + \cdots + c_{mk-1}\beta^{k-1}\rho^{m-1} = 0$$

where the $c_i \in F$ and are not all zero. But $\beta \in N_1$ so that this becomes

$$d_0 + d_1\rho + d_2\rho^2 + \cdots + d_{m-1}\rho^{m-1} = 0$$

where the $d_i \in N_1$. Since the numbers $1, \rho, \rho^2, \ldots, \rho^{m-1}$ are linearly independent over N_1, the d_i are all zero; i.e.,

$$d_0 = c_0 + c_1\beta + c_2\beta^2 + \cdots + c_{k-1}\beta^{k-1} = 0,$$
$$d_1 = c_k + c_{k+1}\beta + c_{k+2}\beta^2 + \cdots + c_{2k-1}\beta^{k-1} = 0,$$
$$\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad ,$$
$$d_{m-1} = c_{k(m-1)} + c_{k(m-1)+1}\beta + c_{k(m-1)+2}\beta^2 + \cdots + c_{mk-1}\beta^{k-1} = 0.$$

But the numbers $1, \beta, \beta^2, \ldots, \beta^{k-1}$ are linearly independent over F so that the c's must all be zero, a contradiction.

Thus, the products $\beta^i\rho^j$ form a basis of N over F. But N is of degree n over F so that $mk = n$ or $m = h$. Since the same argument is valid for any of the roots of $f(x) = 0$ it follows that all the factors $f_1(x)$, $f_2(x)$, ..., $f_k(x)$ are irreducible in N_1.

Let the normal equation $p(x) = 0$ define the normal field N and let G be the Galois group of N relative to F. Suppose G has the series of composition G, H_1, H_2, ..., H_s, I and prime quotient groups G/H_1, H_1/H_2, ..., H_{s-1}/H_s, H_s. Then $H_1 \subset G$ leaves some normal field N_1 invariant, where $F \subset N_1 \subset N$. By Theorem 6, H_1 is the Galois group of N relative to N_1; by Theorem 3, G/H_1 is the Galois group of N_1 relative to F. G/H_1 is simple, since H_1 is maximal. Now, by the previous argument $p(x)$ has a factor $p_1(x)$ of degree h with coefficients in N_1, which is irreducible in N_1. That is, $p_1(x) = 0$ is a normal equation defining the field N over N_1, where the Galois group of N relative to N_1 is H_1. Then, since H_2 is a maximal invariant subgroup of H_1, H_2 leaves some field N_2 invariant, where $F \subset N_1 \subset N_2 \subset N$. Now, N_2 is normal relative to N_1, since N_2 coincides with each of its conjugates under the automorphisms H_1. Then H_2 is the Galois group of N relative to N_2, and H_1/ H_2 is the Galois group of N_2 relative to N_1 and is simple. Continuing in this manner, the fields $F \subset N_1 \subset N_2 \subset \ldots \subset N_{s-1} \subset N_s \subset N$ are obtained, where N_i is normal relative to N_{i-1}, H_{i-1}/H_i is the Galois group of N_i relative to N_{i-1}, and H_i is the Galois group of N relative to N_i.

SOLUTION BY RADICALS

An equation $p(x) = 0$ with coefficients in a field F is solvable by radicals relatively to F if all the roots of $p(x) = 0$ can be obtained in a finite number of steps from the numbers of F by the rational operations and root extractions. The object now is to establish the result that an equation is solvable by radicals relatively to its coefficient field if and only if the factors of composition of its Galois group are all primes. The sufficiency follows almost immediately from Theorems 11 and 12, which are proved by MacDuffee (3, pp.109-111).

If, corresponding to the prime quotient groups G/H_1, H_1/H_2, ..., H_{s-1}/H_s, H_s of the Galois group G of $p(x) = 0$, there exist the normal fields $N \supset N_s \supset \dots \supset N_1 \supset F$, then $p(x) = 0$ is solvable by radicals relatively to F if and only if the resolvent of N_i is solvable by radicals relatively to the field N_{i-1} for every i. Since the roots of any one resolvent are polynomials in each root of every other resolvent, it is immaterial which resolvent of N_i is chosen.

An equation is called cyclic if its Galois group is cyclic.

THEOREM 11. Every [normal] cyclic equation $p(x) = 0$ of degree n is solvable by radicals relatively to the field $F(\rho)$ where ρ is a primitive nth root of unity.

THEOREM 12. Every root of unity can be expressed in terms of radicals relatively to the rational field.

By the last two theorems every normal cyclic equation is solvable by radicals relatively to its field of coefficients. The resolvent of the root field N of the cyclic equation $p(x)=0$ is a normal cyclic equation. Hence, numbers of N, in particular the roots of $p(x)=0$, are expressible as radicals. This result is stated in the following theorem.

THEOREM 13. Every cyclic equation $p(x)=0$ of degree n is solvable by radicals relatively to the field of its coefficients.

In order to prove the necessity in the statement at the beginning of this section, it will be useful to establish the results stated in Theorems 14 through 18.

THEOREM 14. Every pth root of unity, where p is a prime, can be expressed in terms of radicals of index less than p.

Proof. The statement is certainly true for $p=2$ and $p=3$. Assume it holds for every prime less than p. The roots $\sigma_1, \sigma_2, \ldots, \sigma_q$ of the reciprocal equation (3, p.111) where $q=(p-1)/2$ can be expressed as linear functions of $\sqrt[q]{\delta_0}$, $\sqrt[q]{\delta_1}$, ..., $\sqrt[q]{\delta_{q-1}}$ where δ_i is a number of the field $F(\rho_1)$, ρ_1 a primitive qth root of unity. Thus, a primitive pth root of unity ρ can be expressed in terms of radicals of a primitive qth root of unity ρ_1, the radicals being of index less than p. If $q=p_1 p_2 \cdots p_k$ is composite, a primitive qth root of unity is

$$\rho_{p_1} \sqrt[p_1]{\rho_{p_2}} \cdot \sqrt[p_1 p_2]{\rho_{p_3}} \cdot \sqrt[p_1 p_2 p_3]{\rho_{p_4}} \cdot \cdot \cdot \sqrt[p_1 p_2 \cdots p_{k-1}]{\rho_{p_k}}$$

where ρ_{p_i} is a primitive p_ith root of unity. Thus, since the statement was assumed to be true for every prime less than p, ρ_1 is expressible in terms of radicals of index less than p. Then ρ is also so expressible.

THEOREM 15. The function $x^p - a = 0$, p a prime, is irreducible in a field $F(\rho)$ if a is not the pth power of any number in $F(\rho)$, where ρ is a primitive pth root of unity (2, p.156).

THEOREM 16. Let p be an odd prime and ρ a primitive pth root of unity. Then the Galois group G of $x^p = A$ relative to $F(\rho)$, where A is in $F(\rho)$, consists of the identity automorphism if one root of $x^p = A$ is in $F(\rho)$, but is a cyclic group of order p if no root of $x^p = A$ is in $F(\rho)$.

Proof. The roots of $x^p = A$ can be written χ, $\rho\chi$, $\rho^2\chi$, ..., $\rho^{p-1}\chi$ where χ is one root of $x^p = A$, for if $x = y\chi$, $y^p = 1$. Thus, the coefficient field $F(\rho)$ is also the root field of $x^p = A$ if $\chi \epsilon F(\rho)$, so that G contains only the identity automorphism.

If no root is in $F(\rho)$, $x^p = A$ is irreducible, for then A is not the pth power of any number in $F(\rho)$. Now, consider the stem field F_i of $x^p = A$ where F_i is obtained by adjoining a root χ_i to the coefficient field $F(\rho)$. A number α of F_i is represented uniquely by $\alpha = a_0 + a_1\chi_i + a_2\chi_i^2 + \ldots + a_{p-1}\chi_i^{p-1}$, $a_j \epsilon F(\rho)$. But $\chi_i = \rho^{i-1}\chi$, so that $\alpha = a_0 + a_1\rho^{i-1}\chi + a_2\rho^{2(i-1)}\chi^2 + \ldots + a_{p-1}\rho^{(p-1)(i-1)}\chi^{p-1} = a_0' + a_1'\chi + a_2'\chi^2 + \ldots + a_{p-1}'\chi^{p-1}$, $a_j' \epsilon F(\rho)$. Thus, since the numbers in the stem field F_i can be written as polynomials of any other root χ with coefficients in $f(\rho)$, F_i is normal. Hence, $x^p = A$ is a normal equation so that G contains exactly p automorphisms.

THEOREM 17. Let the normal field $F(\rho)$ be defined by the irreducible equation $f(x) = 0$ of degree n with coefficients in F, and let $F(\chi)$ be defined by $x^p = A$. Then, if χ is not in $F(\rho)$, $F(\chi) \wedge F(\rho) = F$.

Proof. Let ω be any number in the intersection. Then, since $F(\omega)\subset F(\chi)$ and $F(\omega)\subset F(\rho)$, $F(\omega)$ is in the intersection. The Galois group K_1 of $F(\chi)$ relative to $F(\omega)$ is a subgroup of the Galois group K of $F(\chi)$ relative to F, which is of prime order. Hence, $K_1 = I$ or $K_1 = K$. However, if $K_1 = I$, $F(\omega) = F(\chi)$ which is impossible, since $F(\chi)$ is not in $F(\rho)$. Then $K_1 = K$ so that $F(\omega) = F$, or $\omega \in F$.

THEOREM 18. Let F contain a number A and the pth roots of unity and let $N = F(\rho)$ be defined by the normal equation $f(x) = 0$ of degree n. Let χ be a root of $x^p = A$. Then, if G is the Galois group of N relative to F, G is the Galois group of $N(\chi)$ relative to $F(\chi)$ if χ is not in N, or H is the Galois group of $N(\chi) = N$ relative to $F(\chi)$ if χ is in N, where H is a maximal invariant subgroup of G of prime index.

Proof. The function $f(x)$ is irreducible in $F(\chi)$ if χ is not in $F(\rho)$, for, if $f(x)$ had factors with coefficients in $F(\chi)$, these coefficients must also be in $F(\rho)$, since $f(x)$ is completely factorable in $F(\rho)$. But, according to the last theorem, the intersection of these two fields contains only numbers in F. Then $f(x) = 0$ defines the normal field $N(\chi)$ with coefficients in $F(\chi)$ so that G is the Galois group of $N(\chi)$ relative to $F(\chi)$.

If χ is in $F(\rho)$, then $F(\rho)\supset F(\chi)\supset F$. Since $F(\chi)$ is normal, the Galois group H of $F(\rho)$ relative to $F(\chi)$ is an invariant subgroup of G by Theorem 1. By Theorem 3, G/H is the Galois group of $F(\chi)$ relative to F, G/H being cyclic of prime order by Theorem 16. Hence, H is maximal of prime index.

It is now possible to prove the result mentioned at the beginning of the section, which is stated again in the following theorem.

THEOREM 19. If G is the Galois group of an equation $p(x)=0$ relative to its coefficient field F, a necessary and sufficient condition that $p(x)=0$ be solvable by radicals relatively to F is that the factors of composition of G consist entirely of primes.

Proof. It should be noted here that by the Jordan-Hölder Theorem the factors of composition for two series of composition are the same except possibly for order.

Assume that the roots of $p(x)=0$ can be derived by rational operations and root extractions from numbers in F or from numbers obtained from them by those operations. Make a list

$$a_1^{1/p_1}, a_2^{1/p_2}, \ldots, a_k^{1/p_k}$$

of all the radicals appearing in the expressions for the roots, where the p's are primes, since a pqth root is a pth root of a qth root. List first the underneath radical in such a two-story radical followed later by the two-story radical itself. Make the list such that a_1 is in F, a_2 is in the field obtained by adjoining to F the first radical, a_3 is in the field obtained by adjoining to F the first two radicals, etc.

By Theorem 14, the pth roots of unity are expressible in terms of radicals of indices less than p. The roots of $x^p=1$, then, can be expressed rationally in terms of radicals forming a chain of the above type where the first number listed is the root of a rational number. List the radicals of the chain for $p = 3$ followed by those for $p = 5$, etc., for the primes up to and including the maximum of $p_1, \ldots, p_k$. After the last of these write the previous list and obtain the list

$$b_1^{1/q_1}, b_2^{1/q_2}, \ldots, b_s^{1/q_s}$$

where the q's are primes, b_1 is in the field F, b_2 is in the field obtained by adjoining to F the first radical, b_3 is in the field obtained by adjoining to F the first two radicals, etc. The roots of $p(x) = 0$ are rational functions of these radicals with coefficients in F. Also, the adjunction to F of the first $r - 1$ radicals results in a field containing all the q_rth roots of unity. By the previous theorem, the adjunction to F of the first radical listed, which is $\sqrt{-3}$, does not affect G if $\sqrt{-3}$ is not in the root field N of $p(x) = 0$, or it reduces G to a maximal invariant subgroup of index q_1 if $\sqrt{-3}$ is in N. The adjunction of the second radical to the resulting field either leaves the resulting Galois group unchanged or reduces it to a maximal invariant subgroup of index q_2. Continuing in this manner a field is obtained containing the roots of $p(x) = 0$, the Galois group of which is the identity I. Now, each time that the group was reduced the resulting group was a maximal invariant subgroup of prime index of the preceding group. Hence, the factors of composition are all primes, so that the condition is necessary.

Now, if the factors of composition are all primes, the groups G/H_1, H_1/H_2, H_2/H_3, ... are all of prime order; hence, they are cyclic. Now, since H_{i-1}/H_i is the Galois group of N_i relative to N_{i-1}, the resolvent of N_i over N_{i-1} is a cyclic equation. Thus, the roots of $p(x) = 0$ are obtainable from the field of coefficients by the solution of a chain of cyclic equations. By Theorem 13 each of these equations is solvable by radicals relatively to the field of the coefficients of the preceding equation.

THE GENERAL EQUATION

The following results are necessary in order to discuss the general equation.

A scalar x of a ring D containing a ring A is called an indeterminate over A if and only if the expression

$$p_0 + p_1 x + \ldots + p_n x^n = 0, \qquad p_i \in A,$$

implies the quantities p_0, p_1, ..., p_n are all zero.

The indeterminates x_1, ..., x_m over A of $D \supset A$ are called independent indeterminates over A if no polynomial in x_1, ..., x_m with coefficients in A is zero, unless these coefficients themselves are all zero.

Let D be a field and x_1, ..., x_n independent indeterminates over D. The equation

$$f(x) = (x - x_1)\ldots(x - x_n) = x^n - c_1 x^{n-1} + \ldots + (-1)^n c_n = 0$$

is then a separable equation with roots in the polynomial ring $D[x_1, \ldots, x_n]$ and coefficients in $F = D(c_1, \ldots, c_n)$. The Galois group G of f(x) relative to F is isomorphic to G_0, a subgroup of the group $G_{n!}$ of all permutations of x_1, ..., x_n. But every permutation of x_1, ..., x_n defines an automorphism of $N = D(x_1, \ldots, x_n)$ which leaves the elements of F invariant. Thus $G_0 = G_{n!}$, so that G is of order n!.

THEOREM 20. The general equation of degree n has for its Galois group the symmetric group of order n!.

Proof. If α_1, ..., α_n are independent indeterminates over some field D, then the general equation is

$$f(x) = x^n + \alpha_1 x^{n-1} + \dots + \alpha_n = 0.$$

Let $F = D(\alpha_1, \dots, \alpha_n)$, which is equivalent to $D(c_1, \dots, c_n)$ where $c_1, \dots, c_n$ are given by

$$f(x) = (x - x_1)\cdots(x - x_n) = x^n - c_1 x^{n-1} + \dots + (-1)^n c_n = 0$$

and are independent indeterminates over D. Then the coefficients α_i may be replaced by the corresponding new independent indeterminates $(-1)^i c_i$ (1, p.148), and it has already been shown that the Galois group of this equation is of order n!.

It has been noted that the general equation of degree $n = 2, 3, 4$ is solvable by radicals. As an example of the theory developed here consider the case of $n = 4$. The Galois group G_0 contains the permutations of the symmetric group of order 24. The alternating group of order 12 is a maximal invariant subgroup of G_0, and its elements are listed below.

$p_1 = 1$	$p_5 = (12)(13)$	$p_9 = (13)(14)$
$p_2 = (12)(34)$	$p_6 = (13)(12)$	$p_{10} = (14)(13)$
$p_3 = (13)(24)$	$p_7 = (12)(14)$	$p_{11} = (23)(24)$
$p_4 = (14)(23)$	$p_8 = (14)(12)$	$p_{12} = (24)(23)$

It can be shown that G_4: p_1, p_2, p_3, p_4 is a maximal invariant subgroup of the alternating group. Now G_4 contains the subgroups $G_{2,1}$: p_1, p_2, $G_{2,2}$: p_1, p_3, $G_{2,3}$: p_1, p_4, which are maximal invariant subgroups of G_4, since G_4 is abelian. Thus, the factors of composition of G_0 are 2, 3, 2, 1, which are all prime.

THEOREM 21. The general equation of degree $n > 4$ is not solvable by radicals.

Proof. The symmetric group G of order n! has the maximal invariant subgroup A, which is the alternating group of order n!/2. But this group is simple for $n > 4$ (2, p.200), so that the factors of composition of G are 2, n!/2. The result follows from Theorem 19, since n!/2 is not a prime for $n > 4$.

BIBLIOGRAPHY

1. Albert, A. Adrian. Modern higher algebra. Chicago, University of Chicago press, 1937. 319p.

2. Dickson, Leonard Eugene. Modern algebraic theories. Chicago, New York, Boston, Sanborn, 1926. 276p.

3. MacDuffee, Cyrus Colton. An introduction to abstract algebra. New York, Wiley, 1940. 303p.

4. Miller, G. A., H. F. Blichfeldt, Leonard Eugene Dickson. Theory and applications of finite groups. New York, Stechert, 1938. 390p.