July 31, 1950

To the Graduate Council:

I am submitting herewith a thesis written by Charles Leston Bradshaw entitled "The Galois Group of a Polynomial Equation with Coefficients in a Finite Field." I recommend that it be accepted for six quarter hours of credit in partial fulfillment of the requirements for the degree of Master of Arts, with a major in Mathematics.

Robert H. Wilson
Major Professor

We have read this thesis
and recommend its acceptance:

G. B. Albert

O. H. Harrold, Jr.

Accepted for the Council:

E. G. Watts
Dean of the Graduate School

THE GALOIS GROUP OF A POLYNOMIAL EQUATION WITH COEFFICIENTS IN A FINITE FIELD

A THESIS

Submitted to
The Committee on Graduate Study
of
The University of Tennessee
in
Partial Fulfillment of the Requirements
for the degree of
Master of Arts

---

by

Charles Leston Bradshaw

August 1950

ACKNOWLEDGMENT

The author wishes to express his appreciation to Professor R. L. Wilson, under whose direction this thesis was written, for his suggestion of the topic and for his valuable assistance in its preparation.

TABLE OF CONTENTS

CHAPTER I

INTRODUCTION

The primary purpose of this thesis is to demonstrate a method for the determination of the Galois group of a polynomial equation with coefficients in a finite field. The problem of finding the Galois group of an arbitrary equation, where the coefficient field is either finite or infinite, is neither new nor unsolved. Van der Waerden[1] illustrates a method which is dependent upon the fact that the permutations of the Galois group are characterized by the property that they transform the quantity

$$Z = x_1r_1 + x_2r_2 + \cdots + x_nr_n$$

into its conjugates. The x_i denote n indeterminants and the r_i the roots of the polynomial under consideration. He performs all possible permutations of the indeterminants x on Z and forms the product

$$F(y,x) = \prod_s (y - s_xZ),$$

where the s_x denote the permutations of the x_i. It is then proved that if the polynomial $F(y,x)$ be decomposed into irreducible factors, the permutations s_x which carry any one of the irreducible factors into itself is exactly the Galois group of the given equation. Cajori[2] suggests a method,

---

[1]B. L. van der Waerden, Modern Algebra (New York: Frederick Ungar Company, 1949), p. 189.

[2]F. Cajori, An Introduction to the Modern Theory of Equations (New York: The Macmillan Company, 1904), p. 169.

somewhat similar to this, in which he forms the Galois resolvent and tests it for reducibility. Wilson[3] completely solves the problem in the case of the infinite field. The method used in this thesis follows that of his in so far as it is applicable.

The method as given here is dependent upon the determination of the roots of an induced equation. This method is used to determine successively whether the Galois group is or is not contained in each of the subgroups of the symmetric group of degree n, where n is the degree of the equation under consideration. The information so obtained permits us to determine which of these subgroups is the Galois group, or whether the Galois group is the symmetric group. We need only note which subgroup contains the Galois group but has no subgroup containing the Galois group.

We shall first select an arbitrary subgroup of the symmetric group of degree n, where again n is the degree of the given equation. Having selected one such group it will be necessary to display a rational function of the roots of the given equation with rational coefficients, which is invariant under all of the permutations of the selected group. We then construct an equation which has coefficients in the coefficient field of the original equation, and which has this

---

[3]R. L. Wilson, "A Method for the Determination of the Galois Group." To appear soon in the Duke Mathematical Journal.

function as one of its roots. We call the equation so constructed the induced equation. It is now necessary to determine if the function displayed above, or one of its conjugates, is an element of the coefficient field $\underline{F}$. If we find that the induced equation has no roots in F, then surely the function is not in F. It may happen that all of the roots of the induced equation, which are in F, are multiple roots. In this case we show, by theorem 8, that it is possible, in a finite number of steps, to construct an induced equation which has no roots in the coefficient field, or else to conclude that the Galois group is contained in the selected subgroup. In most instances it will be unnecessary to use theorem 8.

We are now in a position to apply a basic theorem in Galois theory (theorem 5). In case the function of the roots, which we have constructed, is a non-repeated root of the induced equation and is in F, the Galois group is contained in the subgroup we had initially selected. If the function is not in F, then the group we have selected does not contain the Galois group.

Examples are given in Chapter IV illustrating this method for finding the Galois group.

CHAPTER II

DEFINITIONS AND NOTATIONS

We state the following well-known definitions and theorems.

DEFINITION 1. A field F is a system of elements closed under two binary operations, addition and multiplication, such that

(a) under addition, F is a commutative group with identity zero;

(b) under multiplication, the elements of F not zero form another commutative group;

(c) addition is distributive with respect to multiplication.

DEFINITION 2. If there is a positive integer p such that $p \cdot a = 0$ for each a in a field F, and if p is the smallest integer with this property, then F is said to have characteristic p. If no such element exists then F is said to have characteristic zero. The two types of fields are often referred to as finite and infinite, respectively.

DEFINITION 3. A set of linearly independent quantities $u_1, u_2, \cdots, u_n$ of an extension N over F is said to form a basis of N over F if each x which is an element of N can be expressed as a linear combination

$$x = a_1u_1 + a_2u_2 + \cdots + a_nu_n,$$

where $a_1, a_2, \cdots, a_n$ are elements of F.

DEFINITION 4. An extension N of F is called a root field of a polynomial $f(x)$ of degree n with coefficients in F if

(a) $f(x)$ can be factored into linear factors

$$f(x) = c(x - r_1)(x - r_2) \cdots (x - r_3)$$

in N, and;

(b) N can be generated over F by the roots of $f(x)$, as

$$N = F(r_1, r_2, \cdots, r_n).$$

DEFINITION 5. If $N = F(r_1, r_2, \cdots, r_n)$ is the root field of a polynomial

$$f(x) = (x - r_1)(x - r_2) \cdots (x - r_n),$$

then the automorphism group of N over F is known as the Galois group of the equation $f(x) = 0$ or as the Galois group of N over F.

DEFINITION 6. A polynomial $f(x)$ of degree n is called separable over a field F if there exists n distinct roots of $f(x)$ in some root field $N \geq F$; otherwise $f(x)$ is called inseparable.

THEOREM 1.[1] The number s of elements in a finite field of characteristic p (p must be prime) is a power of the prime p, that is, $s = p^n$.

---

[1]R. D. Carmichael, Introduction to the Theory of Groups of Finite Order (Boston: Ginn and Company, 1937), p. 245.

THEOREM 2.[2] For any prime p and any positive integer n there exists a finite field with $s = p^n$ elements.

THEOREM 3.[3] Any two finite fields with the same number of elements are isomorphic.

THEOREM 4.[4] The root field N over F of the equation $x^s - x = 0$ with $s = p^n$ is a finite field with $s = p^n$ elements. We call N a Galois field.

In view of theorem 3 it follows that a particular Galois field, so far as its abstract properties are concerned, is completely determined by s. Moreover, a Galois field is abstractly identical with any finite field with the same number of elements. There is no loss of generality in referring to the coefficient field as a Galois field.

The following conventions and notation will be observed throughout this thesis.

1. The coefficients of the given polynomial are to be in a finite field, F. It is no restriction to require the equation to be monic. If $f(x) = 0$ is an equation of degree n,

$$f(x) = b_0x^n + b_1x^{n-1} + \cdots + b_n = 0,$$

---

[2]G. Birkhoff and S. MacLane, A Survey of Modern Algebra (New York: The Macmillan Company, 1948), p. 429.

[3]Ibid., p. 430.

[4]A. A. Albert, Modern Higher Algebra (Chicago: University of Chicago Press, 1937), p. 167.

we may multiply the polynomial by b_o^{-1}; this surely exists since we have assumed $f(x)$ to be of degree n, hence $b_o \neq 0$. We obtain an equation in the form

$$(1) \qquad p(x) = x^n + a_1 x^{n-1} + \cdots + a_n.$$

It is obvious that the Galois group of $p(x) = 0$ is identical with that of $f(x) = 0$ since the roots of the two polynomials, and thus the root fields, are the same. The notation $p(x) = 0$ will in every case refer to a polynomial of type (1). We shall further require that $p(x) = 0$ be separable. If the equation is irreducible over F there is no loss of generality in doing this, since it has been proved[5] that any irreducible equation over a Galois field is separable. However, we shall make no assumption regarding the reducibility of the polynomial under consideration.

2. We shall denote by Γ an arbitrary subgroup of the symmetric group, S_n. Γ can be any one of these subgroups, but having been chosen will be considered as a fixed group. The Galois group of the equation $p(x) = 0$ will be denoted by G. Both Γ and G will be considered as permutation groups on n symbols. This will always be possible since both Γ and G are subgroups of S_n. In using the word "subgroup", we make no distinction between a proper subgroup and an improper subgroup unless a statement is made to that effect.

---

[5] Van der Waerden, op. cit., p. 124.

3. We shall denote n indeterminants by $x_1, x_2, \cdots, x_n$ and in a similar manner the roots of $p(x) = 0$ shall be denoted by $r_1, r_2, \cdots, r_n$ where the roots are taken in some fixed order. Although the order is fixed it is immaterial which root is denoted by r_1, which by r_2, etc. The r_i are distinct since we have required that $p(x) = 0$ be a separable equation.

CHAPTER III

DETERMINATION OF THE GALOIS GROUP

Γ has been defined to be a fixed group which is a subgroup of S_n. We wish to determine whether or not it is possible to find a rational function $f_1(x_1, x_2, \cdots, x_n)$ of the n indeterminants, with coefficients in F, which is invariant under the permutations of Γ, but under no permutations not in Γ. If this is possible, and if $f_1(r_1, r_2, \cdots, r_n)$ is a number in F and distinct from all the numbers obtained by applying to $f_1(r_1, r_2, \cdots, r_n)$ permutations outside Γ, we apply the following theorem.

THEOREM 5.[1] The Galois group G relative to the coefficient field F of a separable equation $p(x) = 0$ is uniquely defined by the following properties:

A: Every rational function with coefficients in F of the roots of $p(x) = 0$ which is invariant under G is equal to a number of F.

B: Every rational function with coefficients in F of the roots of $p(x) = 0$ which is equal to a number of F is invariant under G.

We thus have as our problem the following:

(a) To construct a rational function $f_1(x_1, x_2, \cdots, x_n)$ with coefficients in F, which is invariant under Γ, but under no permutations not in Γ, and

---

[1] C. C. MacDuffee, Introduction to Abstract Algebra (New York: John Wiley and Sons, Inc., 1940), p. 102.

(b) To determine whether $f_1(r_1, r_2, \cdots, r_n)$ is a number in F and whether or not this number is left invariant by any permutations outside Γ.

We proceed as follows to set up an equation which we call the equation induced by Γ, or simply, the induced equation.

Let $g_1(x_1, x_2, \cdots, x_n)$ be defined by

(2) $$g_1(x_1, x_2, \cdots, x_n) = x_1^{n-1} x_2^{n-2} \cdots x_{n-2}^{2} x_{n-1}.$$

Assume that Γ is of order $\underline{h}$, then we shall denote by $g_1, g_2, \cdots, g_h$ the $\underline{h}$ functions obtained by applying the $\underline{h}$ permutations of Γ to $g_1(x_1, x_2, \cdots, x_n)$. It is obvious that the $\underline{g_i}$ are distinct. We now define $f_1(x_1, x_2, \cdots, x_n)$ as follows:

(3) $$f_1(x_1, x_2, \cdots, x_n) = g_1 + g_2 + \cdots + g_h.$$

The $\underline{h}$ permutations of Γ will leave $f_1(x_1, x_2, \cdots, x_n)$ invariant. This is true since the $\underline{h}$ permutations form a group and they will merely interchange the g_i in (3). On the other hand, any permutation not in Γ will change g_1 into some function different from any of the g_i considered above. This, of course, changes $f_1(x_1, x_2, \cdots, x_n)$ into some other rational function of the n indeterminants with coefficients in F. We say that this second function is conjugate to $f_1(x_1, x_2, \cdots, x_n)$. We now have a function $f_1(x_1, x_2, \cdots, x_n)$ which is invariant under the permutations of Γ, but is altered by any permutation not in Γ.

Let $\underline{s_i}$ be any permutation of $\lceil$, and let $\underline{t_2}$ be any permutation of S_n which does not belong to $\lceil$. A successive application of $\underline{s_i}$ and $\underline{t_2}$ on $f_1(x_1, x_2, \cdots, x_n)$, that is $t_2(s_i f_1)$, will give some function $f_2(x_1, x_2, \cdots, x_n)$ which is conjugate to $f_1(x_1, x_2, \cdots, x_n)$ but distinct from it. Since $f_2(x_1, x_2, \cdots, x_n)$ is a conjugate of $f_1(x_1, x_2, \cdots, x_n)$, it is a rational function of the n indeterminants with coefficients in F. We also note that since $s_i f_1 = f_1$ for each of the h distinct $\underline{s_i}$ of $\lceil$,

$$t_2 s_i f_1 = t_2 f_1 = f_2$$

for each of the h distinct $\underline{s_i}$. It follows that $t_2\lceil$ is a set of h elements distinct from the elements of $\lceil$, and distinct from each other, such that $t_2 s_i f_1 = t_2 f_1 = f_2$. It is noted that $t_2 \lceil$ actually forms a left coset of the subgroup $\lceil$ in the symmetric group, $\underline{S_n}$.

If $\lceil$ and $t_2\lceil$ do not exhaust S_n the existence of a permutation $\underline{t_3}$, which is in neither $\lceil$ nor $t_2\lceil$, is assured. As in the preceding discussion $t_3 s_i f_1 = t_3 f_1$ must define another function $f_3(x_1, x_2, \cdots, x_n)$, of the n indeterminants, conjugate to f_1 and f_2 and distinct from f_1 and f_2. We have already shown that f_1 and f_2 are distinct, and in exactly the same manner f_1 and f_3 are distinct. We now show that f_2 and f_3 are distinct. Assuming the contrary implies that

$$t_3 s_i f_1 = t_2 s_j f_1$$

for some $\underline{s_i}$ and some $\underline{s_j}$. From this it follows that

$$t_2^{-1}t_3s_if_1 = s_jf_1 = f_1$$

and

$$t_2^{-1}t_3s_if_1 = t_2^{-1}t_3f_1.$$

We conclude from this that $(t_2^{-1}t_3)$ must be an element of Γ, since it leaves f_1 invariant. If this is true then

$$t_2^{-1}t_3 = s_\ell$$

for some ℓ, and

$$t_3 = t_2s_\ell,$$

which means that t_3 is contained in $t_2\Gamma$ contradicting the hypothesis that t_3 is distinct from any of the elements of $t_2\Gamma$. If Γ, $t_2\Gamma$ and $t_3\Gamma$ do not exhaust the symmetric group, we can continue this process, and in a finite number of steps use all of the elements of the symmetric group. We can now write

$$S_n = \Gamma + t_2\Gamma + t_3\Gamma + \cdots + t_k\Gamma,$$

where $k = \frac{n!}{h}$. We define k distinct functions by this process. We denote these k functions by

(4) $f_1(x_1, x_2, \cdots, x_n), f_2(x_1, x_2, \cdots, x_n), \cdots,$

$f_k(x_1, x_2, \cdots, x_n).$

It has been pointed out that each of the f_i is a rational function whose coefficients belong to F.

THEOREM 6. If Γ is an arbitrary subgroup of the symmetric group of degree n, it is always possible to construct a rational function of n indeterminants with coefficients in F which is invariant under the permutation of Γ, and which is altered by any permutation not in Γ.

The discussion here in no way implies that the manner in which we have constructed the function $f_1(x_1, x_2, \cdots, x_n)$ is the only manner in which a function may be constructed satisfying the conditions of theorem 6. This is simply a method whereby we can be certain of obtaining at least one such function.

Let $f_1(x_1, x_2, \cdots, x_n)$ be a function which satisfies theorem 6, and let $f_2(x_1, x_2, \cdots, x_n), \cdots, f_k(x_1, x_2, \cdots, x_n)$ be the functions conjugate to f_1 defined as in (4). We now consider $f_1(r_1, r_2, \cdots, r_n), f_2(r_1, r_2, \cdots, r_n), \cdots, f_k(r_1, r_2, \cdots, r_n)$. Each of these $f_i(r_1, r_2, \cdots, r_n)$ represents a number in the root field of $p(x) = 0$. We have in no way inferred that these numbers are distinct. We now wish to determine if any of the $f_i(r_1, r_2, \cdots, r_n)$ are in F. To this end we construct the equation

$$(5) \qquad F(y) = \sum_{i=1}^{k} \left[y - f_i(r_1, r_2, \cdots, r_n) \right] = 0$$

with roots $f_1(r_1, r_2, \cdots, r_n), f_2(r_1, r_2, \cdots, r_n), \cdots, f_k(r_1, r_2, \cdots, r_n)$. We shall call this equation the <u>induced equation</u>. It is obvious that the induced equation is dependent upon the choice of f_1, and is not necessarily unique.

The coefficients of (5) are in F, for the coefficients are symmetric functions of the f_i, and the f_i are in turn symmetric in the roots. Thus, the induced equation is an equation of degree k, with leading coefficient unity, and all of its coefficients in F.

It is possible to determine all of the roots of $F(y) = 0$ which are in F. If there is no root of this equation which is in F, then no f_i is in F, and in particular f_1 is not in F. Since we have a rational function of the roots of $p(x) = 0$ which is invariant under Γ, and which is not in F, then by theorem 5, Part A, G cannot be a subgroup of Γ. If the induced equation $F(y) = 0$ has at least one non-repeated root in F, then some f_i is in F. If this non-repeated root is f_1, we then have a rational function of the roots of $p(x) = 0$ which is invariant under Γ, and since the root is a non-repeated root the rational function is not invariant under permutations outside Γ. Since this function is in F, we are assured by theorem 5, Part B, that G is contained in Γ. If the non-repeated root of $F(y) = 0$ is not f_1, but is $f_i (i \neq 1)$, the function f_i is invariant under the permutations $s_i \Gamma s_i^{-1}$, for

$$s_i \Gamma s_i^{-1} f_i = s_i \Gamma s_i^{-1} s_i f_1 = s_i \Gamma f_1 = s_i f_1 = f_i .$$

Thus f_i is invariant under the permutations of a group which is conjugate to Γ. We need only renumber the roots of $p(x) = 0$ in order to make f_i become f_1, and we again have f_1 in F. Using the same argument as above we may conclude that G is contained in Γ. We have proved the following theorem:

THEOREM 7. If the induced equation has at least one non-repeated root in F, then G is contained in Γ. If the equation has no roots in F, then G is not contained in Γ.

If equation (5) has only multiple roots in F, no inference may be drawn, since the functions $f_i(r_1, r_2, \cdots, r_n)$ are then invariant under Γ, but also under permutations not in Γ.

We now prove the following theorem:

THEOREM 8. For any given polynomial equation of degree n and an arbitrary subgroup Γ of S_n, it is possible (if the order of Γ is not a multiple of p) to construct an induced equation, depending upon a parameter a, such that in a finite number of steps we are assured of

(a) finding an induced equation with at least one non-repeated root in F, or

(b) finding an induced equation with no roots in F, or

(c) being able to conclude that $G \subseteq \Gamma$.

Proof: Suppose that equation (4) has roots in F, but they are all repeated roots. Let one of these roots be of multiplicity m. We may assume, by renumbering the roots if necessary, that the first m numbers, f_i, are equal, that is $f_1 = f_2 = \cdots = f_m$. Let

$$H = \Gamma + s_2\Gamma + \cdots + s_m\Gamma .$$

H is a group, since it is obviously the set of all permutations that leave f_1 invariant. Since we have assumed that exactly m roots are equal, this function is not invariant under a permutation not in H. By theorem 5 the Galois group G of the polynomial must be contained in H.

We now consider the n! functions

$$g_1^{(j)} = r_1^{b_1} r_2^{b_2} \cdots r_{n-2}^{b_{n-2}} r_{n-1}^{b_{n-1}}, \quad (j = 1, 2, \cdots, n!),$$

where the b_i are integers and $0 \leq b_i \leq n - i$. By considering the successive adjunction to F of $r_1, r_2, \cdots, r_n$, in that order, it is clear that the totality of these functions form a basis (not necessarily minimal) for the root field of $p(x) = 0$. We now apply the fundamental theorem of Galois theory.

THEOREM 9.[2] [Fundamental theorem of Galois theory] If $p(x)$ is a polynomial in a field F and G the group of the equation $p(x) = 0$, where N is the root field of $p(x) = 0$, then:

(a) Each intermediate field B is the fixed field for a subgroup G_B of G, and distinct subgroups have distinct fixed fields. We say B and G_B "belong" to each other.

(b) For each intermediate field B, we have (B/F) equal the index of G_B and (N/B) equal the order of G_B.

Now, by the fundamental theorem, if Γ is a proper subgroup of G there is an intermediate field B belonging to Γ such that $B \supset F$ and B is a subfield of the root field of $p(x) = 0$. Since B is a subfield of the root field of $p(x) = 0$, and since the $g_1^{(j)}$ form a basis for the root field, any element in B must be a linear combination of the $g_1^{(j)}$. Let

---

[2]Emil Artin, Galois Theory (Ann Arbor: Edwards Brothers, Inc., 1942), p. 46.

(7) $$\bar{f}_1 = \sum_{j=1}^{n!} a_j g_1^{(j)}, \qquad (a_i \in F),$$

be such an element of B. Denote by $g_1^{(j)}, g_2^{(j)}, \cdots, g_h^{(j)}$ the h functions obtained by applying the h permutations of Γ to $g_1^{(j)}$. Let

$$\bar{f}_i = \sum_{j=1}^{n!} a_j g_i^{(j)}, \qquad (i = 1, 2, \cdots, h),$$

denote the h functions obtained from (7) by applying the h permutations of Γ. Since B belongs to Γ, any element of B is invariant under all of the permutations of Γ. Thus, we have $\bar{f}_1 = \bar{f}_2 = \cdots = \bar{f}_h$. If h is not a multiple of p, then: $\bar{f}_1 = \frac{1}{h}\left[\bar{f}_1 + \bar{f}_2 + \bar{f}_3 + \cdots + \bar{f}_h\right]$

$$= \frac{1}{h} \sum_{i=1}^{h} \bar{f}_i$$

$$= \frac{1}{h} \sum_{i=1}^{h} \left[\sum_{j=1}^{n!} a_j g_i^{(j)} \right]$$

$$= \sum_{i=1}^{n!} a_j \left\{ \frac{1}{h} \sum_{i=1}^{h} g_i^{(j)} \right\} .$$

If we define $f_1^{(j)} = \frac{1}{h} \sum_{i=1}^{h} g_i^{(j)}, \qquad (j = 1, 2, \cdots, n!)$, we shall have a basis for the field B. These $f_1^{(j)}$ must constitute a basis since $\bar{f}_1$ was any number in B and we have shown that it could be expressed in terms of the $f_1^{(j)}$. We have

defined $n!$ basis elements for a field of at most degree k over F, hence this is surely not a minimal basis. Furthermore, there is no implication that the $f_1^{(j)}$ are all distinct.

Since F is properly contained in B there must be at least one element in B which is not in F. Also, since all of the elements of B are linear combinations of the $f_1^{(j)}$, there must be at least one $f_1^{(j)}$ not in F. We now form the function

$$f_1(a) = \sum_{j=1}^{n!} a^{j-1} f_1^{(j)}, \tag{8}$$

where we are considering $\underline{a}$ as a parameter. $f_1(a)$ is invariant under the permutations of Γ, and any permutation not in Γ may change $f_1(a)$. Using $f_1(a)$ in lieu of the f_1 in (3) we can obtain, as before, the conjugate functions $f_i(a)$ and the induced equation which will now be dependent upon our choice of the parameter $\underline{a}$;

$$F(y,a) = \prod_{i=1}^{k} [y - f_i(a)] = 0,$$

where

$$f_1(a) = \sum_{j=1}^{n!} a^{j-1} \left\{ \frac{1}{h} \sum_{i=1}^{h} g_i^{(j)} \right\} .$$

The induced equation, of degree k in y, has coefficients symmetric in the roots of $p(x) = 0$, and hence for any value of $\underline{a} \in F$ the coefficients of $F(y,a) = 0$ are in F. We can

determine for any value of the parameter $\underline{a}$ whether or not this induced equation has a root in F. We now choose $\lceil k(n! - 1) + 1 \rceil$ distinct values in F, assuming that this is possible. If we let $\underline{a}$ take each of these values in turn we shall have $\lceil k(n! - 1) + 1 \rceil$ induced equations, one for each value of the parameter. If each of these induced equations has a root in F, then some one of the $f_i(a)$ must be a number in F for at least $\underline{n!}$ distinct values of $\underline{a}$ in F. Let a_ℓ, $(\ell = 1, 2, \cdots, n!)$, denote the n! distinct values $\underline{a}$ and b_ℓ, $(\ell = 1, 2, \cdots, n!)$, the corresponding values of the $f_i(a)$. From (8) we have the system of equations

$$(9) \qquad \sum_{j=1}^{n!} a_\ell^j - 1 f_i^{(j)} = b_\ell, \quad (\ell = 1, 2, \cdots, n!).$$

The coefficients of the $f_i^{(j)}$ in (9) form the Vandermonde determinant.

$$\begin{vmatrix} 1 & a_1 & a_1^2 & \cdots & a^{n!} - 1 \\ 1 & a_2 & a_2^2 & \cdots & a^{n!} - 1 \\ \cdot & \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdot & \cdots & \cdot \\ 1 & a_{n!} & a_{n!}^2 & \cdots & a_{n!}^{n!} - 1 \end{vmatrix} .$$

This determinant is known to be non-vanishing if the a_i are distinct. We have chosen the a_i distinct and from F, hence the value of the determinant is a number in F and is not zero. Since the b_ℓ are numbers in F, Cramer's rule gives

each of the $f_i^{(j)}$ as numbers in F. This implies that $B \equiv F$ and $G \subseteq \Gamma$ contrary to our assumption that Γ is properly contained in G. Thus, by assigning to $\underline{a}$ not more than $\lfloor k(n! - 1) + 1 \rfloor$ distinct values from F, we are assured of either finding an induced equation which has no root in F, or being able to conclude that $G \subseteq \Gamma$.

The finite field F may not contain $\lfloor k(n! - 1) + 1 \rfloor$ distinct elements. In this case it is necessary to extend F via a separable polynomial equation, $q(x) = 0$. We choose $q(x) = 0$, of degree $\underline{q}$ in x, such that the degree of $q(x)$ is greater than the degree of $p(x)$, and such that $p(x)$ and $q(x)$ are relatively prime. We also require that $q(x)$ have coefficients in F and be irreducible in F. Such an equation for any degree q is known[3] to exist. Let F_1 denote the root field of $q(x) = 0$ over F. Obviously $F \subset F_1$, since $q(x)$ is of degree greater than one, and $F \subseteq N$ where N is the root field of $p(x) = 0$ over F. We also have the relation $F_1 \cap N = F$ since the degree of $q(x)$ is greater than the degree of $p(x)$ and $q(x)$ was chosen to be irreducible. Since it is possible to choose the degree of $q(x) = 0$ as large as we please, we may choose it sufficiently large that F_1 will contain at least $\lfloor k(n! - 1) + 1 \rfloor$ distinct elements. As in the preceding argument, if we let $\underline{a}$ take

---

[3]L. E. Dickson, Linear Groups with an Exposition of the Galois Field Theory (Leipzig: B. G. Teubner, 1901), pp. 14-18.

each of these $\lfloor k(n! - 1) + 1 \rfloor$ distinct values in turn, we will obtain $\lfloor k(n! - 1) + 1 \rfloor$ induced equations. If each of these equations has a root in F_1, then some $f_i^{(j)}$ must be in F_1 for at least $\underline{n!}$ distinct values of $a \in F_1$. We again have the system (9) and Cramer's rule gives each of the $f_i^{(j)} \in F_1$. The $f_i^{(j)}$ are surely elements of N since they are functions of the roots of $p(x) = 0$, and N is the root field of $p(x) = 0$ over F. Since $F_1 \cap N = F$, each of the $f_i^{(j)} \in F$ and this again implies that $G \subseteq \Gamma$. As before, if $\underline{a}$ is assigned at most $\lfloor k(n! - 1) + 1 \rfloor$ distinct values from F_1 we are assured of either obtaining an induced equation which has no roots in F_1, or being able to conclude that $G \subseteq \Gamma$. If an induced equation has no roots in F_1, then it has no roots in F since $F \subseteq F_1$.

In view of the foregoing argument, it is clear that if h is not a multiple of p and if we make not more than $\lfloor k(n! - 1) + 1 \rfloor$ distinct choices of $a \in F$, or if necessary $a \in F_1$, one of the following must occur:

(a) We will obtain an induced equation, $F(y,a) = 0$, having no roots in F, or

(b) We will obtain an equation, $F(y,a) = 0$, having at least one non-repeated root in F, or

(c) Each of the equations, $F(y,a)$ has only multiple roots in which case we may conclude that $G \subseteq \Gamma$.

We have assumed throughout the proof of theorem 8 that h is not a multiple of p. If it happens that h is a

multiple of p it will be possible, in many cases, to avoid the use of theorem 8 by employing some special device suitable to the particular situation. Two such methods, translation of the roots of $p(x) = 0$ and setting up a different function satisfying theorem 6, are illustrated in the examples. In case the induced equation has only multiple roots and h is a multiple of p, and if it is impossible to find a device to avoid the use of theorem 8, the Galois group G can be determined by setting up the Galois resolvent and proceeding in the manner suggested by van der Waerden and Cajori.

Thus, with the single exception mentioned above, it is always possible either to apply the criteria given in theorem 7 to determine whether or not $G \subseteq \Gamma$, or else to conclude by theorem 8 that $G \subseteq \Gamma$.

CHAPTER IV

EXAMPLES

EXAMPLE 1. We shall first consider the case of the general cubic equation and later introduce numerical examples using the results obtained here. Now, it is well-known[1] that the Galois group of a polynomial equation with coefficients in a finite field is either cyclic of order n or a direct product of cyclic groups, according as the equation is irreducible or reducible. Using this fact, the problem of determining the Galois group in the case of the cubic equation is somewhat trivial; for, the Galois group is determined by the reducibility of the cubic equation, and to test for reducibility it is only necessary to determine whether or not the equation has a linear factor. However, the cubic equation adequately displays the method of this paper and we shall determine the Galois group without regard to reducibility.

Let $p(x) = 0$ be of the form

$$p(x) = x^3 + bx^2 + cx + d = 0.$$

There are four possibilities for the Galois group. They are as follows:

(a) S_3, the symmetric group of order six, defined by the permutations (1), (123), (132), (12), (13), (23).

(b) C_3, the cyclic group of order three, defined by the permutations (1), (123), (132).

---

[1] van der Waerden, op. cit., p. 191.

(c) S_2, the symmetric group of order two, which can be defined by the permutations (1), (12).

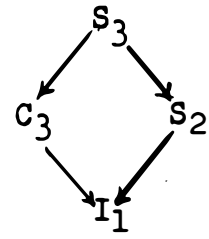
(d) I_1, the identity group, defined by the permutation (1).

It is clear, in view of our previous statement that G must be the cyclic group of order n or a direct product of cyclic groups, that G cannot equal S_3. G will equal I_1 if and only if $p(x) = 0$ is completely reducible in F. We include these two groups for the purpose of generality.

We have the relations

$$I_1 \subset S_2 \subset S_3$$
$$I_1 \subset C_3 \subset S_3$$

or, schematically



In order to completely solve the problem we need only make two choices for Γ . These are as follows:

(a) Let $\Gamma = C_3$. If $G \subseteq \Gamma$, then either $G = C_3$ or $G = I_1$. If $G \nsubseteq \Gamma$, then either $G = S_3$ or $G = S_2$.

(b) Let $\Gamma = S_2$. If $G \subseteq \Gamma$, then either $G = S_2$ or $G = I_1$. If $G \nsubseteq \Gamma$, then either $G = S_3$ or $G = C_3$.

If we find that $G \subseteq C_3$ but $G \nsubseteq S_2$, then $G = C_3$. If $G \subseteq C_3$ and $G \subseteq S_2$, then $G = I_1$, since $S_2 \cap C_3 = I_1$. If $G \nsubseteq C_3$ and $G \nsubseteq S_2$, then $G = S_3$. If $G \nsubseteq C_3$ but $G \subseteq S_2$, then $G = S_2$.

We shall first select $\Gamma = C_3$ and construct the induced equation as follows:

$$g_1(r_1, r_2, r_3) = r_1^2 r_2$$
$$g_2(r_1, r_2, r_3) = r_1 r_3^2$$
$$g_3(r_1, r_2, r_3) = r_2^2 r_3$$
$$f_1(r_1, r_2, r_3) = g_1 + g_2 + g_3 = r_1^2 r_2 + r_1 r_3^2 + r_2^2 r_3.$$

If t_2 is some permutation not in Γ, say (12), we have

$$t_2 f_1 = f_2 = r_1 r_2^2 + r_2 r_3^2 + r_1^2 r_3.$$

Γ and $t_2\Gamma$ exhaust S_3, hence we obtain only the two functions f_1 and f_2. We will not be concerned with multiple roots in this case, for if $f_1 = f_2$, then

$$r_1^2 r_2 + r_3^2 r_1 + r_2^2 r_3 = r_2^2 r_1 + r_3^2 r_2 + r_1^2 r_3$$

or

$$r_1^2 r_2 - r_2^2 r_1 + r_2^2 r_3 - r_3^2 r_2 + r_3^2 r_1 - r_1^2 r_3 = 0$$

and on factoring,

$$(r_1 - r_2)(r_1 - r_3)(r_2 - r_3) = 0. \tag{10}$$

Since we have assumed $p(x) = 0$ to be separable, no two roots can be equal and no factor in (10) can be zero. Hence, f_1 cannot equal f_2. The induced equation is

$$F(y) = \prod_{i=1}^{2} (y - f_i)$$
$$= y^2 - (f_1 + f_2)y + f_1 f_2 = 0.$$

Using direct computation and known[2] expressions for the symmetric functions we have

---

[2]L. Weisner, Introduction to the Theory of Equations (New York: The Macmillan Company, 1947), p. 114.

$$f_1 + f_2 = \Sigma r_1^2 r_2 = (\Sigma r_1)(\Sigma r_1 r_2) - 3\Sigma r_1 r_2 r_3 = 3d - bc.$$

$$f_1 f_2 = \Sigma r_1^3 r_2^3 + 3\Sigma r_1^2 r_2^2 r_3^2 + \Sigma r_1^4 r_2 r_3$$

$$= (\Sigma r_1^2 r_2^2)(\Sigma r_1 r_2) - (\Sigma r_1^3 r_2^2 r_3) + 3(\Sigma r_1^2 r_2^2 r_3^2)$$

$$+ (\Sigma r_1 r_2 r_3)(\Sigma r_1)$$

$$f_1 f_2 = c^3 + b^3 d + 9d^2 - 6bcd.$$

The induced equation with coefficients expressed in terms of the coefficients of $p(x) = 0$ is then

(11) $F(y) = y^2 - (3d - bc)y + (c^3 + b^3 d + 9d^2 - 6bcd) = 0.$

Now, choosing $\Gamma = S_2$, we have

$$g_1(r_1, r_2, r_3) = r_2^2 r_1$$

$$g_2(r_1, r_2, r_3) = r_1 r_2^2$$

$$f_1 = g_1 + g_2 = r_1^2 r_2 + r_1 r_2^2.$$

Let t_2 be any permutation not in Γ, say (13), and we have

$$t_2 f_1 = f_2 = r_3^2 r_2 + r_2^2 r_3.$$

Γ and $t_2\Gamma$ do not exhaust S_3 and there must be a t_3 in S_3 which is in neither Γ nor $t_2\Gamma$. One such t_3 is (23).

$$t_3 f_1 = f_3 = r_1^2 r_3 + r_2^2 r_1.$$

Γ, $t_2\Gamma$ and $t_3\Gamma$ exhaust S_3 and we have the three functions f_1, f_2 and f_3. We now investigate the possibilities of multiple roots in this case. Suppose that $f_1 = f_2$, then

$$r_1^2 r_2 + r_2 r_1 = r_1^2 r_3 + r_3 r_1^2$$

$$r_1 r_2 + r_2^2 = r_1 r_3 + r_3^2$$

$$r_1(r_2 - r_3) = -(r_2 - r_3)(r_2 + r_3)$$

$$(r_2 - r_3)(r_1 + r_2 + r_3) = 0.$$

Again r_3 cannot equal r_2 and we have multiple roots if and

only if $r_1 + r_2 + r_3 = 0$, that is, if $b = 0$. If $b = 0$ and if F is not of characteristic 3, it is possible to avoid the use of theorem 8 by using a translation of the roots of $p(x) = 0$. We need only let $x = z - 1$ and obtain a new equation $p(z-1) = 0$ in which $b \neq 0$. It is obvious that the group G of $p(z - 1) = 0$ is the same as the group G of $p(x) = 0$. It is then necessary to use theorem 8 only when $b = 0$ and F is of characteristic 3. The use of theorem 8 is illustrated in example 1-D. The induced equation is of the form

$$F(y) = \prod_{i=1}^{3} (y - f_1) = y^3 - (f_1 + f_2 + f_3)y^2$$

$$+ (f_1f_2 + f_1f_3 + f_2f_3)y + f_1f_2f_3 = 0.$$

Using methods similar to those used in obtaining (11), the induced equation becomes

$$(12) \qquad F(y) = y^3 - (3d - bc)y^2 + (3d^2 + b^3d - 2bcd)y$$

$$- (d^3 - bcd) = 0.$$

If $b = 0$, (12) becomes

$$F(y) = y^3 - 3dy^2 + 3d^2y - d^3 = (y - d)^3 = 0.$$

It is readily seen that if $b = 0$ all three roots of the induced equation are equal to d.

We now seek to determine the Galois groups of certain numerical examples applying the results of (11) and (12).

EXAMPLE 1-A. Let $p(x) = x^3 + x^2 + x + 3 = 0$, where F is the field $GF(5)$. Choosing $\Gamma = C_3$ and using (11) we have

$$F(y) = y^2 + 2y + 2 = 0.$$

This equation has the roots $y = 1$ and $y = 2$. By theorem 7, $G \subseteq C_3$. If we choose $\Gamma = S_2$ and use (12), the induced equation becomes

$$F(y) = y^3 + 2y^2 + 4y + 2 = 0.$$

This equation has no roots in F which implies that $G \not\subseteq S_2$. We must have $G = C_3$. This result is in agreement with our statement that G is cyclic of order n if $p(x) = 0$ is irreducible, since it is easily shown that the $p(x) = 0$ in this example is irreducible in $GF(5)$.

EXAMPLE 1-B. Let $p(x) = x^3 + x^2 + x + 1 = 0$, where F is the field $GF(3)$. If $\Gamma = C_3$, we obtain from (11)

$$F(y) = y^2 + 2y + 2 = 0.$$

This equation has no roots in F, hence $G \not\subseteq C_3$. If $\Gamma = S_2$, then by (12): $F(y) = y^3 + y^2 + 2y = 0$.

This equation has the non-repeated root $y = 0$. This implies that $G \subseteq S_2$. $G = S_2$, since $G \not\subseteq C_3$. It can be readily shown that $p(x) = 0$ has the one linear factor $x + 1$.

EXAMPLE 1-C. Let $p(x) = x^3 + x + 1 = 0$, where F is the field $GF(7)$. If $\Gamma = C_3$, then

$$F(y) = y^2 + 4y + 3 = 0.$$

This equation has the roots $y = 4$ and $y = 6$, hence $G \subseteq C_3$. If $\Gamma = S_2$ the equation (12) will always have multiple roots since $b = 0$. Using the translation suggested previously, we let $x = z - 1$ and the equation under consideration becomes

$$z^3 + 4z^2 + 4z + 6 = 0.$$

Using (12) the induced equation is

$$F(y) = y^3 + 5y^2 + 6y + 6 = 0.$$

This equation has no roots in F, hence $G \not\subseteq S_2$ and we must have $G = C_3$. One may readily verify the fact that $p(x) = 0$ is irreducible in $GF(7)$.

EXAMPLE 1-D. We now consider the cubic equation which has $b = 0$ and where F is GF(3). Choosing $\Gamma = S_2$ and using the method of theorem 7, we will always obtain multiple roots. As was pointed out in example 1, a translation of the roots is not sufficient in this case. We apply the methods of theorem 8 to obtain an induced equation which is dependent upon a parameter. Let the cubic equation be of the form

$$p(x) = x^3 + cx + d = 0$$

and let F be GF(3). Choosing $\Gamma = S_2$, we have

$$g_i^{(j)} = r_1^{\alpha_1} r_2^{\alpha_2}, \quad 0 \le \alpha_i \le 2, \quad (j = 1,2,3,4,5,6),$$

$$\left.\begin{aligned} g_1^{(1)} &= r_1^2 \\ g_1^{(2)} &= r_1 r_2 \\ g_1^{(3)} &= r_1 \\ g_1^{(4)} &= r_2 \\ g_1^{(5)} &= r_1^2 r_2 \\ g_1^{(6)} &= 1 \end{aligned}\right\} g_1^{(j)} \qquad \left.\begin{aligned} g_2^{(1)} &= r_2^2 \\ g_2^{(2)} &= r_1 r_2 \\ g_2^{(3)} &= r_2 \\ g_2^{(4)} &= r_1 \\ g_2^{(5)} &= r_1 r_2^2 \\ g_2^{(6)} &= 1 \end{aligned}\right\} g_2^{(j)}$$

$$f_1^{(j)} = \tfrac{1}{2} \sum_{i=1}^{2} g_i^{(j)} = 2 \sum_{i=1}^{2} g_i^{(j)}, \quad (j = 1,2,3,4,5,6).$$

Using the fact that $r_1 + r_2 + r_3 = 0$ and known expressions for the symmetric functions, we have

$$f_1^{(1)} = 2(r_1^2 + r_2^2) = 2c + r_3^2,$$

$$f_1^{(2)} = 2(2r_1 r_2) = \frac{d}{r_3},$$

$$f_1^{(3)} = 2(r_1 + r_2) = r_3,$$

$$f_1^{(4)} = 2(r_1 + r_2) = r_3,$$

$$f_1^{(5)} = 2(r_1^2 r_2 + r_1 r_2^2) = 2r_1 r_2(r_1 + r_2) = d,$$

$$f_1^{(6)} = 1.$$

Now, $f_1^{(3)} \equiv f_1^{(4)}$, $f_1^{(5)} \in F$ and $f_1^{(6)} \in F$. Since we are interested in forming an intermediate field B over F, we need not consider the functions $f_1^{(4)}$, $f_1^{(5)}$ and $f_1^{(6)}$ in setting up the induced equation. We define $f_1(a)$ as follows:

$$f_1(a) = \sum_{j=1}^{3} a^{j-1} f_1^{(j)}$$

$$= 2(r_1^2 + r_2^2) + (r_1 r_2)a + (r_1 + r_2)a^2$$

$$= 2c + r_3^2 + \frac{da}{r_3} + r_3 a^2.$$

It is obvious that $f_1(a)$ is invariant under the permutations, (1), (12), of Γ and any permutation not in Γ will change $f_1(a)$. Choosing $t_2 = (13)$ and $t_3 = (23)$, we obtain the conjugate functions

$$f_2(a) = 2c + r_1^2 + \frac{da}{r_1} + r_1 a^2$$

$$f_3(a) = 2c + r_2^2 + \frac{da}{r_2} + r_2 a^2.$$

The induced equation is

$$F(y,a) = \prod_{i=1}^{3} [y - f_i(a)]$$

$$= [y + 2(2c + r_3^2 + \frac{da}{r_3} + r_3 a^2)]$$
$$[y + 2(2c + r_1^2 + \frac{da}{r_1} + r_1 a^2)]$$
$$[y + 2(2c + r_2^2 + \frac{da}{r_2} + r_2 a^2)] = 0.$$

Expanding and applying known expressions for the symmetric functions, we obtain

$$(13) \qquad F(y,a) = y^3 + 2c(a+1)y^2 + c(a^4+2c)y + \lfloor da^6 + 2c^2a^5 + c(c+d)a^4 + 2d(c+1)a^3 + (cd)a^2 + (2c^3)a + (c^3+2d^2)\rfloor = 0.$$

Equation (13) is dependent upon a parameter $\underline{a}$ and we can determine, for any value of the parameter, whether or not this equation has roots in F. In general it would be necessary to choose $\lfloor k(n!-1)+1\rfloor = \lfloor 3(6-1)+1\rfloor = 16$ values for $\underline{a}$ to be assured of obtaining positive results. However, in this case all that is necessary is to choose $\lfloor 3(3-1)+1\rfloor = 7$ values for $\underline{a}$, since in setting up the induced equation we used only the three functions $f_1^{(1)}$, $f_1^{(2)}$ and $f_1^{(3)}$. Thus, in not more than seven distinct choices for $\underline{a}$ we are assured of being able to determine whether or not $G \subseteq \Gamma$.

Consider the numerical example

$$p(x) = x^3 + 2x + 1 = 0,$$

where F is $GF(3)$. It is sufficient to choose $q(\lambda) = \lambda^2 + 1 = 0$, since the field F_1 would then contain the <u>nine</u> elements $0, 1, 2, \lambda, 2\lambda, 1+\lambda, 1+2\lambda, 2+\lambda, 2+2\lambda$, where we are denoting the roots of $q(\lambda) = 0$ by λ and 2λ. In the proof of theorem 8 it was convenient to require that the degree of $q(x)$ be greater than the degree of $p(x)$, which obviously is not the case here. Our reason for placing this requirement on the degree of $q(x)$ was to insure the fact that $F_1 \cap N = F$. This relation surely holds here since F_1 and N have only the elements $0, 1, 2$ in common. Using (13) the induced equation becomes

$$F(y,a) = y^3 + (a+1)y^2 + 2(a^4+1)y + (a^6 + 2a^5 + 2a^2 + a + 1) = 0.$$

Choosing $a = 0 \in F_1$, we have

$$F(y,0) = y^3 + y^2 + 2y + 1 = 0.$$

This equation has no roots in F_1 and we may conclude that $G \not\subseteq S_2$. By using (11) it is easily shown that $G \subseteq C_3$, hence $G = C_3$.

As another example, let

$$p(x) = x^3 + x + 1 = 0,$$

where again F is $GF(3)$. Using (13) we obtain

$$F(y,a) = y^3 + 2(a+1)y^2 + (a^4+2)y + (a^6 + 2a^5 + 2a^4 + a^3 + a^2 + 2a) = 0.$$

It is again sufficient to choose $q(\lambda) = \lambda^2 + 1 = 0$.

If $\underline{a} = 1$, we have

$$F(y,1) = y^3 + y^2 = 0.$$

This equation has the non-repeated root $y = 2$, hence $G \subsetneq S_2$. Using (11), it is readily shown that $G \not\subseteq C_3$, hence $G = S_2$.

EXAMPLE 1-E. In forming the function satisfying theorem 6, we mentioned the fact that there were other ways of forming this function. In many cases a simpler function can be obtained, and in some cases it is possible to avoid the problem of multiple roots, and a subsequent use of theorem 8, by properly choosing this function. To illustrate this fact we wish to show that it is possible to avoid the use of theorem 8 in the case of the cubic equation as was necessary in example 1-D.

Let

$$p(x) = x^3 + bx^2 + cx + d = 0,$$

and let $\Gamma = S_2$, and define f_1 as follows:

$$f_1 = r_1 + r_2.$$

Assuming that S_2 is again defined by the permutations (1) and (12), it is readily seen that f_1 is invariant under the permutations of Γ, and any permutation not in Γ will change f_1. We obtain the conjugate functions

$$f_2 = r_1 + r_3$$

$$f_3 = r_2 + r_3.$$

In this case no two roots of the induced equation can be equal, for if $f_1 = f_2$, we have

$$r_1 + r_2 = r_1 + r_3$$

and

$$r_2 = r_3.$$

This is contrary to our assumption that $p(x) = 0$ is a separable equation. Hence, $f_1 \neq f_2$ and in a similar manner $f_1 \neq f_3$ and $f_2 \neq f_3$. The induced equation is

$$F(y) = \prod_{i=1}^{3}(y - f_i)$$

$$= [y - (r_1 + r_2)][y - (r_1 + r_3)][y - (r_2 + r_3)]$$

$$= y^3 - 2by^2 + (b^2 + c)y + (d - bc) = 0.$$

Consider one of the numerical examples of example 1-D, that is,

$$p(x) = x^3 + 2x + 1 = 0,$$

where F is GF(3). The induced equation is

$$F(y) = y^3 + 2y + 1 = 0.$$

This equation has no roots in F, hence $G \not\leq S_2$. Choosing $\Gamma = C_3$ and using (11), we have $G \leq C_3$, hence $G = C_3$. This is in agreement with the conclusion reached in example 1-D.

EXAMPLE 2. We now investigate the problem of determining the Galois group of the quartic equation. No attempt will be made to give a complete analysis, as was done in the case of the cubic equation. However, we wish to show that the determination of G can be made dependent upon the determination of the linear factors of a single equation. Let the quartic equation be of the form

$$p(x) = x^4 + ax^3 + bx^2 + cx + d = 0.$$

Using the fact that G is either cyclic of order n or a direct product of cyclic groups, depending upon whether or not $p(x) = 0$ is irreducible, we have the following:

1. If $p(x) = 0$ is completely reducible in F, then G is simply the identity group, I_1.

2. If $p(x) = 0$ has one and only one linear factor in F, then $G = C_3$, the cyclic group of order three.

3. If $p(x) = 0$ has just two linear factors in F, then G is the cyclic group of order two, C_2.

4. If $p(x) = 0$ has no linear factors in F, then either $p(x) = 0$ is irreducible in F in which case $G = C_4$, the cyclic group of order four, or $p(x) = 0$ has two quadratic

factors irreducible in F in which case $G = C_2 \times C_2 = V_4$, the four group.

Since the problem is readily solved in the first three cases by determining the roots of $p(x) = 0$ which are in F, we shall consider case 4 where $p(x) = 0$ has no linear factors in F. It will be sufficient to determine whether or not $G \subseteq V_4$. If $G \subseteq V_4$, and if $p(x) = 0$ has no linear factors in F, then $G = V_4$. If $G \not\subseteq V_4$, and if $p(x) = 0$ has no linear factors in F, then $G = C_4$.

Choosing $\Gamma = V_4$, where V_4 is defined by the permutations (1), (12)(34), (13)(24), (14)(23), we proceed to set up the induced equation by defining $f_1(r_1, r_2, r_3, r_4)$ as follows:

$$f_1(r_1, r_2, r_3, r_4) = r_1r_2 + r_3r_4 - r_1r_3 - r_2r_4.$$

We have defined a function satisfying theorem 6 in a manner different from that suggested in Chapter III in order to obtain a function of lower degree. As before, we obtain the conjugate functions

$$f_2 = r_1r_3 + r_2r_4 - r_1r_2 - r_3r_4 = -f_1$$
$$f_3 = r_1r_2 + r_3r_4 - r_1r_4 - r_2r_3$$
$$f_4 = r_1r_4 + r_2r_3 - r_1r_2 - r_3r_4 = -f_3$$
$$f_5 = r_1r_3 + r_2r_4 - r_1r_4 - r_2r_3$$
$$f_6 = r_1r_4 + r_2r_3 - r_1r_3 - r_2r_4 = -f_5.$$

We now investigate the possibility of multiple roots. f_1 is not zero, for if

$$f_1 = r_1r_2 + r_3r_4 - r_1r_3 - r_2r_4 = 0$$
$$(r_1r_2 - r_1r_3) - (r_2r_4 - r_3r_4) = 0$$
$$(r_1 - r_4)(r_2 - r_3) = 0.$$

Since neither of these factors can be zero, $f_1 \neq 0$. In a similar fashion it can be shown that none of the conjugate functions, f_i, can equal zero. If the characteristic, p, of F is not two, then $f_1 \neq f_2$, for if

$$f_1 = f_2,$$

we have

$$f_1 = -f_1,$$

and since $f_1 \neq 0$ this is impossible. Similarly, $f_3 \neq f_4$ and $f_5 \neq f_6$. The function f_1 is distinct from f_3 and f_6 since we have the relations $f_1 - f_3 = f_6$ and $f_1 - f_6 = f_3$, and neither f_3 nor f_6 is zero. All the permutations that take f_1 into f_4 and f_5 are even, hence if two of these functions are equal all three must be equal. This is true because the permutations under which f_1 is left invariant form a group, since the product would still leave the function invariant, and since we would also have the inverse permutation present; but, if only two of these functions are equal, we have a set of eight permutations, all of which are even, and such a set cannot form a group which is a subgroup of the symmetric group of degree four. Hence, this case is not possible. The only remaining possibility for multiple roots is for $f_1 = f_4 = f_5$. Since $f_1 = f_4$, we have

(14) $r_1r_2 + r_3r_4 - r_1r_3 - r_2r_4 = r_1r_4 + r_2r_3 - r_1r_2 - r_3r_4,$

and since $f_1 = f_5$, we have

(15) $r_1r_2 + r_3r_4 - r_1r_3 - r_2r_4 = r_1r_3 + r_2r_4 - r_1r_4 - r_2r_3$.

Adding (14) and (15), we obtain

$$2r_1r_2 + 2r_3r_4 - 2r_1r_3 - 2r_2r_4 = r_1r_3 + r_2r_4 - r_1r_2 - r_3r_4,$$

and

$$3r_1r_2 + 3r_3r_4 - 3r_1r_3 - 3r_2r_4 = 0.$$

Upon factoring this last expression, we have

$$3(r_1 - r_4)(r_2 - r_3) = 0.$$

Since no two roots can be equal, this relation cannot hold unless the characteristic, p, of F is three, hence these three functions cannot be a triple root unless $p = 3$. If $p = 3$, then by multiplying (14) by 2, we have

(16) $$2(r_1r_2 + r_3r_4) + (r_1r_3 + r_2r_4)$$
$$= 2(r_1r_4 + r_2r_3) + (r_1r_2 + r_3r_4).$$

Adding (15) and (16), we obtain

$$(r_1r_4 + r_2r_3) + (r_1r_2 + r_3r_4) + (r_1r_3 + r_2r_4) = 0.$$

This implies that we have multiple roots if and only if $b = 0$. A translation of the roots in this case is not sufficient to avoid the use of theorem 8. Theorem 8 can be used since $h = 4$ is not a multiple of $p = 3$.

The induced equation is

$$F(y) = \prod_{i=1}^{6} (y - f_i) = 0.$$

Again, using the symmetric functions this equation becomes

$$(17)\quad F(y) = y^6 - (2b^2 - 6ac + 24d)y^4$$
$$+ (b^4 + 9a^2c^2 + 144d^2 - 6ab^2c + 24b^2d - 72acd)y^2$$
$$- (256d^3 - 192acd^2 - 128b^2d^2 + 144bc^2d - 27c^4$$
$$+ 144a^2bd^2 - 6a^2c^2d - 80ab^2cd + 16b^4d + 18abc^3$$
$$- 4b^3c^2 - 27a^4d^4 + 18a^3bcd - 4a^2b^3d - 4a^3c^3$$
$$+ a^2b^2c^2d^2) = 0.$$

EXAMPLE 2-A. As an example of the discussion above, consider

$$p(x) = x^4 + 2x^3 + 3x^2 + 4x + 2 = 0,$$

where F is $GF(5)$. It is readily shown that $p(x) = 0$ has no linear factors in F, hence either $G = C_4$ or $G = V_4$. Choosing $\Gamma = V_4$ and using (17) the induced equation is

$$F(y) = y^6 + 2y^4 + y^2 + 1 = 0.$$

This equation has the non-repeated root $y = 1$, hence $G \subseteq V_4$, and since $p(x) = 0$ has no linear factors in F, $G = V_4$.

EXAMPLE 2-B. Let

$$p(x) = x^4 + 2x^3 + 2x^2 + x + 2 = 0,$$

where F is $GF(7)$. Again $p(x) = 0$ has no linear factors in F, and G must either be C_4 or V_4. If $\Gamma = V_4$, we have from (17)

$$F(y) = y^6 + 5y^4 + y^2 + 2 = 0,$$

which has no roots in F, hence $G \not\subseteq V_4$. $G = C_4$, since $p(x) = 0$ has no linear factors in F.

CHAPTER V

SUMMARY

In summary, it is possible to determine the Galois group of a separable polynomial equation over a finite field, without regard to reducibility, in the following manner:

1. Determine all of the subgroups of the symmetric group, S_n. G must be one of these subgroups or S_n itself. Since we know that G must be either cyclic or a direct product of cyclic groups, it will be possible in actual practice to rule out certain subgroups, and perhaps S_n, as possibilities for G.

2. Test each of the subgroups which may be G by constructing the induced equation and then applying the criteria given in theorem 7 to determine whether or not the subgroup tested contains G.

3. If G is contained in one of the selected subgroups, Γ, but is contained in no subgroup of Γ, then $G = \Gamma$.

The method of this thesis is a constructive method whereby one can determine the Galois group, although, as was pointed out in Chapter IV, this may not be the simplest manner in which the problem may be solved. In the case of the finite field it is only necessary to determine the irreducible factors of the polynomial under consideration. However, in cases of higher degree this is often a difficult problem. The method given here reduces the problem of reducibility to that of

determining a linear factor. Another advantage is that once the general induced equation has been constructed, the application to special cases is immediate.

We have used the symmetric functions in computing the coefficients of the induced equation. At times it may be more convenient to use some other method to determine these coefficients. As at least one alternative method, Wilson[1] illustrates the use of matrices employing the characteristic equation. We would again emphasize that the methods discussed here can be used to a greater advantage by utilizing all known facts in a particular situation.

---

[1]R. L. Wilson, op. cit.

BIBLIOGRAPHY

BIBLIOGRAPHY

Albert, A. A. Modern Higher Algebra. Chicago: The University of Chicago Press, 1937.

Artin, Emil. Galois Theory. Ann Arbor: Edwards Brothers, Inc., 1942.

Birkhoff, G., and MacLane, S. A Survey of Modern Algebra. New York: The Macmillan Company, 1948.

Cajori, F. An Introduction to the Modern Theory of Equations. New York: The Macmillan Company, 1904.

Carmichael, R. D. Introduction to the Theory of Groups of Finite Order. Boston: Ginn and Company, 1937.

Dickson, L. E. Linear Groups with an Exposition of the Galois Field Theory. Leipzig: B. G. Teubner, 1901.

MacDuffee, C. C. An Introduction to Abstract Algebra. New York: John Wiley and Sons, Inc., 1940.

van der Waerden, B. L. Modern Algebra. New York: Frederick Ungar Publishing Company, 1949.

Weisner, L. Introduction to the Theory of Equations. New York: The Macmillan Company, 1947.

Wilson, R. L. "A Method for the Determination of the Galois Group." To appear soon in the Duke Mathematical Journal.