THE DETERMINATION OF THE GALOIS GROUP OVER A FINITE FIELD

CHARLES L. BRADSHAW
Tennessee Polytechnic Institute, Cookeville, Tennessee

1. Introduction. The primary purpose of this paper 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 determining the Galois group of an arbitrary equation, where the coefficient field is either finite or infinite, is neither new nor unsolved. Wilson (1950) completely solves the problem in the case of the infinite field. The method of this paper follows that of his in so far as is possible. The author wishes to thank Professor Wilson for his aid in the preparation of this paper.

The method of this paper is to determine successively whether the Galois group is or is not contained in each of the subgroups of the symmetric group of degree equal to the degree of the given equation. 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 subroup contains the Galois group but has no subgroup containing the Galois group.

2. Notation. We shall assume that the polynomial under consideration is of the form

$$p(x) = x^n + a_1x^{n-1} + \ldots + a_n = 0 \tag{1}$$

where the coefficients a_i are numbers in a finite field F. We also 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 (van der Waerden, 1949, p. 189) that any irreducible equation over a Galois field is separable. However, we shall make no assumption regarding the reducibility of the polynomial under consideration.

We shall denote by Γ an arbitrary subgroup of the symmetric group, S_n, n being the degree of the given polynomial. 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.

We shall denote n indeterminants by $x_1, x_2, \ldots, x_n$ and in a similar manner the roots of $p(x) = 0$ shall be denoted by $r_1, r_2, \ldots, r_n$ 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 separable.

3. Determination of G. 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 $f_1(x_1, x_2, \ldots, x_n)$ of the n indeterminants with coefficients in F, which is invariant under the permutations of Γ but under no permutation not in Γ. If this is possible, and if $f_1(r_1, r_2, \ldots, r_n)$ is a number in F and distinct from all the numbers obtained by applying to $f_1(r_1, r_2, \ldots, r_n)$ permutations outside Γ, we apply the following theorem:

THEOREM 1. (MacDuffee, 1940, p. 102) 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 in 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 $f_1(x_1, x_2, \ldots, x_n)$ with coefficients in F, which is invariant under Γ, but under no permutations not in Γ, and

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

We proceed as follows to set up an equation, called the induced equation. Define

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

and define $g_i(x_1, x_2, \ldots, x_n)$, $(i = 1, 2, \ldots, h)$, as the h functions obtained from $g_1(x_1, x_2, \ldots, x_n)$ by performing each of the h permutations of Γ upon the x_i. Define

(3) $$f_1(x_1, x_2, \ldots, x_n) = \sum_{i=1}^{h} g_i(x_1, x_2, \ldots, x_n).$$

Any permutation of Γ will leave f_1 invariant and any permutation not in Γ will change f_1 into some other rational function of the n indeterminants with coefficients in F. We say that this second function is conjugate to f_1. Hence, f_1 is invariant under the permutations of Γ, but is altered by any permutation not in Γ.

By using all of the permutations of S_n, we obtain k functions f_i $(i = 1, 2, \ldots, k)$ where $k = n/h$. It can be shown that the f_i are distinct.

Define the induced equation as follows:

(4) $$\theta(y) = \prod_{i=1}^{K} [y - f_i(r_1, r_2, \ldots, r_n)] .$$

The function (3) are not necessarily the only functions of n indeterminants invariant under precisely the permutations of Γ, hence the induced equation is not necessarily unique. In some cases this may not produce the simplest equation induced by Γ, but it does give at least one method for obtaining an induced equation.

The following theorem is proved by Wilson (1950):

THEOREM 2. If the equation induced by Γ has no roots in F, then the Galois group G is not contained in Γ. If the equation induced by Γ has at least one non-repeated root in F, then G is either Γ, or a subgroup of Γ.

If the equation (4) has only multiple roots in F, no inference may be drawn, since the functions $f_i(r_1, r_2, \ldots, r_n)$ are then invariant under Γ, but also under permutations not in Γ.

We now prove the following theorem:

THEOREM 3. 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, where p is the characteristic of the finite field) 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: Consider the n! functions

$$g_1^{(j)} = r_1^{b_1} r_2^{b_2} \cdots r_{n-1}^{b_{n-1}} \qquad (j = 1, 2, \ldots, n!) \tag{5}$$

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

$$\bar{f}_1 = \sum_{j=1}^{n!} a_j g_1^{(j)}, \qquad (a_i \in F) \tag{6}$$

be such an element of B. Denote by $g_i^{(j)}$ (i = 1, 2, ..., h) the h functions obtained by applying the h permutations of Γ to $g_1^{(j)}$. Let

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

denote the h functions obtained from (6) by applying the h permutations of Γ. Since B is the fixed field for Γ, $\bar{f}_1 = \bar{f}_2 = \ldots = \bar{f}_h$.

If h is not a multiple of p, then $\bar{f}_1 = 1/h(\bar{f}_1 + \bar{f}_2 + \ldots + \bar{f}_h)$

$$\bar{f}_1 = 1/h \sum_{i=1}^{h} \bar{f}_i = 1/h \sum_{i=1}^{h} \left[\left(\sum_{j=1}^{n!} a_j g_i^{(j)} \right) \right]$$

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

If we define $f_1^{(j)} = 1/h \sum_{i=1}^{h} g_i^{(j)}$ (j = 1, 2, ..., n!) we shall have a basis for 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 $F \subset B$ 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

$$f_1(a) = \sum_{j=1}^{n!} a^{j-1} f_1^{(j)} \tag{7}$$

where a is a parameter. Using (7) in lieu of (3) we can obtain as before the conjugate functions $f_i(a)$ and the induced equation which will now be dependent on our choice of the parameter a;

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

We choose $k(n! - 1) + 1$ distinct values in F, assuming that this is possible. If we let a take each of these values in turn we shall have $k(n! - 1) + 1$ 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 n! distinct values of a in F. Let a_ℓ ($\ell = 1, 2, \ldots, n!$), denote the n! distinct values a and b_ℓ ($\ell = 1, 2, \ldots, n!$), the corresponding values of the $f_i(a)$. From (7) we have the system

$$\sum_{j=1}^{n!} a^{j-1} f_i^{(j)} = b_\ell \qquad (\ell = 1, 2, \ldots, n!) \tag{8}$$

The coefficients $f_i^{(j)}$ in (8) form the Vandermonde determinant, and, hence is non-vanishing. 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 the assumption that Γ is properly contained in G. Thus, by assigning to a not more than $k(n! - 1) + 1$ distinct values from F, we are assured of either finding an induced equation which has no roots in F, or being able to conclude that $G \subseteq \Gamma$.

The finite field F may not contain $k(n! - 1) + 1$ distinct elements. In this case it is necessary to extend F via a separable polynomial equation, $q(x) = 0$, of degree q in x, such that the degree of $q(x)$ and $p(x)$ are relatively prime. We also require that $q(x)$ have coefficients in F and be irreducible in F. Such and equation for any

degree q is known (Dickson, 1901, pp. 14-18) 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 $q(x)$ 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 $k(n! - 1) + 1$ distinct elements. As in the preceding argument, if we let a take each of these $k(n! - 1) + 1$ distinct values in turn, we will obtain $k(n!-1)+1$ 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 $n!$ distinct values of $a \in F_1$. We again have the system (8) 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 a is assigned at most $k(n! - 1) + 1$ 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 $F \subseteq F_1$.

4. An Example. In the case of the cubic equation $p(x) = x^3+bx^2+cx+d=0$ we have four possibilities for G; namely, the symmetric group of order three, S_3, the cyclic group C_3, the symmetric group of order two, S_2, and the identity group, I. We have the following inclusions:

$$S_3 \supset C_3 \supset I$$

$$S_3 \supset C_2 \supset I$$

It is clear that we need make only two choices for Γ. Those are C_3 and S_2. If $\Gamma = C_3$, we have,

$$f_1 = r_1^2 r_2 + r_1 r_3^2 + r_2^2 r_3$$

$$f_2 = r_1 r_2^2 + r_2 r_3^2 + r_1^2 r_3$$

and the induced equation

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

It can readily be shown that multiple roots cannot occur in this case. Using the symmetric function, we have,

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

If $\Gamma = S_2$, the induced equation is

$$f(y) = y^3 - (3d - bc)y^2 + (3d^2 + b^3d - 2bcd)y - (d^3 - bcd) = 0$$

If $b=0$, we have $f(y) = (y-d)^3 = 0$ and all three roots are equal to d. The equation has multiple roots in this case only. A translation of the roots or an application of theorem 3 will work in this case.

5. Summary. The method of this paper is a constructive method whereby one can determine the Galois group, although this may not be the simplest manner in which the problem can 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 as given here reduces the problem of reducibility to that of determining a linear factor.

Bibliography

Dickson, L. E. 1901. *Linear groups with an exposition of the Galois field theory.* B. G. Teubner, Leipzig.

MacDuffee, C. C. 1940. *An introduction to abstract algebra.* John Wiley and Sons, Inc., New York.

van der Waerden, B. L. 1949. *Modern algebra.* Frederick Ungar Publishing Company, New York.

Wilson, R. L. 1950. A method for the determination of the Galois group. *Duke Math. Jour.* 17.

NEWS OF TENNESSEE SCIENCE

(Continued from page 200)

Stern, Thomas N., V. V. Cole, Anne C. Bass, and R. R. Overman (Univ. of Tenn., Memphis). 1951. Dynamic aspects of sodium metabolism in experimental adrenal insufficiency using radioactive sodium. *Amer. Jour. Physiol.*, 164(2) : 437-449. Feb.

Straub, Conrad P. (ORNL). 1951. Observations on the removal of radioactive materials from waste solutions. *Sewage and Indus. Wastes,* 23(2) : 188-193. Feb.

Yambert, D. W. (T. V. A.). 1950. Geese on Hiwassee Island. *Migrant,* 21(1) : 1-3. Mar.

RECENT PUBLICATIONS WITH REFERENCE TO TENNESSEE OR TO TENNESSEE MATERIAL

Stevenson, H. M. 1950. Distribution of certain birds in the Southeastern United States. *Amer. Midl. Nat.,* 43(3) : 605-626. May. Compilation includes many Tenn. records.

Stevenson, H. M., and T. A. Imhof. 1950. The fall migration in the Tennessee River in Alabama. *Migrant,* 21(1) : 3-9. Mar.