A METHOD FOR THE DETERMINATION OF THE GALOIS GROUP

By R. L. Wilson

1. **Introduction.** The problem of determining the Galois group of an equation is neither new nor unsolved. A general method of forming the Galois resolvent of an equation, and then testing the resolvent for irreducibility is mentioned by Cajori [4; 169–170]. Berwick [2], [3] presented a more direct method in certain cases. The converse problem of obtaining all equations which have a given group as their Galois group was discussed in general terms by E. Noether [9]. Seidelmann [10] gave in parametric form the equations of the third and fourth degree corresponding to each possible Galois group. Later, Garver [5] obtained some of these same results using the Tschirnhaus transformation, with the remark that his method might prove to be more feasible than that of Seidelmann in cases of higher degree. A simpler solution was given for certain cases by Lester [7], and, finally, Hull [6] obtained a result for the cyclic quintic, dependent upon the solution of certain diophantine equations.

It is the purpose of this paper to demonstrate a method for the determination of the Galois group of a polynomial equation which is dependent only upon the determination of all of the rational 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 equal to the degree of the given equation. This information permits the use of a sieve process to determine which of the subgroups of the symmetric group is the Galois group, or whether the Galois group is the symmetric group itself.

The author wishes to thank Professors C. C. MacDuffee and G. W. Whaples for their aid and direction in the preparation of this paper.

2. **Notation.** We shall assume throughout this paper that the equation under consideration is of the form

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

where the coefficients a_i are numbers in a separable field F. It is clearly no restriction to require that each equation be in the above form. We shall denote by G the Galois group of (1) relative to F, and by Γ we shall denote an arbitrary subgroup of the symmetric group of degree n. Γ can be any one of these subgroups, but having been chosen, we shall require Γ to be a fixed group. We shall consider both G and Γ to be permutation groups on n symbols.

By $x_1, x_2, \cdots, x_n$ we shall designate n indeterminates. Similarly, we shall denote the roots of $p(x) = 0$ by $r_1, r_2, \cdots, r_n$.

Received May 14, 1949. Presented to the American Mathematical Society at the meeting in Chicago, April 1947.