STICHTING
MATHEMATISCH CENTRUM
2e BOERHAAVESTRAAT 49
AMSTERDAM

AFDELING ZUIVERE WISKUNDE

ZW 1964-007

An algebraic application of the wreath product

by

W. Kuyk

This work has been done during the time that the author was a Postdoctorate Fellow of the National Research Council.

1. Introduction

This paper is concerned with the following problem. Let L be a finite galoisian field extension of a field K, with Galois group B. Let furthermore M be a finite galoisian field extension of L with Galois group A. Then the Galois group G of M/K — i.e. the Galois group of the least normal field extension N of K containing M — is completely determined by the given extensions.

Our problem is to determine the set S(B,A) of all possible Galois groups of M/K that may occur if arbitrary extensions L of arbitrary fields K and arbitrary extensions M of L, with Galois groups B and A, respectively, are considered.

In fact, we prove:

Theorem. Let A and B be two given finite groups. Then any element G of S(B,A) can be obtained as a subgroup of the wreath product $A \wr B$ of A and B. $A \wr B$ is itself an element of S(B,A).

From the theorem it follows immediately that $A \wr B$ is the group with the least possible order satisfying the property that it contains a copy of each $G \in S(B,A)$. Apart from this one easily computes that the maximal possible degree of a field N as defined above is ba^b, where a and b are the respective orders of A and B. The order of the wreath product $A \wr B$ however is also $b.a^b$. For the definition of the wreath product see M. Hall [1], p. 81 or M.Krasner and L. Kaloujnine [2].

2. Proof of the theorem

Let $K \subset L \subset M \subset N$ be finite field extensions such that L/K is galoisian with Galois group B, M/L galoisian with Galois group A, while N is the least galoisian extension field of K containing M.

We may, in order to prove the theorem, assume K to be infinite. For if K is finite, then M=N and B and A are cyclic, while the Galois group of M/K is a group extension of A by B. These group extensions however are contained in the wreath product $A \wr B$, by the immersion theorem of [2].

Let $\{\beta_1, \dots, \beta_b\}$ be a set of conjugates of L/K, b being the order of B. Let furthermore $\{\alpha_1, \dots, \alpha_a\}$ be a set of conjugates of M/L, a being the order of A. Choose $c \in K$ such that $\gamma_{11} = \alpha_1 + c\beta_1$ is a primitive element for $M = K(\alpha_1, \beta_1)$. Denote $\alpha_j + c\beta_1$ by γ_{1j} $(j=1, \dots, a)$. Let τ_i: $\beta_1 \to \beta_i$ $(1 \leq i \leq b)$ denote the K-automorphisms of L, and choose by every τ_i an extension K-automorphism $\bar{\tau}_i$ of N. Define $\bar{\tau}_i \alpha_j = \alpha_{ij}$ and let $\gamma_{ij} = \alpha_{ij} + c\beta_i$. Then $\alpha_{1j} = \alpha_j$ $(j=1, \dots, a)$. Now, the elements $\gamma_{i1}, \dots, \gamma_{ia}$ are for every i $(1 \leq i \leq b)$ the zero's of an irreducible polynomial f_i with coefficients in L, while the set of all γ_{ij} are the zero's of the polynomial $f = f_1 f_2 \dots f_b$ with coefficients in K. f is irreducible as the degree ab of f is equal to the degree of the field $K(\gamma_{11}) = K(\alpha_1, \beta_1)$ over K, γ_{11} being a zero of f. It follows that $K(\gamma_{ij}) = K(\alpha_j, \beta_i)$ so that $K(\gamma_{11}, \dots, \gamma_{ba})$ is the least normal field extension of K containing M; thus $N = K(\gamma_{11}, \dots, \gamma_{ba})$.

So the Galois group G of N/K can be represented as a permutation group of the elements γ_{ij}. We will show this permutation group to be embeddable into the wreath product of the permutation group A (on the set $\{\alpha_1, \dots, \alpha_a\}$) and the permutation group B (on the set $\{\beta_1, \dots, \beta_b\}$). We apply an old trick, by which the permutations of G are carried over to permutations of a set of indeterminates. Let $t_1, \dots, t_a$ be a set of indeterminates, and form the expressions $y_{11} = t_1 \gamma_{11} + \dots + t_a \gamma_{1a}$, σy_{11} where σ runs through the Galois group A of M/L (σ permutes the elements $\gamma_{11}, \dots, \gamma_{1a}$ in just the same way as the elements $\alpha_{11}, \dots, \alpha_{1a}$ respectively).

The elements y_{11}, $\sigma y_{11} (\sigma \in A)$ are conjugates with respect to $L_t = L(t_1,\dots,t_a)$. Let f_{1t} be their (irreducible) polynomial. Then the coefficients of this polynomial can be uniquely expressed in the form

$$(1)\ a_o(t_1,\dots,t_a)+a_1(t_1,\dots,t_a)\beta_1+\dots a_{b-1}(t_1,\dots,t_a)\beta_1^{a-1}$$

with $a_i(t_1,\dots,t_a) \in K_t = K(t_1,\dots,t_a)$. Now, the group consisting of all permutations of $t_1,\dots,t_a$ leaving the joint elements $a_i(t_1,\dots,t_a)$ thus obtained invariant, is the same as the permutation group A (of the elements $\gamma_{11},\dots,\gamma_{1a}$ instead of $t_1,\dots,t_a$ respectively). See for this [3], § 61. If we apply a K-automorphism $\bar{\tau}_i$ to f_{1t} then f_{1t} is carried into a conjugate (irreducible) polynomial, f_{it} say, which is obtained by replacing the coefficients of f_{1t} having the form (1), by their conjugates

$$(2)\ a_o(t_1,\dots,t_a)+a_1(t_1,\dots,t_a)\beta_i+\dots+a_{b-1}(t_1,\dots,t_a)\beta_i^{a-1}.$$

The zero's of f_{it} are necessarily $\bar{\tau}_i y_{11} = y_{i1} =$

$$= t_1\ \bar{\tau}_i\ \gamma_{11} + \dots + t_a\ \bar{\tau}_i\ \gamma_{1a} =$$

$$= t_1\ \gamma_{i1} + \dots + t_a\ \gamma_{ia},\ \bar{\tau}_i\ \sigma\ y_{11}\ (\sigma \in A).$$

As, however, the joint coefficients (2) of f_{it} remain invariant under precisely the same permutations of $t_1,\dots,t_a$ as those letting (1) invariant, it follows from the same theorem of [3] that the Galois group of f_i with respect to L is the same permutation group A (of the elements $\gamma_{i1},\dots,\gamma_{ia}$ instead of $t_1,\dots,t_a$ or $\gamma_{11},\dots,\gamma_{1a}$ respectively).

Now, let τ be an arbitrary K-automorphism of N, the restriction of which to L is $\tau_i (1 \leq i \leq b)$. Then we show that τ can be represented as a permutation of $\gamma_{11}, \ldots, \gamma_{ba}$, which can be split into two permutations, one of which permutes the sets formed by the zero's of the respective polynomials $f_1, \ldots, f_b$ according to the permutation $\beta_1 \to \beta_i$ of B, leaving the second indices of the γ_{ij} invariant, while the other permutes the zero's $\gamma_{i1}, \ldots, \gamma_{ia}$ of each polynomial f_i according to a permutation occurring in the Galois permutation group A of the zero's of f_i. So this second permutation will be a permutation of the direct product $A \times \ldots \times A$ (b times) on the set $V = \{\gamma_{11}, \ldots, \gamma_{ba}\}$, while the first one permutes the subsets $V_1 = \{\gamma_{11}, \ldots, \gamma_{1a}\}$, $\ldots$, $V_b = \{\gamma_{b1}, \ldots, \gamma_{ba}\}$ of V according to B. The full set of all permutations on V generated by B and $A \times \ldots \times A$ however, is just the wreath product of A and B.

Now, the possibility of splitting the permutation on V representing τ into two permutations of the described kind follows readily by the following argument. Under τ the set V_1 is carried into the set V_i, whereas at the same time the second indices of the elements $\gamma_{11}, \ldots, \gamma_{1a}$ of V_1 are submitted to some permutation π. So τ can be split into two permutations, the first one given by $\gamma_{1j} \to \gamma_{ij} (1 \leq j \leq a)$, the second one by π. If we apply those permutations to the zero's of f_{1t} respectively, then the coefficients (1) of f_{1t} are carried into the coefficients (2) of f_{it} by the first one, whereas π necessarily leaves those coefficients invariant. But there are no other permutations of $\gamma_{i1}, \ldots, \gamma_{ia}$ leaving the coefficients (2) of f_{it} invariant than those of A.

Remarks on the theorem:

1. If N has maximal possible degree ba^b over K, then G is isomorphic to $A \wr B$. The fact that there exist Galoisian field extensions with group $A \wr B$ follows by working with purely transcendental field extensions over arbitrary fields.
2. Not every subgroup of $A \wr B$ is of course an element of S(B,A). One observes readily that only those group divisors G of $A \wr B$ occur in S(B,A) that contain a subdirect product of $A \times \ldots \times A$ (b times) as an invariant subgroup, with index b.
3. Let $\bar{A}$ be the Galois group of N with respect to L. Then we have the exact sequence $1 \to \bar{A} \to G \to B \to 1$, by Galois theory. $A \wr B$ is a split extension $1 \to A^B \to A \wr B \to B \to 1$ where $A^B = A \times \ldots \times A$ (b times). The embedding φ of G into $A \wr B$ as given in the proof of the theorem is easily shown to be such that the following diagram is commutative

$$\begin{array}{ccccccccc} 1 & \to & A^B & \to & A \wr B & \to & B & \to & 1 \\ & & \uparrow \varphi & & \uparrow \varphi & & \| & & \\ 1 & \to & A & \to & G & \to & B & \to & 1. \end{array}$$

4. By the theorem (and remark 2) the so called embeddability problem for galoisian field extension can be generalized. This problem, raised by Hasse (see P. Wolf [4]), takes the following form. Given any element $G \in S(B,A)$ and galoisian field extensions L/K and M/L with Galois groups B and A respectively, then find necessary and sufficient conditions that the Galois group G' of M/K be isomorphic to G.

Mathematical Centre, Amsterdam
University of Ottawa, Ottawa.

References:

[1] M. Hall, The theory of groups, McMillan 1959.

[2] M. Krasner - L. Kaloujnine, Produit complet de permutations et problèm d'extension de groupes, Acta Szegel 13, 14 (1950, 1951).

[3] B.L van der Waerden, Algebra I, Springer 1955.

[4] P. Wolf, Algebraische Theorie der Galoisschen Algebren, Deutscher Verlag, Berlin 1956.