POLYNOMIALS WITH CERTAIN PRESCRIBED CONDITIONS ON THE GALOIS GROUP

ELIZABETH ROWLINSON AND HANS SCHWERDTFEGER

Introduction. In this paper, some contributions are made to the theory of algebraic equations over the rational field with conditions imposed on the Galois group.[1] In § 1, for a given abstract group G all faithful permutation representations $\bar{G}$ are obtained, and it is shown that if one of them is the group of some equation with splitting field K, then any of them is the group of some equation, also with splitting field K. The method of proof enables us to construct an equation having as group a given faithful permutation representation $\bar{G}$ of a prescribed group G if we are given an equation having as group some faithful representation $\tilde{G}$ of G. In § 2, equations having nilpotent group are considered, non-normal extension fields are discussed, and a canonical form is obtained for the roots of non-normal irreducible equations; this form is used to characterize fields and equations with nilpotent groups. In §§ 3 and 4 we are concerned with the problem of constructing irreducible equations with prescribed group. In § 3 we give a method when the group is Abelian; it involves finding cyclic direct factor fields as subfields of appropriately chosen cyclotomic fields. In § 4 we reduce the problem for any group to that of solving a set of Diophantine equations; for groups of very low order, particular solutions can be obtained on a computer. The method depends on the Normal Basis Theorem of Artin (**1**, p. 66) and is a generalization of a method developed by L. M. Young for cyclic groups (**6**).

1.1. As in (**2**), we consider the Galois group $\mathfrak{G}[f(x)]$ of the polynomial $f(x)$ over the field R_0 of the rational numbers to be a permutation group, and the Galois group $\mathfrak{G}(K)$ of the normal algebraic extension K of R_0 to be an automorphism group. If K is the splitting field of $f(x)$, then $\mathfrak{G}[f(x)]$ is a faithful permutation representation of $\mathfrak{G}(K)$.

1.2. We shall first establish a theorem by means of which it is possible to find all faithful permutation representations of a given finite group G by examination of its subgroups. It is a generalization of a theorem given in (**3**, p. 57).

Received May 12, 1967. This paper contains, in condensed form, the results obtained in the Ph.D. thesis of the first author, McGill University, August, 1965. The work was supported by a grant from the National Research Council of Canada.

[1]For consistency, the ground field has been taken as the rational field throughout the paper; however, the results obtained in §§ 1 and 2 are valid for any ground field of characteristic 0.

Two permutation groups are called equivalent if one of them can be obtained from the other by a reordering of the set of permuted symbols. In Galois theory, where the symbols are the roots of $f(x)$, equivalent permutation groups can be considered identical.

THEOREM 1.2. *Let G be a group, and let $\bar{G}$ be a faithful representation of G as a permutation group. Then $\bar{G}$ corresponds to a set $H_1, \ldots, H_k$ of subgroups of G for which*

$$\left(\bigcap_{g\in G} H_1{}^g\right) \cap \left(\bigcap_{g\in G} H_2{}^g\right) \cap \ldots \cap \left(\bigcap_{g\in G} H_k{}^g\right) = 1. \tag{1.2.1}$$

Conversely, to any such set of subgroups there corresponds a faithful representation $\bar{G}$ of G.

Proof. (a) Let $\bar{G}$ be a faithful permutation representation of G, and let $(t_{11} = 1, t_{12}, \ldots, t_{1n_1}), (t_{21}, t_{22}, \ldots, t_{2n_2}), \ldots, (t_{k1}, \ldots, t_{kn_k})$ be a set of systems of transitivity of $\bar{G}$. Let $\bar{H}_i$ be the subgroup of $\bar{G}$ which leaves fixed the symbol t_{i1}, and g_{ij} an element of $\bar{G}$ carrying t_{i1} into t_{ij}; there is such an element for $j = 1, \ldots, n_i$, and

$$\bar{G} = \bar{H}_i \cup g_{i2}\bar{H}_i \cup \ldots \cup g_{in_i}\bar{H}_i, \qquad n_i = [\bar{G} : \bar{H}_i].$$

Since $\bar{H}_i{}^{g_{ij}}$ is the subgroup which leaves t_{ij} fixed, the normal subgroup

$$\bar{N}_i = \bigcap_{j=1,\ldots,n_i} \bar{H}_i{}^{g_{ij}} = \bigcap_{g\in G} \bar{H}_i{}^g$$

leaves fixed $t_{i1}, \ldots, t_{in_i}$; hence, $\bigcap_{i=1}^{k} \bar{N}_i$ leaves fixed all symbols t_{ij} and is therefore the identity. If $H_1, \ldots, H_k$ are the subgroups of G corresponding, respectively, to $\bar{H}_1, \ldots, \bar{H}_k$ under the isomorphism $\bar{G} \simeq G$, (1.2.1) follows.

(b) Let $H_1, \ldots, H_k$ be subgroups of G satisfying (1.2.1); let

$$G = H_i \cup g_{i2}H_i \cup \ldots \cup g_{in_i}H_i,$$

where $n_i = [G : H_i]$ $(i = 1, \ldots, k)$. For $g \in G$, let

$$\Pi(g) = \begin{pmatrix} H_1, & g_{12}H_1, \ldots, & g_{1n_1}H_1, & H_2, \ldots, & g_{2n_2}H_2, \ldots, & H_k, \ldots, g_{kn_k}H_k \\ gH_1, & gg_{12}H_1, \ldots, & gg_{1n_1}H_1, & gH_2, \ldots, & gg_{2n_2}H_2, \ldots, & gH_k, \ldots, gg_{kn_k}H_k \end{pmatrix}.$$

$\Pi(g)$ is a permutation, and gives a homomorphism of G whose kernel consists of all elements g for which $gg_{ij}H_i = g_{ij}H_i$ (all i, j), or $g \in H_i{}^{g_{ij}}$ (all i, j). But from (1.2.1), $\bigcap_{i,j} H_i{}^{g_{ij}} = 1$, and thus the homomorphism is an isomorphism.

Note. Each of the sets $H_i, \ldots, g_{in_i}H_i$ is a system of transitivity of $\bar{G}$; if $N_i = \bigcap_{g\in G} H_i{}^g$, then $\{\Pi(g): g \in N_i\}$ is the subgroup which leaves the system fixed, and $\{\Pi(g): g \in H_i\}$ is the subgroup which leaves fixed H_i.

Two well-known results follow as corollaries.

COROLLARY 1. *Taking $k = 1$, we see that any transitive faithful representation $\bar{G}$ of G corresponds to some subgroup H for which $\bigcap_{g\in G} H^g = 1$, and to any such subgroup there corresponds a transitive representation $\bar{G}$. The degree of $\bar{G}$ is $[G : H]$.*

COROLLARY 2. *If G is Abelian, the only subgroup satisfying $\bigcap_{g\in G}H^g = 1$ is the identity; thus the only transitive faithful representation is the regular representation.*

1.3. The following theorem shows that if a faithful permutation representation of a group G is the Galois group of an equation over R_0 with splitting field K, then every faithful permutation representation $\bar{G}$ of G is the Galois group of some equation, also with splitting field K.

THEOREM 1.3. *Let K be a field such that $\mathfrak{G}(K) = G$. Let $\bar{G}$ be any faithful permutation representation of G; then there exists an equation $\bar{f}(x) = 0$ with splitting field K and Galois group $\bar{G}$.*

Proof. In the notation of Theorem 1.2, let $H_1, \ldots, H_k$ be the subgroups of G corresponding to the representation $\bar{G}$. To each of these subgroups H_i there corresponds an intermediate field K_i between K and R_0 such that

$$\mathfrak{G}(K/K_i) = H_i \quad \text{and} \quad [K_i : R_0] = [G : H_i] = n_i.$$

Let $K_i = R_0(\beta_i)$ and let the minimum polynomial of β_i be $f_i(x)$, with roots $\beta_i = \beta_{i1}, \ldots, \beta_{in_i}$; we order the roots so that the conjugate subgroups $H_i^{g_{ij}}$ $(j = 1, \ldots, n_i)$ correspond, respectively, to the conjugate subfields $R_0(\beta_{ij})$ $(j = 1, \ldots, n_i)$.

Any automorphism in $N_i = \bigcap_j H_i^{g_{ij}}$ leaves fixed all the subfields $R_0(\beta_{ij})$ $(j = 1, \ldots, n_i)$, and hence leaves fixed their composite $R_0(\beta_{i1}, \ldots, \beta_{in_i})$; moreover, any automorphism in G which leaves fixed $R_0(\beta_{i1}, \ldots, \beta_{in_i})$ leaves fixed each of $R_0(\beta_{ij})$ $(j = 1, \ldots, n_i)$ and therefore is an element of N_i. Thus N_i corresponds to $R_0(\beta_{i1}, \ldots, \beta_{in_i})$, which is the splitting field of $f_i(x)$.

Similarly, $\bigcap_{i=1}^{k} N_i$ corresponds to the composite of the splitting fields of $f_1(x), \ldots, f_k(x)$, that is, of $\bar{f}(x) = f_1(x) \ldots f_k(x)$. $\bar{f}(x)$ thus has splitting field K, and therefore $\mathfrak{G}[\bar{f}(x)]$ is a faithful representation of G. Since $f_1(x), \ldots, f_k(x)$ are irreducible, the representation has k systems of transitivity of lengths $n_1, n_2, \ldots, n_k$; the subgroup which leaves fixed β_i is $\bar{H}_i \simeq H_i$, and thus $\mathfrak{G}[\bar{f}(x)] = \bar{G}$.

COROLLARY 1. *We have that $\bar{f}(x) = f_1(x) \ldots f_k(x)$, where $\deg f_i(x) = [G : H_i]$. Thus, $\deg \bar{f}(x) = \sum_i [G : H_i]$, and therefore the minimum degree of $\bar{f}(x)$ is the minimum value of $\sum_i [G : H_i]$ over all possible choices of $H_1, \ldots, H_k$.*

COROLLARY 2. *Taking $k = 1$ in Corollary 1, we obtain that the minimum degree for an irreducible equation with splitting field K is $\min[G : H]$ over all subgroups H for which $\bigcap H^g = 1$.*

COROLLARY 3. *Let B_i be the splitting field $R_0(\beta_{i1}, \ldots, \beta_{in_i})$. Then*

$$\mathfrak{G}[f_i(x)] \simeq \mathfrak{G}(B_i) \simeq G/N_i = G/(\bigcap_{g\in G} H_i^g).$$

https://doi.org/10.4153/CJM-1969-027-8 Published online by Cambridge University Press

COROLLARY 4. *Suppose that G is a direct product $G_1 \times \ldots \times G_m$. We can take*

$$H_i = \prod_{\substack{\lambda=1; \\ \lambda \neq i}}^{m} G_\lambda;$$

in this case, $\bar{f}(x) = f_1(x) \ldots f_m(x)$, where, by Corollary 3, $\mathfrak{G}[f_i(x)] \simeq G/(\bigcap_{g \in G} H_i^g) = G/H_i \simeq G_i$.

1.4. The method of proof of Theorem 1.3 can be used to construct the polynomial $\bar{f}(x)$ when K is given as the splitting field of some polynomial $\tilde{f}(x)$ with known roots and Galois group $\tilde{G}$. The construction proceeds as follows:

Let the roots of $\tilde{f}(x)$ be $\alpha_1, \ldots, \alpha_m$; a primitive element θ in the splitting field $R_0(\alpha_1, \ldots, \alpha_m)$ of $\tilde{f}(x)$ can be obtained in the form $c_1\alpha_1 + \ldots + c_m\alpha_m$ by following the method normally used to prove the theorem on the Primitive Element (**2**, pp. 174–175). We require now an element β_i in $R_0(\theta)$ such that $R_0(\beta_i)$ is the fixed field under the automorphisms of the subgroup H_i; the method given in (**2**, p. 211) enables us to find such an element, and its minimum polynomial $f_i(x)$ can be constructed. The required polynomial $\bar{f}(x)$ is then given by $\bar{f}(x) = f_1(x) \ldots f_k(x)$.

Examples. (1) Let $\tilde{f}(x) = x^3 - r$ ($r \in R_0$, $r^{\frac{1}{3}} \notin R_0$). Then $\tilde{G}$ is $\mathfrak{S}_3$, the symmetric group of degree 3; G is therefore defined by $\{a, b\}$, $a^3 = b^2 = (ab)^2 = 1$, and $\tilde{G}$ corresponds to the subgroup $H = \{b\}$. Following the method given, an equation was constructed with group $\bar{G}$, the regular representation of G. The element $r^{\frac{1}{3}} - wr^{\frac{1}{3}}$, primitive in K, was chosen as θ, where w is a primitive cube root of unity. Since the subgroup H corresponding to $\bar{G}$ is the identity, $\beta = \theta$; the result $\bar{f}(x) = x^6 + 27r^2$ was obtained.

(2) Using the fact that $\bar{f}(x) = x^6 + 27r^2$ has group $\bar{G}$, another equation $\tilde{f}'(x)$ with group $\tilde{G}$ was obtained. Since $\bar{f}(x)$ is normal, we can take $\theta = r^{\frac{1}{3}} - wr^{\frac{1}{3}}$, where $a(\theta) = wr^{\frac{1}{3}} - w^2r^{\frac{1}{3}}$, $b(\theta) = r^{\frac{1}{3}} - w^2r^{\frac{1}{3}}$. Following (**2**, p. 211), we obtain β_i in the form $k^2 - 3kr^{\frac{1}{3}} + 3r^{\frac{2}{3}}$, where k can take any value such that the three conjugates of β_i are different. $k = 0$ satisfies this condition, and the resulting equation is $\tilde{f}'(x) = x^3 - 27r^2$.

2.1. Let $K = R_0(\alpha_1)$ be a non-normal algebraic extension of R_0, and let $f(x) = (x - \alpha_1) \ldots (x - \alpha_n)$ be the minimum polynomial of α_1. Let $\bar{K}$ be the splitting field of $f(x)$ over R_0.

Let S be the automorphism group of K over R_0, and let G be the Galois group of $\bar{K}$.

We shall prove a theorem relating the group S to the group G; the result was obtained in another form by Loewy (**4**), but his proof is quite different from the one given here.

THEOREM 2.1. *Let H be the subgroup of G which has K as fixed field. Then $S \simeq \mathfrak{N}_G(H)/H$, where $\mathfrak{N}_G(H)$ is the normalizer of H in G.*

Proof. Let $a \in \mathfrak{N}_G(H)$; a maps α_1 into one of its conjugates, and thus induces an isomorphism σ_a: $R_0(\alpha_1) \to R_0(a\alpha_1)$. Since H is the subgroup of G which leaves fixed $R_0(\alpha_1)$, aHa^{-1} is the subgroup of G which leaves fixed $R_0(a\alpha_1)$. But $aHa^{-1} = H$, and therefore $R_0(\alpha_1) = R_0(a\alpha_1)$. σ_a is thus an automorphism, and $a \to \sigma_a$ gives a homomorphism of $\mathfrak{N}_G(H)$ into S.

Let $\sigma \in S$; σ maps α_1 to one of its conjugates. All conjugates of α_1 occur as $g\alpha_1$ for some $g \in G$; let a_σ be an element of G which carries α_1 to $\sigma\alpha_1$. Since $R_0(\alpha_1) = R_0(a_\sigma\alpha_1)$, $H = a_\sigma H a_\sigma^{-1}$, and $a_\sigma \in \mathfrak{N}_G(H)$. The homomorphism is therefore onto. Its kernel consists of all elements $a \in \mathfrak{N}_G(H)$ for which σ_a is the identity; that is, H. Thus $S \simeq \mathfrak{N}_G(H)/H$.

2.2. Using Theorem 2.1, we obtain a canonical form for the roots of $f(x)$. Since $\bar{K}$ is the splitting field of $f(x)$, $\mathfrak{G}[f(x)] \simeq G$. H is the subgroup of G which leaves fixed $R_0(\alpha_1)$, and thus $\mathfrak{G}[f(x)]$ is the transitive representation

$$\bar{G} = \left\{ \begin{pmatrix} H, g_2H, \ldots, g_nH \\ gH, gg_2H, \ldots, gg_nH \end{pmatrix} : g \in G \right\},$$

where $G = H \cup g_2H \cup \ldots \cup g_nH$.

Let $S = \{\sigma_i : i = 1, \ldots, s\}$. Since $\sigma_i\alpha_1$ is an element of $R_0(\alpha_1)$, it can be written $\phi_i(\alpha_1)$, where $\phi_i(x)$ is a polynomial of degree less than n. $\phi_i(\alpha_1)$ is a root of $f(x)$; moreover, any root which can be written as a polynomial in α_1 occurs in the set $\{\phi_i(\alpha_1): i = 1, \ldots, s\}$, since such a root gives rise to an automorphism of $R_0(\alpha_1)$.

THEOREM 2.2. *The roots $\alpha_1, \phi_2(\alpha_1), \ldots, \phi_s(\alpha_1)$ form a system of imprimitivity for $\bar{G}$; each conjugate system can be written $\alpha_r, \phi_2(\alpha_r), \ldots, \phi_s(\alpha_r)$.*

Proof. Let α_r be a root of $f(x)$ not included in the set $\phi_i(\alpha_1)$. Since $f(\phi_i(\alpha_1)) = 0$, $f(x)$ divides $f(\phi_i(x))$, and therefore $f(\phi_i(\alpha_r)) = 0$. Thus $\phi_i(\alpha_r)$ is a root for $i = 1, \ldots, s$. None of these roots is included in the set $\{\phi_i(\alpha_1)\}$; otherwise, we have that $R_0(\alpha_1) = R_0(\phi_i(\alpha_1)) = R_0(\phi_j(\alpha_r)) = R_0(\alpha_r)$ for some i and j, and this is not so. Continuing until the roots are exhausted, we obtain disjoint sets of the required form.

Let $g \in \bar{G}$; suppose that g carries $\phi_k(\alpha_r)$ into $\phi_{k'}(\alpha_{r'})$. Then g carries the field $R_0(\phi_k(\alpha_r)) = R_0(\alpha_r)$ onto the field $R_0(\phi_{k'}(\alpha_{r'})) = R_0(\alpha_{r'})$. Thus it must carry each of the roots $\phi_i(\alpha_r)$ $(i = 1, \ldots, s)$ to one of the roots $\phi_j(\alpha_{r'})$ $(j = 1, \ldots, s)$ and hence each of the sets $\{\phi_i(\alpha_r)\}$ is a system of imprimitivity.

We have now shown that the roots of $f(x)$ have the form

$$\begin{array}{cccc} \alpha_1 & \phi_2(\alpha_1) & \ldots & \phi_s(\alpha_1) \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ \alpha_m & \phi_2(\alpha_m) & \ldots & \phi_s(\alpha_m) \end{array} \qquad (sm = n,\ s < n); \tag{2.2.1}$$

each row is a system of imprimitivity for $\bar{G}$. The automorphism group S can

be written $\{\sigma_i\colon \sigma_i(\alpha_1) = \phi_i(\alpha_1)\}$; it is isomorphic to the group of functions $\{\phi_i(x) \bmod f(x)\colon i = 1, \ldots, s\}$.

2.3. In the theorem of this section we use the preceding results to characterize nilpotent fields and equations.

THEOREM 2.3. *A normal field N is a nilpotent extension of R_0 (i.e., $\mathfrak{G}(N)$ is nilpotent) if and only if every intermediate field between N and R_0 other than R_0 has a non-trivial automorphism group.*

Proof. All properties of nilpotent groups used are proved in (**3**, Chapter **10**).

(a) Suppose that N is a nilpotent extension of R_0. Let K be any intermediate field between N and R_0, and let $\bar{K}$ be the smallest normal extension of R_0 containing K. The Galois group G of $\bar{K}$ over R_0 is a factor group of $\mathfrak{G}(N)$, and hence is nilpotent. Let H be the subgroup of G which leaves K fixed; since we take $K \neq R_0$, H is a proper subgroup of G. Thus, since G is nilpotent, H is a proper subgroup of $\mathfrak{N}_G(H)$. Hence, if S is the automorphism group of K over R_0, then by Theorem 2.1, $S \simeq \mathfrak{N}_G(H)/H \neq 1$.

(b) Suppose that every intermediate field between N and R_0 has a non-trivial automorphism group over R_0. Let H be a maximal subgroup of $\mathfrak{G}(N)$, and let K be the fixed field in N under the automorphisms of H. Let $K = R_0(\alpha)$, and let $f(x)$, of degree n, be the minimum polynomial of α. Since K has a non-trivial automorphism group over R_0, K must contain at least one of the conjugates of α (i.e., α is not the only root of $f(x)$ in $R_0(\alpha)$).

Suppose that $f(x)$ is not normal; let s be the number of its roots which lie in $R_0(\alpha)$. Then the roots of $f(x)$ have the form (2.2.1), and each row is a system of imprimitivity for the Galois group of $f(x)$. Consider the expression

$$\psi(c) = \prod_{i=1}^{s} (c - \phi_i(\alpha)) \qquad (c \in R_0).$$

Under the permutations of the Galois group of $f(x)$, $\psi(c)$ takes at most m different values; it therefore has degree at most m over R_0. No two conjugates of $\psi(c)$ can be identically equal, and therefore we can choose a value for c such that they are all different. $\psi(c)$ then has degree m over R_0.

Consider the field $R_0(\psi(c))$; we have that $R_0(\alpha) \supset R_0(\psi(c)) \supset R_0$ (proper inclusions). Let the subgroup of $\mathfrak{G}(N)$ for which $R_0(\psi(c))$ is the fixed field be H_1; then $H \subset H_1 \subset G$ (proper inclusions). But this is not so, since H is maximal. $f(x)$ is therefore normal, and $R_0(\alpha)$ is normal over R_0; H is thus a normal subgroup of $\mathfrak{G}(N)$. Hence $\mathfrak{G}(N)$ is nilpotent, since its maximal subgroups are normal.

Note. N is equivalently characterized by the condition that every *minimal* intermediate field must have a non-trivial automorphism group. For suppose that N satisfies this condition; as in part (b), let H be a maximal subgroup of $\mathfrak{G}(N)$, and let $R_0(\alpha)$ be the fixed field for H. Then $R_0(\alpha)$ is a minimal intermediate field, and the proof proceeds as before.

COROLLARY 1. *The theorem can equivalently be stated as a characterization of nilpotent equations in the following way.*

An equation $f(x) = 0$ *with roots* $\alpha_1, \ldots, \alpha_n$ *has nilpotent Galois group if and only if, corresponding to any polynomial value* $p(\alpha_1, \ldots, \alpha_n)$ *not in* R_0, *there exists a polynomial* $q(x)$ *such that* $p(\alpha_1, \ldots, \alpha_n)$ *and* $q\{p(\alpha_1, \ldots, \alpha_n)\}$ *are different and conjugate over* R_0.

COROLLARY 2. *An irreducible equation* $f(x) = 0$ *of prime degree has nilpotent Galois group if and only if it is normal, and therefore cyclic.*

Proof. (a) Suppose that $f(x)$ has nilpotent Galois group $\bar{G}$, and is not normal. If α is a root, there must be (by Corollary 1) at least one more root of the form $\phi(\alpha)$. Hence by Theorem 2.2, $\bar{G}$ is imprimitive. But this is impossible, since $\bar{G}$ is of prime degree. $f(x)$ is therefore normal, and thus cyclic.

(b) If $f(x)$ is cyclic, then it is also nilpotent.

3.1. In this section we give a method enabling us to construct equations with given Abelian group.

Let A be any finite Abelian group. Then A can be written in the following form:

$$A = C_{p_1^{\alpha_{11}}} \times \ldots \times C_{p_1^{\alpha_{1r_1}}} \times C_{p_2^{\alpha_{21}}} \times \ldots \times C_{p_2^{\alpha_{2r_2}}} \times \ldots \times C_{p_k^{\alpha_{k1}}} \times \ldots \times C_{p_k^{\alpha_{kr_k}}},$$

where $C_{p_i^{\alpha_{ij}}}$ is the cyclic group of order $p_i^{\alpha_{ij}}$ (p_i prime, $i = 1, \ldots, k$).

Let $m = p_i^{\alpha_{ij}}$. The arithmetic progression $1, 1 + m, 1 + 2m, \ldots$ includes an infinite number of primes; we select one such prime π. Similarly, a value of π is chosen for each pair (i, j) in such a way that all the primes π are different.

Let ϵ_π denote a primitive πth root of unity. The Galois group $\mathfrak{G}[R_0(\epsilon_\pi)]$ of the πth cyclotomic field is cyclic of order $\pi - 1$. Let $s = (\pi - 1)/m$ (integral). Then $\mathfrak{G}[R_0(\epsilon_\pi)]$ contains a subgroup S which is cyclic of order s; let B be the subfield of $R_0(\epsilon_\pi)$ which is fixed under the automorphisms of S. Then $\mathfrak{G}(B) \simeq \mathfrak{G}[R_0(\epsilon_\pi)]/S$, a cyclic group of order m.

By Gauss' method (**2**, p. 320) we obtain a primitive element in the field B as $\theta = \epsilon_\pi + \epsilon_\pi^{\rho^m} + \ldots + \epsilon_\pi^{\rho^{(s-1)m}}$, where ρ is a primitive $(\pi - 1)$th congruence root of 1 (mod π). Since all the values of π are different, the composite of all the fields $R_0(\epsilon_\pi)$ is a direct product. Hence the composite $\bar{B}$ of all the fields B is also a direct product; its Galois group is the direct product of the Galois groups of its components, and thus is isomorphic to A.

Let $B_{ij}, \pi_{ij}, \theta_{ij}$, be the field B and the values of π and θ, respectively, which correspond to the pair (i, j). We consider the expression $\sum_i \sum_j \theta_{ij}$ in $\bar{B}$. Each element θ_{ij} has $p_i^{\alpha_{ij}}$ conjugates, and thus there are $o(A)$ conjugate expressions of the form $\sum_i \sum_j \theta_{ij}'$, where θ_{ij}' is some conjugate of θ_{ij}. These expressions are all different since the fields B_{ij} intersect only in R_0. Thus $\sum_i \sum_j \theta_{ij}$ has degree $o(A)$ over R_0, and is therefore primitive in $\bar{B}$. $\bar{B}$ is normal, and hence the equation $\prod(x - \sum_i \sum_j \theta_{ij}') = 0$ has group A.

Note 1. It is not necessary to use the decomposition of A into cyclic direct factors of prime power order; any decomposition into cyclic direct factors will suffice. The values of m can then be taken as the orders of these cyclic direct factors.

Note 2. The construction yields a field of group A as a subfield of the cyclotomic field of index $\Pi_{i,j}\pi_{ij}$. It was proved by Kronecker that every Abelian field is a subfield of some cyclotomic field; however, our construction yields only those Abelian fields which are subfields of cyclotomic fields of square-free index.

3.2. *Examples.* (1) We construct an equation for the group $A \simeq C_2 \times C_2$ (the so-called four-group).

We take $\pi_{11} = 3$, $\pi_{12} = 5$. We have that $B_{11} = R_0(\epsilon_3)$, and therefore $\theta_{11} = \epsilon_3$. To find θ_{12}, we require a primitive 4th congruence root of 1 mod 5; $\rho = 2$ is such a value. Thus, $\theta_{12} = \epsilon_5 + \epsilon_5^4$, and the field $R_0(\epsilon_3 + \epsilon_5 + \epsilon_5^4)$ has group A. By finding the conjugates of $\epsilon_3 + \epsilon_5 + \epsilon_5^4$ and multiplying, we obtain the corresponding equation as $f(x) = x^4 + 4x^3 + 5x^2 + 2x + 4 = 0$.

(2) Let $A \simeq C_2 \times C_3$. A is isomorphic to the cyclic group of order 6; we therefore immediately have one equation of group A, the 7th cyclotomic equation. We construct another one.

We take $\pi_{11} = 3$, $\pi_{21} = 7$. Again, $\theta_{11} = \epsilon_3$. For θ_{21}, we require a primitive 6th congruence root of 1 mod 7; we set $\rho = 3$. Then $\theta_{21} = \epsilon_7 + \epsilon_7^6$, and the field $R_0(\epsilon_3 + \epsilon_7 + \epsilon_7^6)$ has group A. The corresponding equation is

$$x^6 + 5x^5 + 8x^4 + 3x^3 + 3x^2 + 30x + 13 = 0.$$

4.1. In this section we give a method for constructing equations with given group; it is an extension of a method given in (**6**) for cyclic groups only.

Let K be a normal algebraic extension of R_0, with Galois group $G = \{\sigma_1 = 1, \sigma_2, \ldots, \sigma_n\}$. Then there exists a normal basis for K over R_0; that is, an element θ in K such that $\sigma_1(\theta), \ldots, \sigma_n(\theta)$ form a basis for K over R_0 (see **1**, p. 66). K can now be considered as a hypercomplex algebra over R_0 with basis elements $\sigma_1(\theta), \ldots, \sigma_n(\theta)$; let $\gamma_{ij}{}^k$ $(i, j, k = 1, \ldots, n)$ be the structure constants of this algebra, defined by

$$\sigma_i(\theta) \cdot \sigma_j(\theta) = \sum_{k=1}^{n} \gamma_{ij}{}^k \sigma_k(\theta) \qquad (\gamma_{ij}{}^k \in R_0).$$

Let $f(x)$ be the normal irreducible polynomial having roots $\sigma_1(\theta), \ldots, \sigma_n(\theta)$; $\mathfrak{G}[f(x)]$ is then the regular representation G_σ of G.

LEMMA 4.1. *θ can be so chosen that the values $\gamma_{ij}{}^k$ have the following properties:*

$$(4.1.1)\quad \begin{cases} (1) & \sum_m \gamma_{jk}{}^m \gamma_{im}{}^l = \sum_m \gamma_{ij}{}^m \gamma_{mk}{}^l & (\textit{all } i, j, k, l), \\ (2) & \gamma_{ij}{}^k = \gamma_{ji}{}^k & (\textit{all } i, j, k), \\ (3) & \sum_i \gamma_{ij}{}^k = \delta_{jk} & (\textit{all } j, k) \quad (\textit{Kronecker } \delta), \\ (4) & \gamma_{\sigma i, \sigma j}^{\sigma k} = \gamma_{ij}{}^k & (\textit{all } i, j, k \textit{ and all } \sigma \in G_\sigma). \end{cases}$$

https://doi.org/10.4153/CJM-1969-027-8 Published online by Cambridge University Press

Proof. Let α_i denote $\sigma_i(\theta)$ $(i = 1, \ldots, n)$. (1) and (2) follow immediately from the associativity and commutativity of K. (3) Let $\sum_i \alpha_i = r$; r is rational and non-zero. The set $\{\alpha_i/r: i = 1, \ldots, n\}$ is then also a normal basis for K, and we can replace θ by θ/r. We assume that this has been done; i.e., θ is so chosen that $\sum_i \sigma_i(\theta) = 1$. Thus $\sum_i \alpha_i \alpha_j = \alpha_j$, giving $\sum_i \sum_k \gamma_{ij}{}^k \alpha_k = \alpha_j$. Equating coefficients of α_k yields (3). (4) The relation $\alpha_i \alpha_j = \sum_k \gamma_{ij}{}^k \alpha_k$ is a relation between the roots of the equation $f(x) = 0$. It is therefore left invariant by any permutation σ in G_σ. Hence $\alpha_{\sigma i}\alpha_{\sigma j} = \sum_k \gamma_{ij}{}^k \alpha_{\sigma k}$, giving $\sum_k \gamma_{\sigma i, \sigma j}^{\sigma k} \alpha_{\sigma k} = \sum_k \gamma_{ij}{}^k \alpha_{\sigma k}$. Equating coefficients of $\alpha_{\sigma k}$ yields (4).

4.2. When θ is chosen as in Lemma 4.1, the coefficients of $f(x)$ can be expressed in terms of the values $\gamma_{ij}{}^k$. Let Γ represent the 3-dimensional array of n^3 rational numbers $\gamma_{ij}{}^k$; let $\sigma\Gamma$ be the array obtained by writing $\gamma_{\sigma i, \sigma j}^{\sigma k}$ in place of $\gamma_{ij}{}^k$. For $\sigma \in G_\sigma$, $\Gamma = \sigma\Gamma$ (by (4.1.1), (4)).

Let $\phi(\alpha_1, \ldots, \alpha_n)$ be any symmetric polynomial in $\alpha_1, \ldots, \alpha_n$. By repeated application of the multiplication law, $\phi(\alpha_1, \ldots, \alpha_n) = \sum_i a_i(\Gamma)\alpha_i$, where each $a_i(\Gamma)$ can be calculated as a polynomial in the elements of Γ.

For any given r, there is a permutation σ_r in G_σ which carries 1 to r, as G_σ is transitive. We have that $\sum_i a_i(\Gamma)\alpha_i = \phi(\alpha_1, \ldots, \alpha_n) = \phi(\alpha_{\sigma_r 1}, \ldots, \alpha_{\sigma_r n}) = \sum_i a_i(\sigma_r\Gamma)\alpha_{\sigma_r i} = \sum_i a_i(\Gamma)\alpha_{\sigma_r i}$. Equating coefficients of α_r, $a_r(\Gamma) = a_1(\Gamma)$; this is true for all r, and thus $\phi(\alpha_1, \ldots, \alpha_n) = a_1(\Gamma)\sum_i \alpha_i = a_1(\Gamma)$ (see the proof of Lemma 4.1, (3)). Thus each coefficient in $f(x)$ can be written as a polynomial in the elements of Γ; let $f(x) = x^n - s_1(\Gamma)x^{n-1} + \ldots + (-1)^n s_n(\Gamma)$.

4.3. We now show that if for a given group G we can find values of $\gamma_{ij}{}^k$ satisfying conditions (4.1.1) such that the resulting polynomial $f(x)$ is irreducible, then $\mathfrak{G}[f(x)] = G_\sigma$.

THEOREM 4.3. *Let G be a group of order n, and let its regular representation as a permutation group be G_σ. Let $\gamma_{ij}{}^k$ $(i, j, k = 1, \ldots, n)$ be rational numbers satisfying conditions* (4.1.1). *From the values $\gamma_{ij}{}^k$, a certain polynomial $f(x)$ can be obtained; if the values $\gamma_{ij}{}^k$ are such that this polynomial is irreducible, its Galois group is G_σ.*

Proof. Let $x_1, \ldots, x_n$ be arbitrary symbols which are multiplied according to the law $x_i x_j = \sum_k \gamma_{ij}{}^k x_k$; let A be the hypercomplex algebra over the rationals having these symbols as basis elements. From (4.1.1), (1) and (2), A is associative and commutative.

As previously, let Γ be the 3-dimensional array of n^3 rational numbers $\gamma_{ij}{}^k$ $(i, j, k = 1, \ldots, n)$, and let $\phi(x_1, \ldots, x_n)$ be any symmetric polynomial in $x_1, \ldots, x_n$. As in § 4.2, since from (4.1.1), (4), $\Gamma = \sigma\Gamma$ (all $\sigma \in G_\sigma$), we have that $\phi(x_1, \ldots, x_n) = a_1(\Gamma)\sum_i x_i$. Let

$$\bar{f}(x) = \prod_{i=1}^{n} (x - x_i);$$

https://doi.org/10.4153/CJM-1969-027-8 Published online by Cambridge University Press

then $\bar{f}(x) = x^n - s_1(\Gamma)(\sum_i x_i)x^{n-1} + \ldots + (-1)^n s_n(\Gamma)\sum_i x_i$, where the $s_i(\Gamma)$ $(i = 1, \ldots, n)$ are polynomials in the elements of Γ. Since $s_1(\Gamma)(\sum_i x_i) = (\sum_i x_i)$, $s_1(\Gamma) = 1$. Let $f(x) = x^n - s_1(\Gamma)x^{n-1} + \ldots + (-1)^n s_n(\Gamma)$.

From (4.1.1), (3), $(\sum_i x_i)x_j = \sum_i \sum_k \gamma_{ij}{}^k x_k = \sum_k \delta_{jk} x_k = x_j$; thus, $(\sum_i x_i)$ is an identity $\bar{1}$ in A. Let $\bar{R}_0$ be the subset of A given by $\{r\bar{1}: r \in R_0\}$. Since $\bar{1}$ is an identity, $\bar{R}_0 \simeq R_0$, and thus $\bar{R}_0$ is a field. $\bar{f}(x)$ is a polynomial over this field.

Suppose that $f(x)$ is irreducible over R_0; then $\bar{f}(x)$ is irreducible over $\bar{R}_0$. Since $\bar{f}(x_1) = 0, \bar{1}, x_1, \ldots, x_1{}^{n-1}$ form a basis for the extension field $\bar{R}_0(x_1)$. As these elements are linearly independent over $\bar{R}_0$, they are linearly independent over R_0 also. They all belong to A, and A is of order n; hence, they form a basis for A, and therefore $A = \bar{R}_0(x_1)$. As $x_2, \ldots, x_n$ also belong to A, it is a splitting field for $\bar{f}(x)$. A is of order n over $\bar{R}_0$, and thus $|\mathfrak{G}(A/\bar{R}_0)| = n$. But by (4.1.1), (4), any permutation $\sigma \in G_\sigma$ of $x_1, \ldots, x_n$ yields an automorphism of A over R_0; hence, $\mathfrak{G}(\bar{f}(x)/\bar{R}_0) = \mathfrak{G}(A/\bar{R}_0) = G_\sigma$.

Under the isomorphism $R_0 \simeq \bar{R}_0$, the polynomial $f(x)$ is carried to $\bar{f}(x)$. Thus the splitting field of $f(x)$ is isomorphic to the splitting field of $\bar{f}(x)$, the roots of $f(x)$ being carried to the roots of $\bar{f}(x)$. Hence $\mathfrak{G}(f(x)/R_0) = \mathfrak{G}(\bar{f}(x)/\bar{R}_0) = G_\sigma$.

Note. The equation $f(x) = x^n - s_1(\Gamma)x^{n-1} + \ldots + (-1)^n s_n(\Gamma)$ depends only on the order of G and not on its structure; the $s_i(\Gamma)$ are known polynomials in the n^3 unknowns $\gamma_{ij}{}^k$. Also, conditions (4.1.1), (1), (2), and (3) do not involve the structure of G. The equation $f(x) = 0$ is therefore a general form for equations of this type having group of order n, provided Γ is such that $f(x)$ is irreducible and that conditions (1), (2), and (3) are satisfied. The structure of the group is then imposed on the general equation by condition (4).

4.4. The conditions of (4.1.1) can be simplified considerably. Let $\Gamma_i = [\gamma_{ij}{}^k]$, $C_k = [\gamma_{ij}{}^k]$, and let P_σ be the $(n \times n)$ matrix obtained by applying the permutation σ to the columns of the identity matrix. Also, let σ_i be the permutation in G_σ which carries 1 to i; we have that $G_\sigma = \{\sigma_i: i = 1, \ldots, n\}$.

Conditions (1)–(4) can now be shown to be equivalent to the following set:

$$
(4.4.1)\quad \begin{cases} \text{(a)}\ C_1 \text{ is symmetric,} \\ \text{(b)}\ \displaystyle\sum_{i=1}^{n} \gamma_{ij}{}^1 = \delta_{j1} \qquad (j = 1, \ldots, n), \\ \text{(c)}\ C_k = P_{\sigma_k} C_1 P_{\sigma_k}{}' \qquad (k = 2, \ldots, n), \\ \text{(d)}\ \displaystyle\sum_m \gamma_{jk}{}^m \gamma_{im}{}^l = \sum_m \gamma_{ij}{}^m \gamma_{mk}{}^l \\ \quad \text{for } i = k+1, \ldots, n-1, j = 1, \ldots, n-1, k = 1, \ldots, n-2, l = 1. \end{cases}
$$

Conditions (a), (b), and (c) clearly imply (2), (3), and (4). The equations included in (1) but not in (d) can be obtained from (d) by forming appropriate double sums and using (2), (3), and (4).

For a given group of order n we can thus write the conditions as Diophantine equations in the $\frac{1}{2}n(n+1)$ variables required to write a general symmetric $(n \times n)$ matrix C_1. Condition (b) yields n linear equations, condition (c) enables us to write down the matrices C_k $(k = 2, \ldots, n)$, and condition (d) yields $\frac{1}{2}(n-1)^2(n-2)$ quadratic equations. Particular solutions for C_1 can be obtained, if solutions exist, by programming the Diophantine equations for a computer. Clearly, the number of equations increases very rapidly with n; the method is therefore only practicable for small groups.

4.5. When a matrix C_1 has been obtained satisfying conditions (4.4.1), we wish to compute $f(x)$. This can be done either directly, following the method of proof of Theorem 4.3, or by using the following result.

LEMMA 4.5. *Let C_1 be a matrix satisfying conditions* (4.4.1). *Let* $\sum_i x_i^{r+1} = S_{r+1} \cdot \bar{1}$; *then S_{r+1} is the sum of the elements in the first row of* $(\Gamma_1)^r$.

Proof. Let

$$x_i^r = (\bar{m}_i^{(r)})'\bar{x}, \quad \text{where} \quad \bar{x} = \begin{bmatrix} x_1 \\ x_2 \\ \cdot \\ \cdot \\ \cdot \\ x_n \end{bmatrix} \quad \text{and} \quad \bar{m}_i^{(r)} = \begin{bmatrix} m_{i1}^{(r)} \\ m_{i2}^{(r)} \\ \cdot \\ \cdot \\ \cdot \\ m_{in}^{(r)} \end{bmatrix}.$$

Then $x_i^{r+1} = (\bar{m}_i^{(r)})'\Gamma_i\bar{x}$, and thus $(\bar{m}_i^{(r+1)})' = (\bar{m}_i^{(1)})'(\Gamma_i)^r$. But from (c), $\Gamma_i = P_{\sigma_i}\Gamma_1 P_{\sigma_i}'$, therefore $(\bar{m}_i^{(r+1)})' = (\bar{m}_i^{(1)})'P_{\sigma_i}(\Gamma_1)^r P_{\sigma_i}'$. Now $m_{ij}^{(1)} = \delta_{ij}$, thus $(\bar{m}_i^{(1)})'P_{\sigma_i} = (\bar{m}_i^{(1)})'P_{\sigma_i^{-1}}' = [1, 0, \ldots, 0]$; hence $(\bar{m}_i^{(r+1)})'$ is the result of applying the permutation σ_i to the first row of $(\Gamma_1)^r$. As i runs from 1 to n, each element of the first row appears in the first place exactly once.

We have that $S_{r+1}\bar{1} = \sum_i x_i^{r+1} = \sum_i (\bar{m}_i^{(r+1)})'\bar{x}$; equating coefficients of x_1, $S_{r+1} = \sum_i m_{i1}^{(r+1)}$. Thus S_{r+1} is the sum of the elements appearing in the first place as i runs from 1 to n, or the sum of the elements in the first row of $(\Gamma_1)^r$.

When the values of S_r have been obtained for $r = 1, \ldots, n$ using this lemma, the values of s_r can be obtained from Newton's equations. $f(x)$ can then be tested for reducibility by Kronecker's method. (See, for instance, **5**, p. 77.) If $f(x)$ is irreducible, it will, by Theorem 4.3, have Galois group G_σ.

4.6. *Example.* We construct an equation having as group G the four-group. The regular representation is $\sigma_1 = 1$, $\sigma_2 = (1\ 2)\ (3\ 4)$, $\sigma_3 = (1\ 3)\ (2\ 4)$, $\sigma_4 = (1\ 4)(2\ 3)$. Let

$$C_1 = \begin{bmatrix} a & b & c & d \\ b & e & f & g \\ c & f & h & i \\ d & g & i & j \end{bmatrix};$$

the four linear equations (b) can then be written down. The matrices C_2, C_3, C_4, Γ_1, Γ_2, Γ_3, and Γ_4 can be constructed in terms of the ten unknowns $a, \ldots, j$, and the nine quadratic equations (d) written down. These thirteen Diophantine equations were programmed for a computer, and a large number of solutions was obtained.[2] One such solution was $a = -\frac{1}{2}$, $b = -\frac{1}{2}$, $c = 1$, $d = 1$, $e = -\frac{1}{4}$, $f = 5/4$, $g = -\frac{1}{2}$, $h = -5/4$, $i = -1$, $j = \frac{1}{2}$. Γ_1 can be written down, and the first rows of Γ_1^2 and Γ_1^3 computed. (It is necessary only to find the first row of each power of Γ_1 if in computing the next higher power we postmultiply by Γ_1.)

Using Lemma 5.4, the values $S_1 = 1$, $S_2 = -3/2$, $S_3 = 5/2$, $S_4 = 11/8$ are obtained, and from Newton's equations we then have that $s_1 = 1$, $s_2 = 5/4$, $s_3 = 7/4$, $s_4 = 19/16$. Thus $f(x) = x^4 - x^3 + 5x^2/4 - 7x/4 + 19/16$; this polynomial is irreducible. Hence by Theorem 4.3, $f(x) = 0$ has as Galois group the regular representation of the four-group.

References

1. E. Artin, *Galois theory*, 2nd ed. (Notre Dame Mathematical Lectures, no. 2, University of Notre Dame, Notre Dame, Indiana, 1959).
2. N. Čebotarev (Tschebotaröw) and H. Schwerdtfeger, *Grundzüge der Galois'schen Theorie* (P. Noordhoff, Groningen, 1950).
3. Marshall Hall, Jr., *The theory of groups* (Macmillan, New York, 1959).
4. A. Loewy, *Neue Elementare Begrundung und Erweiterung der Galois'schen Theorie*, S.-B. Heidelberger Akad. Wiss. Math.-Natur. Kl. 1925 (7), 1–50 and 1927 (1), 1–27.
5. B. L. van der Waerden, *Modern algebra*, Vol. I (Ungar, New York, 1953).
6. L. M. Young, *On certain cyclic extensions of the field of rational numbers* (Applied Mathematics and Statistical Laboratories, Stanford University, Technical Report, No. 1, 1961).

McGill University,
Montreal, P.Q.

[2]This was carried out by Professor W. D. Thorpe, Director of the McGill Computing Centre.