Revised

Title for binding.

On algebraic equations with prescribed Galois group.

On algebraic equations with prescribed Galois group

by

Elizabeth Rowlinson, M.A., B.Sc. (Oxon.)

A thesis submitted to the Faculty of Graduate Studies and Research in partial fulfilment of the requirements for the degree of Doctor of Philosophy.

Department of Mathematics,
McGill University,
Montreal.

August, 1965.

Acknowledgements

I would like to thank Professor H. Schwerdtfeger for his many suggestions and for his unfailing kindness and encouragement.

I am grateful to the National Research Council for financial assistance during the year 1964 - 5.

Contents

Introduction

The Galois theory of equations over the rational field can be divided into two main parts. Firstly, there arises the problem of finding the group of a given equation and of obtaining information about the roots from properties of the group; secondly, there occurs the inverse problem of constructing equations with given group. It is well known that tremendous obstacles are encountered in every attempt at a constructive solution of these problems.

There are several methods for finding the group of an equation in particular cases; for example, the group of an equation of low degree can often be obtained by Mertens' method of fundamental modules (reference 1, pages 189 - 199). The classical Galois theory relates properties of the splitting field to properties of the Galois group (reference 1, chapters III and IV).

The inverse problem has been approached from various directions. For the symmetric group, many methods have been developed, including those of Bauer, Perron, and Schur (reference 1, pages 390 - 398). For certain groups, a theorem of E. Noether (reference 2) can be used to solve the problem; by this method Kuyk and Mullender have obtained a general form for equations with given Abelian groups (reference 3). The work of Šafarevič in class field theory has shown that for any solvable group there

exists a normal extension of the rational field, but equations are not explicitly constructed (reference 4).

In this thesis some results are obtained in both parts of the theory by more elementary methods. In the first chapter, definitions and notations are established; the Galois group of an equation is defined as a permutation group, which can be considered as a faithful representation $\overline{G}$ of an abstract finite group G. For a given abstract group G, all such faithful representations $\overline{G}$ are obtained; it is shown that if there is an equation with splitting field K having as group one of the representations $\overline{G}$, then for any of the representations $\overline{G}$ there is an equation with splitting field K and group $\overline{G}$. The proof is constructive, and examples are given.

In Chapter II, 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.

Chapter III is concerned with the inverse problem; two methods are given for obtaining irreducible equations with prescribed group. The first is for Abelian groups, and involves finding cyclic direct factor fields as subfields of appropriately chosen cyclotomic fields. The second method depends on a theorem of Artin, and is a generalization of a method developed by Young for cyclic

groups (reference 5). For any group the problem is reduced to that of solving a set of Diophantine equations; for groups of low order, particular solutions can be obtained on a computer.

This thesis is original except where otherwise stated.

Chapter I

Definitions; faithful representations of a finite group by permutation groups; equations which have the same splitting field but different permutation groups.

§ 1. Definitions

The Galois group can be introduced in several different ways. We shall use the following definitions :-

Definition 1.1. Let $f(x) = 0$ be an equation of degree n with coefficients in a field F; let its roots be $\alpha_1, \ldots, \alpha_n$. Any equation $\phi(\alpha_1, \ldots, \alpha_n) = 0$, where ϕ is a rational function in n variables with coefficients in F, is called a relation between the roots. The Galois group $\mathcal{G}(f(x)/F)$ is the group of all permutations of degree n which, when applied to the roots $\alpha_1, \ldots, \alpha_n$ leave invariant the system of relations between them.

Definition 1.2. Let K be a normal algebraic extension of a field F. The Galois group $\mathcal{G}(K/F)$ is the group of all automorphisms of K which leave fixed the elements of F.

If K is the splitting field $F(\alpha_1, \ldots, \alpha_n)$ of $f(x)$, each permutation in $\mathcal{G}(f(x)/F)$ induces an automorphism in $\mathcal{G}(K/F)$, and each automorphism in $\mathcal{G}(K/F)$ induces a permutation in $\mathcal{G}(f(x)/F)$; this correspondence is an isomorphism (Reference 1, p. 212). $\mathcal{G}(f(x)/F)$ is therefore a faithful representation of $\mathcal{G}(K/F)$ by a permutation group of degree n.

We take the ground field F to be the field of rationals R_0; we write $\mathcal{G}(f(x))$ for $\mathcal{G}(f(x)/R_0)$, and $\mathcal{G}(K)$ for $\mathcal{G}(K/R_0)$.

§2. Faithful representations of a finite group by permutation groups.

The theorem of this section makes it possible to find all faithful permutation group representations of a finite group by examination of its subgroups. It is a generalization of a theorem given in reference 6, p. 57.

Two permutation groups are called equivalent if one can be obtained from the other by a re-ordering of the set of permuted elements; equivalent permutation groups of degree n are thus conjugate subgroups of the symmetric group $\mathcal{S}_n$. For the purposes of Galois theory, such groups can be considered identical, since the roots of an equation can be ordered arbitrarily. We shall make no distinction between them.

Theorem 2.1. Let G be a group, and let $\overline{G}$ be a faithful representation of G as a permutation group. Then $\overline{G}$ corresponds to a set $H_1, \ldots, H_k$ of subgroups of G for which

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

Moreover to any such set of subgroups there corresponds a

faithful representation $\bar{G}$.

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

$$\bar{G} = \bar{H}_i + g_{i2}\bar{H}_i + \ldots + g_{in_i}\bar{H}_i \quad (n_i = [\bar{G}:\bar{H}_i]).$$

$\bar{H}_i^{g_{ij}}$ is the subgroup which leaves t_{ij} fixed, and so $\bigcap_{j=1}^{n_i} \bar{H}_i^{g_{ij}}$ is the subgroup which leaves $t_{i1}, \ldots, t_{in_i}$ fixed. Let $\bar{N}_i = \bigcap_j \bar{H}_i^{g_{ij}} = \bigcap_{g \in G} \bar{H}_i^{g}$; $\bar{N}_i$ is a normal subgroup of $\bar{G}$. $\bigcap_{i=1}^{k} \bar{N}_i$ is the subgroup which leaves fixed all digits, and so is the identity. Thus

$$\left(\bigcap_{g \in G} \bar{H}_1^{g}\right) \cap \ldots \cap \left(\bigcap_{g \in G} \bar{H}_k^{g}\right) = 1.$$

Let $H_1, \ldots, H_k$ be the subgroups of G corresponding to $\bar{H}_1, \ldots, \bar{H}_k$ respectively under the isomorphism $\bar{G} \simeq G$; then $\left(\bigcap_{g \in G} H_1^{g}\right) \cap \ldots \cap \left(\bigcap_{g \in G} H_k^{g}\right) = 1.$

(b) Let $H_1, \ldots, H_k$ be subgroups of G such that

$$\left(\bigcap_{g \in G} H_1^g\right) \cap \ldots \cap \left(\bigcap_{g \in G} H_k^g\right) = 1 ;$$

let $G = H_i + g_{i2}H_i + \ldots + g_{in_i}H_i \quad (n_i = [G:H_i])$.

For $g \in G$, let $\overline{\Pi}(g) =$

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

The set $gH_i, \ldots, gg_{in_i}H_i$ is a permutation of the set $H_i, \ldots, g_{in_i}H_i$, and so $\overline{\Pi}(g)$ is a permutation. Since $\overline{\Pi}(g\,g') = \overline{\Pi}(g)\,\overline{\Pi}(g')$, $\overline{\Pi}$ is a homomorphism of G, whose kernel consists of all elements g for which $\overline{\Pi}(g) = 1$, i.e. $gg_{ij}H_i = g_{ij}H_i$ (all i, j), or $g \in H_i^{g_{ij}}$ (all i, j). But

$$\bigcap_{ij} H_i^{g_{ij}} = \left(\bigcap_{j} H_1^{g_{1j}}\right) \cap \ldots \cap \left(\bigcap_{j} H_k^{g_{kj}}\right)$$

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

The kernel of $\overline{\Pi}$ is thus the identity and the homomorphism is an isomorphism. The group $\overline{G} = \{\overline{\Pi}(g) : g \in G\}$ is therefore a faithful representation of G.

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

Corollary 1.[1] Since each of the groups H_i corresponds to a system of transitivity of $\overline{G}$, all transitive faithful representations of G are obtained by taking $k = 1$ in the theorem. Thus any transitive faithful representation $\overline{\overline{G}}$ of G corresponds to some subgroup H for which $\bigcap_{g \in G} H^g = 1$, and to any such subgroup there corresponds a representation $\overline{\overline{G}}$. The degree of $\overline{\overline{G}}$ is $[G:H]$.

Corollary 2. If the group G is abelian, all subgroups are normal; thus the only subgroup for which $\bigcap_{g \in G} H^g = 1$ is the identity. Hence by corollary 1, the only transitive faithful representation of G corresponds to $H = 1$; this is the regular representation.

§ 3. Equations which have the same splitting field but different permutation groups.

The following theorem shows that if a permutation representation of a group G is the Galois group of an equation over R_o, then every permutation representation $\overline{G}$ of G is the Galois group of some equation.

Theorem 3.1. Let K be a field such that $\mathcal{G}(K) = G$. Let $\overline{G}$ be any faithful representation of G as a permutation group; then there exists an equation $\overline{f}(x) = 0$ with splitting field K and Galois group $\overline{G}$.

Proof. We use the notation of Theorem 2.1. Let $H_1, \ldots, H_k$

---

1) This is equivalent to Theorem 5.3.2 of reference 6.

be the subgroups of G corresponding to the representation $\overline{G}$. By the Fundamental Theorem of Galois Theory, to each of these subgroups H_i there corresponds an intermediate field K_i between K and R_o such that $\mathcal{G}(K/K_i) = H_i$. Let $K_i = R_o(\beta_i)$. We have $[K:R_o(\beta_i)]\,[R_o(\beta_i):R_o] = [K:R_o] = o(G)$.

$$\therefore\ [R_o(\beta_i):R_o] = \frac{o(G)}{o(H_i)} = [G:H_i] = n_i\ .$$

Let the minimum polynomial of β_i be $f_i(x)$, with roots $\beta_i = \beta_{i1}, \beta_{i2}, \ldots, \beta_{in_i}$; we order the roots so that the conjugate subgroups $H_i^{g_{ij}}$ $(j = 1, \ldots, n_i)$ correspond respectively to the conjugate subfields $R_o(\beta_{ij})$ $(j = 1,\ldots,n_i)$.

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

Similarly the intersection $\bigcap_{i=1}^{k} N_i$ corresponds to the composite of the fields $R_o(\beta_{i1},\ldots,\beta_{in_i})$ $(i = 1,\ldots,k)$; this composite is the splitting field of $\overline{f}(x) = f_1(x) \ldots f_k(x)$. But $\bigcap_{i=1}^{k} N_i = \left(\bigcap_{g\in G} H_1^g\right) \cap \ldots \cap \left(\bigcap_{g\in G} H_k^g\right) = 1$; the corresponding field is therefore K. $\overline{f}(x)$ thus has splitting field K, and so $\mathcal{G}(\overline{f}(x))$ is a

representation of G. Since $f_1(x), \ldots, f_k(x)$ are irreducible, the representation has k systems of transitivity of lengths $n_1, \ldots, n_k$; the subgroup which leaves fixed β_i is $\overline{H}_i \simeq H_i$, and so $\mathcal{G}(\overline{f}(x)) = \overline{G}$.

Corollary 1. We have $\overline{f}(x) = f_1(x) \ldots f_k(x)$, where deg $f_i(x) = [G:H_i]$. Thus deg $\overline{f}(x) = \sum_i [G:H_i]$, and so the minimum degree for $\overline{f}(x)$ is min $\sum_i [G:H_i]$ over all possible choices of $H_1, \ldots, H_k$.

Corollary 2. Taking $k = 1$ in the theorem and in Corollary 1, we obtain the following result :-

Let K be a field such that $\mathcal{G}(K) = G$. Let $\overline{\overline{G}}$ be any faithful representation of G as a transitive permutation group; then there exists an irreducible equation $\overline{\overline{f}}(x) = 0$ with Galois group $\overline{\overline{G}}$ and splitting field K. Since deg $\overline{\overline{f}}(x) = [G:H]$, the minimum degree for $\overline{\overline{f}}(x)$ is min $[G:H]$ over all subgroups H for which $\bigcap H^g = 1$.

Corollary 3. Let B_i be the splitting field $R_o(\beta_{i1}, \ldots, \beta_{in_i})$ of $f_i(x)$. B_i is a normal field, and is the fixed field under the automorphisms of the normal subgroup N_i of G. Thus $\mathcal{G}(f_i(x)) \simeq \mathcal{G}(B_i) \simeq G/N_i = G/\left(\bigcap_{g \in G} H_i^g\right)$.

Corollary 4. Suppose G is a direct product $G_1 \times \ldots \times G_m$. We can take $H_i = \bigotimes_{\substack{\lambda=1 \\ \lambda \neq i}}^{m} G_\lambda$; in this case

$\overline{f}(x) = f_1(x) \ldots f_m(x)$, where, by Corollary 3,

$$\mathcal{G}(f_i(x)) \simeq G/\left(\bigcap_{g\in G} H_i^g\right) = G/H_i \simeq G_i.$$

Let $\tilde{B}_i$ be the composite of the fields $B_1, \ldots, B_{i-1}, B_{i+1}, \ldots, B_m$; the subgroup of G for which $\tilde{B}_i$ is the fixed field is $\bigcap_{\substack{\mu=1\\ \mu\neq i}}^{m} H_\mu$, or G_i. B_i is the fixed field under the subgroup H_i, and so $B_i \cap \tilde{B}_i$ is the fixed field under the subgroup generated by G_i and H_i. But this is the whole group; thus $B_i \cap \tilde{B}_i = R_o$, and $K = \prod_{i=1}^{n} B_i$. This choice of subgroups H_i therefore gives $\overline{f}(x)$ as what could perhaps be called a direct product of the polynomials $f_1(x), \ldots, f_m(x)$.

Corollary 5. Suppose G is a semi-direct product $G_1 . G_2$ where $G_1 \triangleleft G$. We can take $H_1 = G_1$, $H_2 = G_2$; for

$$\left(\bigcap_{g\in G} H_1^g\right) \cap \left(\bigcap_{g\in G} H_2^g\right) = G_1 \cap \left(\bigcap_{g\in G} G_2^g\right) \subseteq G_1 \cap G_2 = 1.$$

We then obtain $\overline{f}(x) = f_1(x)\, f_2(x)$, where

$$\mathcal{G}(f_1(x)) \simeq G/\left(\bigcap_{g\in G} H_1^g\right) = G/H_1 \simeq G_2$$

$$\mathcal{G}(f_2(x)) \simeq G/\left(\bigcap_{g\in G} H_2^g\right) = G/\left(\bigcap_{g\in G} G_2^g\right).$$

The field K is thus the composite of the normal fields B_1 and B_2 with Galois groups G_2 and $G/\left(\bigcap_{g\in G} G_2^g\right)$ respectively. It may occur that $\bigcap_{g\in G} G_2^g = 1$; in this case $B_2 = K$ and $B_1 \subset B_2$.

The method of proof of Theorem 3.1 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 $R_o(\alpha_1, \ldots, \alpha_m)$ 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 (see, for instance, reference 1, p. 174 - 5, or reference 8, p. 126 - 7). The procedure is iterative, the basic step being to construct a primitive element ξ in a field $R_o(\lambda, \mu)$. Let the minimum polynomials of λ, μ, be $l(x)$, $m(x)$, respectively, with roots $\lambda = \lambda_1, \ldots, \lambda_r$ and $\mu = \mu_1, \ldots, \mu_s$. Consider the equations

$$\lambda_i + x\mu_j = \lambda_1 + x\mu_1 \quad \begin{pmatrix} i = 1, \ldots, r \\ j = 2, \ldots, s \end{pmatrix} \quad ;$$

each of them has not more than one root in R_o. We select a value c in R_o different from all these roots; then $\lambda_i + c\mu_j \neq \lambda_1 + c\mu_1 \quad \begin{pmatrix} i = 1, \ldots, r \\ j = 2, \ldots, s \end{pmatrix}$, and we show that $\xi = \lambda + c\mu$ is primitive in $R_o(\lambda, \mu)$.

The greatest common divisor of $l(\xi - cx)$ and $m(x)$ is $x - \mu$; for if any root other than μ of $m(x)$, say μ_j $(j \neq 1)$, were a root of $l(\xi - cx)$, we would

have $\xi - c\mu_j = \lambda_i$ (some i), which is not so. μ therefore lies in $R_o(\xi)$, and hence so does $\xi - c\mu$, or λ.

Thus we can construct a primitive element ξ_ρ in $R_o(\xi_{\rho-1}, \alpha_\rho)$ in the form $\xi_\rho + c_\rho\alpha_\rho$ for $\rho = 2, \ldots, m$, taking $\xi_1 = \alpha_1$. ξ_m can then be taken as θ.

We require now an element β_i in $R_o(\theta)$ such that $R_o(\beta_i)$ is the fixed field under the automorphisms of the subgroup H_i; we use the method given in reference 1, p. 211.

Consider the expression $\psi(k) = \prod_{h \in H_i} (k - h(\theta))$ $(k \in R_o)$. If under the isomorphism $\tilde{G} \simeq G$, the element g in G corresponds to the element $\tilde{g}$ in $\tilde{G}$, we have

$$g(\theta) = g(c_1\alpha_1 + \ldots + c_m\alpha_m) = c_1\alpha_{\tilde{g}(1)} + \ldots + c_m\alpha_{\tilde{g}(m)}.$$

$\psi(k)$ can therefore be computed as a function of k. Any automorphism $h_i \in H_i$ leaves $\psi(k)$ invariant; for

$$h_i(\psi(k)) = \prod_{h \in H_i} (k - hh_i(\theta)) = \prod_{h \in H_i} (k - h(\theta))$$

$\psi(k)$ is therefore an element of $R_o(\beta_i)$. Let

$$G = H_i + g_{i2}H_i + \ldots + g_{in_i}H_i \quad (g_{i1} = 1);$$

we have $g_{ij}(\psi(k)) = \prod_{h \in H_i} (k - g_{ij}h(\theta))$ $(j = 1, \ldots, n_i)$.

No two of these expressions are identical; for if

$g_{ij_1}(\psi(k)) \equiv g_{ij_2}(\psi(k))$ $(j_1 \neq j_2)$, then for any h in H_i there exists h' in H_i such that $g_{ij_1}h = g_{ij_2}h'$, and so $g_{ij_1}/g_{ij_2} \in H_i$, which is not so. A value for k in R_o can therefore be chosen so that the n_i values $g_{ij}\psi(k)$ are all different; $\psi(k)$ then has n_i, or $[G:H_i]$, different conjugates, and so is primitive in K_i and can be taken as β_i.

As in the proof of Theorem 3.1, we have

$$f_i(x) = \prod_{j=1}^{n_i} [x - g_{ij}(\psi(k))], \quad \text{and} \quad \bar{f}(x) = f_1(x) \ldots f_k(x).$$

<u>Examples.</u> 1. Let $\tilde{f}(x) = x^3 - r$ $(r \in R_o,\ r^{1/3} \notin R_o)$

$$= (x - r^{1/3})(x - wr^{1/3})(x - w^2r^{1/3})$$

where w is a primitive cube root of unity.
The discriminant of $\tilde{f}(x)$ is $-27r^2$; since this is not a square in R_o, $\tilde{G}$ is γ_3, the symmetric group of degree 3. The abstract group G is therefore defined by $\{a, b\}$, $a^3 = b^2 = (ab)^2 = 1$; the representation $\tilde{G}$ corresponds to the subgroup $H = \{b\}$. The splitting field K of $\tilde{f}(x)$ is $R_o(r^{1/3}, w)$; we construct an equation $\bar{f}(x)$ with the same splitting field and as Galois group $\bar{G}$ the regular representation of G.

The following table displays the corresponding elements of G, $\tilde{G}$, and $\bar{G}$.

G	$\widetilde{G}$ $(H = \{b\})$	$\overline{G}$ $(H = 1)$
1	$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix}$
b	$\begin{pmatrix} H & aH & a^2H \\ H & a^2H & aH \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$	$\begin{pmatrix} 1 & b & a & a^2 & ab & a^2b \\ b & 1 & a^2b & ab & a^2 & a \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 6 & 5 & 4 & 3 \end{pmatrix}$
a	$\begin{pmatrix} H & aH & a^2H \\ aH & a^2H & H \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & b & a & a^2 & ab & a^2b \\ a & ab & a^2 & 1 & a^2b & b \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 4 & 1 & 6 & 2 \end{pmatrix}$
a^2	$\begin{pmatrix} H & aH & a^2H \\ a^2H & H & aH \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$	$\begin{pmatrix} 1 & b & a & a^2 & ab & a^2b \\ a^2 & a^2b & 1 & a & b & ab \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 6 & 1 & 3 & 2 & 5 \end{pmatrix}$
ab	$\begin{pmatrix} H & aH & a^2H \\ aH & H & a^2H \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$	$\begin{pmatrix} 1 & b & a & a^2 & ab & a^2b \\ ab & a & b & a^2b & 1 & a^2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 2 & 6 & 1 & 4 \end{pmatrix}$
a^2b	$\begin{pmatrix} H & aH & a^2H \\ a^2H & aH & H \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & b & a & a^2 & ab & a^2b \\ a^2b & a^2 & ab & b & a & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 5 & 2 & 3 & 1 \end{pmatrix}$

Table 1.

We wish to construct a primitive element θ in K in the form $\theta = c_1 r^{1/3} + c_2 w r^{1/3} + c_3 w^2 r^{1/3}$. Since $R_o(r^{1/3}, wr^{1/3}, w^2 r^{1/3}) = R_o(r^{1/3}, wr^{1/3})$, we can take $c_3 = 0$ and $c_1 = 1$.

The expressions $\lambda_i + x\mu_j$ are $r^{1/3} + xr^{1/3}$, $wr^{1/3} + xr^{1/3}$, $w^2 r^{1/3} + xr^{1/3}$, $r^{1/3} + xw^2 r^{1/3}$, $wr^{1/3} + xw^2 r^{1/3}$, $w^2 r^{1/3} + xw^2 r^{1/3}$; since $\lambda_1 + x\mu_1 = r^{1/3} + xwr^{1/3}$, the only ineligible values for c_2 are $0, 1$. We take $c_2 = -1$, giving $\theta = r^{1/3} - wr^{1/3}$. Since the subgroup H corresponding to $\overline{G}$ is the identity, we can take $\beta = \theta$. The conjugates of θ, obtained by applying the elements of $\tilde{G}$ to the roots of $\tilde{f}(x)$, are $r^{1/3} - w^2 r^{1/3}$, $wr^{1/3} - w^2 r^{1/3}$, $w^2 r^{1/3} - r^{1/3}$, $wr^{1/3} - r^{1/3}$, $w^2 r^{1/3} - wr^{1/3}$; thus

$$\overline{f}(x) = (x - \overline{r^{1/3} - wr^{1/3}})\,(x - \overline{r^{1/3} - w^2 r^{1/3}})\,(x - \overline{wr^{1/3} - w^2 r^{1/3}})$$
$$(x - \overline{w^2 r^{1/3} - r^{1/3}})\,(x - \overline{wr^{1/3} - r^{1/3}})\,(x - \overline{w^2 r^{1/3} - wr^{1/3}})$$

$$= x^6 + 27r^2 .$$

[This result can be verified independently. Let $\overline{K}$ be the splitting field of $\overline{f}(x)$; we have $x^6 + 27r^2 = x^6 - (i\sqrt{3}\, r^{1/3})^6$, and so $\overline{K} = R_o(i\sqrt{3}\, r^{1/3}, -w)$, since $-w$ is a primitive 6^{th} root of unity. But $w = \frac{1}{2}\sqrt{3} - 1$; hence $\overline{K} = R_o(r^{1/3}, w) = K$. Thus $[\overline{K}:R_o] = 6$, and so $x^6 + 27r^2$ is normal; its Galois group is therefore the regular representation $\overline{G}$ of G.]

2. Using that $\overline{f}(x) = x^6 + 27r^2$ has group $\overline{G}$, we obtain an equation $\tilde{f}'(x)$ with the same splitting field and group $\tilde{G}$.

$x^6 + 27r^2$ is normal, and so we take $\theta = r^{1/3} - wr^{1/3}$. The representation $\tilde{G}$ corresponds to the subgroup $H = \{b\}$, thus $\psi(k) = \prod_{h\in\{b\}} (k - h(\theta)) = (k - \theta)(k - b(\theta))$. Since $G = H + aH + a^2H$, we can take $g_1 = 1$, $g_2 = a$, $g_3 = a^2$. The conjugates of $\psi(k)$ are :-

$$\psi(k) = (k - \theta)(k - b(\theta)) = (k - r^{1/3} - wr^{1/3})(k - r^{1/3} - w^2r^{1/3})$$
$$= k^2 - 3kr^{1/3} + 3r^{2/3}$$

$$a\psi(k) = (k - a(\theta))(k - ab(\theta)) = (k - wr^{1/3} - w^2r^{1/3})(k - wr^{1/3} - r^{1/3})$$
$$= k^2 - 3kwr^{1/3} + 3w^2r^{2/3}$$

$$a^2\psi(k) = (k - a^2(\theta))(k - a^2b(\theta)) = (k - w^2r^{1/3} - r^{1/3})(k - w^2r^{1/3} - wr^{1/3})$$
$$= k^2 - 3w^2kr^{1/3} + 3wr^{2/3}.$$

$k = 0$ therefore satisfies the condition that no two of $\psi(k)$, $a\psi(k)$, $a^2\psi(k)$ be equal. The corresponding equation is $\tilde{f}'(x) = (x - 3r^{2/3})(x - 3w^2r^{2/3})(x - 3wr^{2/3})$
$= x^3 - 27r^2$.

[The splitting field of $\tilde{f}'(x)$ is clearly $R_o(r^{1/3}, w)$, as it should be.]

Note. The method of Example 1 enables one to find a normal equation whose group is the full linear group of any given prime degree p. For any irreducible binomic equation $x^p - a$ has this group, and can be taken as $\tilde{f}(x)$. (see reference 1, pages 294 - 38)

Chapter II

Non-normal field extensions; a form for the roots of non-normal irreducible equations; application to nilpotent fields and equations.

§ 1. Non-normal field extensions

In Chapter I, the Galois group was defined only for a normal extension field; there are three different ways of defining a set $\mathcal{G}(K)$ analogous to a Galois group when K is a non-normal extension of R_o. Let $K = R_o(\alpha_1)$, and let the minimum polynomial of α_1 be $f(x) = (x - \alpha_1) \ldots (x - \alpha_n)$; let $\overline{K}$ be the splitting field of $f(x)$ over R_o. The three definitions are as follows :-

a) We can define $\mathcal{G}(K)$ to be $\mathcal{G}(\overline{K})$. This is used in, for instance, reference 8, p. 154. The set $\mathcal{G}(K)$ is then a group G, but it does not satisfy the relation $|\mathcal{G}(K)| = [K:R_o]$.

b) We can take $\mathcal{G}(K)$ to be the set M of all isomorphisms over R_o (including automorphisms) from K to its conjugate subfields in $\overline{K}$. These isomorphisms are induced by the mappings $\alpha \longrightarrow \alpha_i$ $(i = 1, \ldots, n)$. The set M is not a group, since there is a rule of combination only between those elements which are automorphisms. However, the relation $|M| = [K:R_o]$ holds. This set is the Loewy Mischgruppe; it is defined in a rather different way and

discussed extensively in reference 9. A Galois theory based on this definition is given in a paper by Baer (reference 10).

c) $\mathcal{G}(K)$ can be defined as the automorphism group S of K over R_o. S is clearly a subset of the set M.

If K is a normal extension each of these definitions leads to the Galois group as defined in ChapterI.

We prove a theorem relating the group S to the group G; it will be used in the next section. The result was obtained first in a different form by Loewy (reference 9) but his proof is quite different from the one given here.

Theorem 1.1. Let H be the subgroup of G which has K as fixed field. Then $S \simeq \mathcal{N}_G(H) / H$, where $\mathcal{N}_G(H)$ is the normalizer of H in G.

Proof. Let $a \in \mathcal{N}_G(H)$; a maps α_1 into one of its conjugates, and so induces an isomorphism $\sigma_a : R_o(\alpha_1) \rightarrow R(a\alpha_1)$. Since H is the subgroup of G which leaves fixed $R_o(\alpha_1)$, aHa^{-1} is the subgroup of G which leaves fixed $R_o(a\alpha_1)$. But $aHa^{-1} = H$, and so by the Fundamental Theorem of the Galois Theory $R_o(\alpha_1) = R_o(a\alpha_1)$. σ_a is thus an automorphism, and is an element of S. The automorphisms $\sigma_{aa'}$ and $\sigma_a \sigma_{a'}$ are both defined by $\alpha_1 \rightarrow aa'(\alpha_1)$, and so $a \rightarrow \sigma_a$ gives a homomorphism of $\mathcal{N}_G(H)$ 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 $\sigma\alpha_1$. The subgroups of G leaving fixed $R_o(\alpha_1)$ and $R_o(\sigma\alpha_1)$ are H and $a_\sigma H a_\sigma^{-1}$; since $R_o(\alpha_1) = R_o(\sigma\alpha_1)$, $H = a_\sigma H a_\sigma^{-1}$ and so $a_\sigma \in \mathcal{N}_G(H)$. The homomorphism is therefore onto.

The kernel of the homomorphism consists of all elements $a \in \mathcal{N}_G(H)$ for which σ_a is the identity (i.e. those which leave fixed $R_o(\alpha_1)$); it is therefore the group H, and so $S \simeq \mathcal{N}_G(H) / H$.

§ 2. The roots of f(x)

Using Theorem 1.1, we display the roots of $f(x)$ in a canonical form.

Since $\overline{K}$ is the splitting field of $f(x)$, $\mathcal{G}(f(x)) \simeq G$. H is the subgroup of G which leaves fixed K, or $R_o(\alpha_1)$. $\mathcal{G}(f(x))$ is therefore the transitive representation

$$\overline{\overline{G}} = \left\{ \begin{pmatrix} H, & gH, & \ldots, & g_m H \\ gH, & gg_2 H, & \ldots, & gg_m H \end{pmatrix} : \; g \in G \right\}$$

where $G = H + g_1 H + \ldots + g_m H$ (cf. Theorem I.2.1, corollary 1). The image $\overline{\overline{H}}$ of H under the isomorphism $G \simeq \overline{\overline{G}}$ is the stability subgroup leaving fixed the first digit.

Let $S = \{\sigma_i : i = 1, \ldots, s\}$. Since S is the

automorphism group of $R_o(\alpha_1)$, $\sigma_i\alpha_1$ is an element of $R_o(\alpha_1)$, and can be written $\phi_i(\alpha_1)$, where $\phi_i(x)$ is a polynomial of degree less than n, the degree of $f(x)$. $\phi_i(\alpha_1)$ 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 $R_o(\alpha_1)$.

Theorem 2.1. The roots $\alpha_1, \phi_2(\alpha_1), \ldots, \phi_s(\alpha_1)$ form a system of imprimitivity for $\overline{\overline{G}}$; 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 so $f(\phi_i(\alpha_r)) = 0$. 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 $R_o(\alpha_1) = R_o(\phi_i(\alpha_1)) = R_o(\phi_j(\alpha_r)) = R_o(\alpha_r)$, 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 $g \in \overline{\overline{G}}$; suppose g carries $\phi_k(\alpha_r)$ to $\phi_{k'}(\alpha_{r'})$. Then g carries the field $R_o(\phi_k(\alpha_r)) = R_o(\alpha_r)$ to the field $R_o(\phi_{k'}(\alpha_{r'})) = R_o(\alpha_{r'})$. 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 so 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 :-

$$\begin{array}{cccc} \alpha_1 & \phi_2(\alpha_1) & \dots & \phi_s(\alpha_1) \\ \vdots & & & \\ \alpha_m & \phi_2(\alpha_m) & \dots & \phi_s(\alpha_m) \end{array} \qquad (sm = n) ;$$

each row is a system of imprimitivity for $\bar{\bar{G}}$. The automorphism group S can be written $\{\sigma_i : \sigma_i(\alpha_1) = \phi_i(\alpha_1)\}$; it is isomorphic to the group of functions $\{\phi_i(x) \mod f(x) : i = 1, \dots, s\}$.

§ 3. Application to nilpotent fields and equations

We first define nilpotent groups, and state the results concerning them which will be used subsequently.

Definition 3.1. A group G is nilpotent if there exists a finite series $G = A_0 \supseteq A_1 \supseteq A_2 \supseteq \dots \supseteq A_r = 1$ such that
(i) $A_i \trianglelefteq G$ $(i = 1, \dots, r)$
(ii) A_{i-1} / A_i is contained in the centre of G/A_i $(i = 1, \dots, r)$.
This definition is applicable to finite and infinite groups; for finite groups the following definition is equivalent.

Definition 3.2. A finite group G is nilpotent if it is the direct product of its Sylow subgroups.

We shall require the following theorems :-

Theorem 3.3. Every proper subgroup of a nilpotent group is a proper subgroup of its normalizer.

Theorem 3.4. A finite group is nilpotent if and only if its maximal subgroups are normal.

Proofs can be found in reference 6, chapter 10. We now use Theorems 1.1 and 2.1 to characterize fields and equations whose Galois groups are nilpotent.

Theorem 3.5. A normal field N is a nilpotent extension of R_o (i.e. $\mathcal{G}(N)$ is nilpotent) if and only if every intermediate field between N and R_o has a non-trivial automorphism group.

Proof. a) Suppose that N is a nilpotent extension of R_o. Let K be any intermediate field between N and R_o, and let $\overline{K}$ be the smallest normal extension of R_o containing K. The Galois group G of $\overline{K}$ over R_o is a factor group of $\mathcal{G}(N)$, and hence is nilpotent. Let H be the subgroup of G which leaves K fixed; since we take $K \neq R_o$, H is a proper subgroup of G. Hence by Theorem 3.3, H is a proper subgroup of $\mathcal{N}_G(H)$. Thus if S is the automorphism group of K over R_o, by Theorem 1.1, $S \simeq \mathcal{N}_G(H) / H \neq 1$.

b) Suppose that every intermediate field between N and R_o has a non-trivial automorphism group over R_o. Let H be a maximal subgroup of $\mathcal{G}(N)$, and let K be the fixed field in N under the automorphisms of H. Let $K = R_o(\alpha)$,

and let $f(x)$, of degree n, be the minimum polynomial of α. Since K has a non-trivial automorphism group over R_o, K must contain at least one of the conjugates of α (i.e. α is not the only root of $f(x)$ in $R_o(\alpha)$).

Suppose $f(x)$ is not normal; let s be the number of its roots which lie in $R_o(\alpha)$. Then, as in Theorem 2.1, the roots of $f(x)$ have the form

$$\begin{array}{cccc} \alpha & \phi_2(\alpha) & \cdots & \phi_s(\alpha) \\ \vdots & & & \\ \alpha_m & \phi_2(\alpha_m) & \cdots & \phi_s(\alpha_m) \end{array} \qquad (sm = n,\ s < n);$$

each row is a system of imprimitivity for the Galois group of $f(x)$. Consider the expression $\psi(c) = \prod_{i=1}^{s} (c - \phi_i(\alpha))$ $(c \in R_o)$. Under the permutations of the Galois group of $f(x)$, $\psi(c)$ takes at most m different values; $\psi(c)$ therefore has degree at most m over R_o. No two conjugates of $\psi(c)$ can be identically equal, and so we can choose a value for c such that they are all different. $\psi(c)$ then has degree m over R_o.

Consider the field $R_o(\psi(c))$; we have

$$R_o(\alpha) \supset R_o(\psi(c)) \supset R_o \quad \text{(proper inclusions)}.$$

Let the subgroup of $\mathcal{G}(N)$ for which $R_o(\psi(c))$ is the fixed field be H_1; by the Fundamental Theorem of Galois Theory

$$H \subset H_1 \subset G \quad \text{(proper inclusions)} .$$

But this is not so, since H is maximal. $f(x)$ is therefore normal, and $R_o(\alpha)$ is a normal field; H is thus a normal subgroup of $\mathcal{G}(N)$. Hence, by Theorem 3.4, $\mathcal{G}(N)$ is nilpotent.

Note. N is equivalently characterized by the condition that every minimal intermediate field must have a non-trivial automorphism group. For suppose N satisfies this condition; let H be a maximal subgroup of $\mathcal{G}(N)$, and, as in part (b) of the preceding proof, let $R_o(\alpha)$ be the fixed field in N under the elements of H. Since H is maximal $R_o(\alpha)$ is minimal; for if there were an intermediate field between $R_o(\alpha)$ and R_o, the subgroup of $\mathcal{G}(N)$ leaving it fixed would be intermediate between H and $\mathcal{G}(N)$. $R_o(\alpha)$ therefore has non-trivial automorphism group; as before, it must then be a normal field, because otherwise the intermediate field $R_o(\psi(c))$ could be constructed. H is thus a normal subgroup, and $\mathcal{G}(N)$ nilpotent.

Corollary. Theorem 3.5 can 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 $\overline{G}$ if and only if, corresponding to any polynomial $p(\alpha_1, \ldots, \alpha_n)$ not in R_o, 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_o.

Proof. (a) Suppose $\overline{G}$ is nilpotent. Let $\beta = p(\alpha_1, \ldots, \alpha_n) \notin R_o$; then $R_o(\beta)$ is a subfield of the splitting field $\overline{K}$ of $f(x)$. Since $\overline{G}$ is nilpotent, by Theorem 3.5 $R_o(\beta)$ has a non-trivial automorphism group. Thus it contains at least one of its conjugates over R_o, i.e. there exists $q(x)$ such that β and $q(\beta)$ are different and conjugate over R_o.

b) Suppose that for every polynomial $p(\alpha_1, \ldots, \alpha_n)$ there exists a corresponding polynomial $q(x)$ with the required property/. Let $R_o(\beta)$ be any subfield of $\overline{K}$, the splitting field of $f(x)$. Since β lies in $\overline{K}$, $\beta = p(\alpha_1, \ldots, \alpha_n)$ for some polynomial p. Thus β has a conjugate $q(\beta) \neq \beta$, and the mapping $\beta \rightarrow q(\beta)$ gives an automorphism of $R_o(\beta)$. $R_o(\beta)$ therefore has a non-trivial automorphism group, and by Theorem 3.5, $\overline{G}$ is nilpotent.

The condition of Theorem 3.5 is clearly satisfied for abelian fields. Since every subgroup of an abelian group is normal, every intermediate field between N and R_o is normal, and so cannot have a trivial automorphism group.

Theorem 2.1 can be applied directly to characterize nilpotent equations of prime degree.

Theorem 3.6. An irreducible equation $f(x) = 0$ of prime degree has nilpotent Galois group if and only if it is normal, and so cyclic.

Proof. a) Suppose $f(x)$ has nilpotent Galois group $\overline{\overline{G}}$, and is not normal. As in Theorem 3.5, part (a), if α is a root of $f(x)$ there must be at least one more root of the form $\phi(\alpha)$. $\overline{\overline{G}}$ is therefore imprimitive. But this is impossible, since $\overline{\overline{G}}$ is of prime degree. $f(x)$ is therefore normal, and so cyclic.

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

Chapter III

Two methods for constructing irreducible equations with given group.

§ 1. A method for constructing equations with given Abelian group

Let A be any finite Abelian group. Then A can be written as a direct product of cyclic groups of prime power order; (see, for instance, ref. 6, p. 40).

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

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

$$p_1(\alpha_{11} \ldots \alpha_{1r_1}),\ p_2(\alpha_{21} \ldots \alpha_{2r_2}),\ \ldots,\ p_k(\alpha_{k1} \ldots \alpha_{kr_k})$$

as the invariants of A.

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

Consider the π^{th} cyclotomic field. Let ε_π denote a primitive π^{th} root of unity; it is a primitive element in this field. The Galois group $\mathcal{G}(R_0(\varepsilon_\pi))$ is

cyclic, of order $\Pi-1$ (reference 1, p. 312). We have constructed Π in such a way that m is a factor of $\Pi-1$; let $s = (\Pi-1)/m$. The Galois group $\mathcal{G}(R_0(\varepsilon_\Pi))$ contains a subgroup S which is cyclic of order s, and so there is a subfield B of $R_0(\varepsilon_\Pi)$ which is the fixed field under the automorphisms of this group. The Galois group of B is then isomorphic to the factor group $\mathcal{G}(R_0(\varepsilon_\Pi))/S$, and so to the cyclic group of order m.

A primitive element in the field B can be constructed as follows :-

Let the automorphism $\varepsilon_\Pi \rightarrow \varepsilon_\Pi^\rho$ be primitive in the cyclic group $\mathcal{G}(R_0(\varepsilon_\Pi))$ (i.e. ρ is a primitive $(\Pi-1)^{th}$ congruence root of 1 mod Π). Then the automorphism $\varepsilon_\Pi \rightarrow \varepsilon_\Pi^{\rho^m}$ is primitive in S.

$$\text{Let } \theta = \varepsilon_\Pi + \varepsilon_\Pi^{\rho^m} + \varepsilon_\Pi^{\rho^{2m}} + \ldots + \varepsilon_\Pi^{\rho^{(s-1)m}} ;$$

θ is clearly fixed under any automorphism in S. Consider the automorphism $\varepsilon_\Pi \rightarrow \varepsilon_\Pi^{\rho^f}$, where f is not a multiple of m (i.e. an automorphism in $\mathcal{G}(R_0(\varepsilon_\Pi))$ but not in S). Under this automorphism θ becomes

$$\phi = \varepsilon_\Pi^{\rho^f} + \varepsilon_\Pi^{\rho^{m+f}} + \ldots + \varepsilon_\Pi^{\rho^{(s-1)m+f}}$$

(The values of ϕ are the s-fold Gauss periods.) If $\theta = \phi$, ε_Π is a root of

$$x + x^{\rho^m \bmod \pi} + x^{\rho^{2m} \bmod \pi} + \ldots + x^{\rho^{(s-1)m} \bmod \pi}$$

$$= x^{\rho^f \bmod \pi} + x^{\rho^{m+f} \bmod \pi} + \ldots + x^{\rho^{(s-1)m+f} \bmod \pi} \quad \ldots\ldots\ldots\ldots \quad 1.1$$

This equation is of degree at most $\pi-1$, and cannot be an identity, since f is not a multiple of m. But the minimum polynomial of ε_π is $x^{\pi-1} + x^{\pi-2} + \ldots + 1 = 0$; equation 1.1 must therefore be this polynomial. This is impossible, since the powers occurring in equation 1.1 are all different, and the coefficients are not all the same. Thus $\theta \neq \phi$. θ is therefore primitive in the field B. Since B is the fixed field for a normal subgroup, it is a normal field.

For each pair (i, j) corresponding to a cyclic direct factor of A we now have a prime number π and a field B with primitive element θ. We denote these by π_{ij}, B_{ij}, θ_{ij}. We show that the field $R_o(\sum_i \sum_j \theta_{ij})$ has group A.

We use the following properties of cyclotomic fields :-

(a) Let $(n, n') = 1$; let ε_n and $\varepsilon_{n'}$ be primitive n^{th} and n'^{th} roots of unity respectively. Then $(\varepsilon_n \varepsilon_{n'})$ is a primitive $(nn')^{th}$ root of unity, and $R_o(\varepsilon_n \varepsilon_{n'}) = R_o(\varepsilon_n, \varepsilon_{n'})$.

(b) Under the conditions of (a), $R_o(\varepsilon_n) \cap R_o(\varepsilon_{n'}) = R_o$.

The composite of the fields $R_o(\varepsilon_{\pi_{ij}})$ (all i, j, except (i, j) = (1, 1)) is, by property (a), the n^{th} cyclotomic field, where $n = \prod_{\substack{\text{all } i,j \\ \text{except } (i,j)=(1,1)}} \pi_{ij}$.

Since the values π_{ij} are all different, $(n, \pi_{11}) = 1$. This composite therefore intersects $R_o(\varepsilon_{\pi_{11}})$ in R_o, by property (b). Consequently the composite of the fields B_{ij} (all i, j except (i, j) = (1, 1)) intersects B_{11} in R_o. The pair (1, 1) can be replaced by any one of the pairs (i, j), and so the direct product of the fields B_{ij} can be formed; its Galois group is the direct product of the Galois groups of the components, and so is isomorphic to A.

Consider the element $\sum_i \sum_j \theta_{ij}$ in $\prod \otimes B_{ij}$.

Each element θ_{ij} has $p_i^{\alpha_{ij}}$ conjugates, and so there are o(A) conjugate expressions of the form $\sum_i \sum_j \theta'_{ij}$, where θ'_{ij} is some conjugate of θ_{ij}. Suppose two of these expressions are equal; suppose $\sum_i \sum_j \theta'_{ij} = \sum_i \sum_j \theta''_{ij}$.

Then $\theta'_{11} - \theta''_{11} = \sum_{\substack{i \\ (i,j)\neq(1,1)}} \sum_j \theta''_{ij} - \sum_{\substack{i \\ (i,j)\neq(1,1)}} \sum_j \theta'_{ij}$.

Since all the fields B_{ij} are normal, the left side of the above equation is an element of B_{11} and the right side an element of $\overline{\bigotimes_{\substack{i,j \\ (i,j)\neq(1,1)}}} B_{ij}$. These fields intersect only in R_o, and so $\theta'_{11} - \theta''_{11} \in R_o$; set $\theta'_{11} = \theta''_{11} + r$. $\theta'_{11} \longrightarrow \theta''_{11}$ is an automorphism of B_{11} of some order; r must therefore be zero, and $\theta'_{11} = \theta''_{11}$. Similarly $\theta'_{ij} = \theta''_{ij}$. All the $o(A)$ conjugate expressions are thus different, and so $\sum_i \sum_j \theta_{ij}$ has degree $o(A)$ over R_o; it is therefore primitive in $\overline{\bigotimes} B_{ij}$.

$\overline{\bigotimes} B_{ij}$ is normal, and so 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 gives a field of group A as a subfield of $\overline{\bigotimes_{i,j}} R_o(\varepsilon_{\pi_{ij}})$, which is the cyclotomic field of index $\prod_{i,j} \pi_{ij}$. It was proved by Kronecker that every Abelian field is a subfield of some cyclotomic field; however our construction gives only those Abelian fields which

are subfields of cyclotomic fields of square free index.

Twp examples of this method are given, illustrating two different ways of carrying out the computation.

Example 1.2. We construct an equation for the group A with invariants 2(1,1) (i.e. $C_2 * C_2$ the four - group).

We require two different primes π_{11} and π_{12} such that $2 \mid \pi_{11}-1$ and $2 \mid \pi_{12}-1$; we take $\pi_{11} = 3$, $\pi_{12} = 5$.

Since $\pi_{11}-1 = 2$, in this case $s = 1$ and $\theta_{11} = \varepsilon_3$. We have $(\pi_{12}-1)/2 = 2$; here $s = 2$. We require a value for ρ, a primitive 4^{th} congruence root of 1 mod 5; $\rho = 2$ is such a value. Thus we can take

$$\theta_{12} = \varepsilon_5 + \varepsilon_5^{\rho^m} = \varepsilon_5 + \varepsilon_5^4 .$$

The field $R_o(\varepsilon_3 + \varepsilon_5 + \varepsilon_5^4)$ then has group A.

The conjugates of $(\varepsilon_3 + \varepsilon_5 + \varepsilon_5^4)$ are $(\varepsilon_3^2 + \varepsilon_5 + \varepsilon_5^4)$, $(\varepsilon_3 + \varepsilon_5^2 + \varepsilon_5^3)$, $(\varepsilon_3^2 + \varepsilon_5^2 + \varepsilon_5^3)$; the equation $f(x) =$

$$\{x-(\varepsilon_3+\varepsilon_5+\varepsilon_5^4)\}\{x-(\varepsilon_3^2+\varepsilon_5+\varepsilon_5^4)\}\{x-(\varepsilon_3+\varepsilon_5^2+\varepsilon_5^3)\}\{x-(\varepsilon_3^2+\varepsilon_5^2+\varepsilon_5^3)\} = 0$$

therefore has group A.

On multiplying and using the relations $\varepsilon_3^2+\varepsilon_3+1 = 0$,

$\varepsilon_5^4 + \varepsilon_5^3 + \varepsilon_5^2 + \varepsilon_5 + 1 = 0$, the equation becomes

$$f(x) = x^4 + 4x^3 + 5x^2 + 2x + 4 = 0.$$

[This result can be verified by obtaining the cubic resolvent (see reference 1, p. 252-3). The resolvent is $x^3 - 5x^2 - 8x + 12$, which has roots 1, -2, 6. $f(x)$ therefore has as group the four group.]

Example 1.3. We take $A \simeq C_2 \times C_3$; the invariants of A are $2(1)$, $3(1)$.

(A is isomorphic to the cyclic group of order 6; we therefore have immediately one equation of group A, the 7^{th} cyclotomic equation. We construct another one.)

We require primes π_{11} and π_{21} such that $2 \mid \pi_{11}-1$, $3 \mid \pi_{21}-1$; we take $\pi_{11} = 3$, $\pi_{21} = 7$. For $(1, 1)$, $s = 1$ and $\theta_{11} = \varepsilon_3$. For $(2, 1)$ $s = 2$. ρ must be chosen as a primitive 6^{th} congruence root of 1 mod 7; we take $\rho = 3$. Then $\theta_{21} = \varepsilon_7 + \varepsilon_7^{\rho^m} = \varepsilon_7 + \varepsilon_7^{3^3} = \varepsilon_7 + \varepsilon_7^6$. The field $R_o(\varepsilon_3 + \varepsilon_7 + \varepsilon_7^6)$ therefore has group A. Since this field is normal, an equation of degree 6 with $(\varepsilon_3 + \varepsilon_7 + \varepsilon_7^6)$ as a root will have group A.

Let $x = \varepsilon_3$; then $x^2 + x + 1 = 0$ ..... (1);

let $y = \varepsilon_7 + \varepsilon_7^6$; since $\varepsilon_7^6 + \varepsilon_7^5 + \varepsilon_6^4 + \varepsilon_7^3 + \varepsilon_7^2 + \varepsilon_7 + 1 = 0$

$$(\varepsilon_7^3 + \frac{1}{\varepsilon_7^3}) + (\varepsilon_7^2 + \frac{1}{\varepsilon_7^2}) + (\varepsilon_7 + \frac{1}{\varepsilon_7}) + 1 = 0$$

i.e. $(y^3 - 3y) + (y^2 - 2) + y + 1 = 0$

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

Let $z = x + y$; substituting $y = z - x$ in (2), then eliminating x between the resulting equation and (1), we have

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

Since this equation is of degree 6 it has group A.

§ 2. A method for constructing equations with given group.

This method is an extension of a method given in reference 5 for cyclic groups only. The proof given here of the basic theorem (Theorem 2.2) is new.

Let K be a normal algebraic extension of the rationals; let its Galois group G be $\{\sigma_1 = 1, \sigma_2, \ldots, \sigma_n\}$. Then there exists in K an element θ such that $\sigma_1(\theta), \ldots, \sigma_n(\theta)$ form a basis for K over R_o. Such a basis is called normal, and its existence is proved in, for instance, reference 11, p. 66. We consider K now as a hypercomplex algebra over R_o with basis elements $\sigma_1(\theta), \ldots, \sigma_n(\theta)$; let γ_{ij}^k $(i, j, k = 1, \ldots, n)$ be the structure constants of this algebra, defined by

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

[We note that this is not the group algebra of the Galois group G. The elements of G are automorphisms, and the group product $\sigma_i \sigma_j$ is given by $\sigma_i [\sigma_j(\theta)]$, not by $\sigma_i(\theta) . \sigma_j(\theta)$.]

Being linearly independent, $\sigma_1(\theta), \ldots, \sigma_n(\theta)$ are all different, and so are a complete set of conjugates; they are therefore the roots of an irreducible polynomial $f(x)$. This polynomial is normal, and its splitting field is K; its Galois group $\mathcal{G}(f(x))$ is thus the regular representation G_σ of G.

Lemma 2.1. θ can be so chosen that the values γ_{ij}^k have the following properties :-

$$(1) \quad \sum_m \gamma_{jk}^m \gamma_{im}^l = \sum_m \gamma_{ij}^m \gamma_{mk}^l \qquad (\text{all } i, j, k, l)$$

$$(2) \quad \gamma_{ij}^k = \gamma_{ji}^k \qquad (\text{all } i, j, k)$$

$$(3) \quad \sum_i \gamma_{ij}^k = \delta_{jk} \qquad (\text{all } j, k) \qquad (\text{Kronecker } \delta)$$

$$(4) \quad \gamma_{\sigma i, \sigma j}^{\sigma k} = \gamma_{ij}^k \qquad (\text{all } i, j, k, \text{ all } \sigma \in G_\sigma).$$

Proof. Let α_i denote $\sigma_i(\theta)$ $(i = 1, \ldots, n)$.

(1) Since K is associative, $\alpha_i(\alpha_j \alpha_k) = (\alpha_i \alpha_j)\alpha_k$;

thus $\sum_m \sum_l \gamma_{jk}^m \gamma_{im}^l \alpha_l = \sum_m \sum_l \gamma_{ij}^m \gamma_{mk}^l \alpha_l$.

Equating coefficients of α_l gives (1).

(2) Since K is commutative $\alpha_i \alpha_j = \alpha_j \alpha_i$.

Thus $\sum_k \gamma_{ij}^k \alpha_k = \sum_k \gamma_{ji}^k \alpha_k$. Equating coefficients of α_k gives (2).

(3) Let $\sum_i \alpha_i = r$; r is rational and non-zero. The set $\left\{\frac{\alpha_i}{r} : i = 1, \ldots, n\right\}$ is then also a normal basis for K, and we can replace θ by $\frac{\theta}{r}$. 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 gives (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

$$\alpha_{\sigma i} \alpha_{\sigma j} = \sum_k \gamma_{ij}^k \alpha_{\sigma k}, \text{ giving}$$

$$\sum_k \gamma_{\sigma i, \sigma j}^{\sigma k} \alpha_{\sigma k} = \sum_k \gamma_{ij}^k \alpha_{\sigma k}.$$

Equating coefficients of $\alpha_{\sigma k}$ gives (4).

When θ is chosen as in Lemma 2.1, the coefficients

of $f(x)$ can be expressed in terms of the values γ_{ij}^{k}. For let Γ represent the three-dimensional array of n^3 rational numbers γ_{ij}^{k}; let $\sigma\Gamma$ be the array obtained by writing $\gamma_{\sigma i,\sigma j}^{\sigma k}$ in place of γ_{ij}^{k}. For $\sigma \in G_\sigma$, $\Gamma = \sigma\Gamma$ (by (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

$$\sum_i a_i(\Gamma)\ \alpha_i = \phi(\alpha_1, \ldots, \alpha_n) = \phi(\alpha_{\sigma_r 1}, \ldots, \alpha_{\sigma_r n})$$

$$= \sum_i a_i(\sigma_r\Gamma)\ \alpha_{\sigma_r i} = \sum_i a_i(\Gamma)\ \alpha_{\sigma_r i}.$$

Equating coefficients of α_r, $a_r(\Gamma) = a_1(\Gamma)$; this is true for all r, and so $\phi(\alpha_1, \ldots, \alpha_n) = a_1(\Gamma) \sum_i \alpha_i$. We have chosen θ so that $\sum_i \alpha_i = 1$, giving $\phi(\alpha_1, \ldots, \alpha_n) = a_1(\Gamma)$. Thus each coefficient of $f(x)$ can be written as a polynomial in the elements of Γ.

Let $f(x) = x^n - s_1(\Gamma)\ x^{n-1} + \ldots + (-1)^n s_n(\Gamma)$.

We now show that if for a given group G we can find values of γ_{ij}^{k} satisfying conditions (1) ... (4) and such that the resulting polynomial $f(x)$ is irreducible, then $\mathcal{G}(f(x)) = G_{\sigma}$.

Theorem 2.2. Let G be a group of order n, and let its regular representation as a permutation group be G_{σ}. Let γ_{ij}^{k} $(i, j, k = 1, \ldots, n)$ be rational numbers satisfying

$$(1) \quad \sum_{m} \gamma_{jk}^{m} \gamma_{im}^{l} = \sum_{m} \gamma_{ij}^{m} \gamma_{mk}^{l} \qquad (\text{all } i, j, k, l)$$

$$(2) \quad \gamma_{ij}^{k} = \gamma_{ji}^{k} \qquad (\text{all } i, j, k)$$

$$(3) \quad \sum_{i} \gamma_{ij}^{k} = \delta_{jk} \qquad (\text{all } j, k)$$

$$(4) \quad \gamma_{\sigma i, \sigma j}^{\sigma k} = \gamma_{ij}^{k} \qquad (\text{all } i, j, k, \text{ all } \sigma \in G_{\sigma}).$$

From the values γ_{ij}^{k} a certain polynomial $f(x)$ with rational coefficients can be obtained; if the values γ_{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 (1) and (2), A is associative and commutative.

As previously, let Γ be the three-dimensional array of n^3 rational numbers γ_{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 before, since from (4) $\Gamma = \sigma\Gamma$ (all $\sigma \in G_\sigma$), we have $\phi(x_1, \ldots, x_n) = \sum_i a_i(\Gamma)\, x_i = a_1(\Gamma) \sum_i x_i$.

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

$$\overline{f}(x) = x^n - s_1(\Gamma)(\sum_i x_i)\, x^{n-1} + \ldots + (-1)^n s_n(\Gamma)(\sum_i x_i),$$

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 now $f(x) = x^n - s_1(\Gamma)\, x^{n-1} + \ldots + (-1)^n\, s_n(\Gamma)$.

From (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 for $a \in A$, $a(\sum_i x_i) = a$, and so $(\sum_i x_i)$ is an identity $\overline{1}$ in A.

Let $\overline{R_o}$ be the subset of A given by $\{r\overline{1} ;\ r \in R_o\}$. Since $\overline{1}$ is an identity, $\overline{R_o} \simeq R_o$, and so $\overline{R_o}$ is a field. $\overline{f}(x)$ is a polynomial over this field.

Suppose $f(x)$ is irreducible over R_o; then $\overline{f}(x)$ is irreducible over $\overline{R_o}$. Since $\overline{f}(x_1) = 0$,

$\overline{1}, x_1, \ldots, x_1^{n-1}$ form a basis for the extension field $\overline{R_o}(x_1)$. As these elements are linearly independent over $\overline{R_o}$, they are also linearly independent over R_o. They all belong to A, and A is of order n; hence they form a basis for A, and so $A = \overline{R_o}(x_1)$. As $x_2, \ldots, x_n$ also belong to A, it is a splitting field for $\overline{f}(x)$.

A is of order n over $\overline{R_o}$, and so $|\mathcal{G}(A/\overline{R_o})| = n$. But by (4), any permutation $\sigma \in G_\sigma$ of $x_1, \ldots, x_n$ gives an automorphism of A over $\overline{R_o}$, hence

$$\mathcal{G}(\overline{f}(x) \,/\, \overline{R_o}) = \mathcal{G}(A \,/\, \overline{R_o}) = G_\sigma.$$

Under the isomorphism $R_o \simeq \overline{R_o}$, the polynomial $f(x)$ is carried to $\overline{f}(x)$. Thus the splitting field of $f(x)$ is isomorphic to the splitting field of $\overline{f}(x)$, the roots of $f(x)$ being carried to the roots of $\overline{f}(x)$. (See reference 8, p. 108.) Hence

$$\mathcal{G}(f(x) \,/\, R_o) = \mathcal{G}(\overline{f}(x) \,/\, \overline{R_o}) = G_\sigma.$$

We note that 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 γ_{ij}^k. Also, conditions (1), (2), and (3) do not involve the structure of G. The equation

$$f(x) = x^n - s_1(\Gamma)\, x^{n-1} + \ldots + (-1)^n\, s_n(\Gamma) = 0$$

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).

2.3 Matrix formulation of the conditions on Γ.

Let $\Gamma_i = [\gamma_{ij}^k]$, $C_k = [\gamma_{ij}^k]$. Let $U = [u_{ij}]$ be the $(n \times n)$ matrix with $u_{ij} = 1$ (all i, j), and $U_{.k} = [u_{ij}^{.k}]$ be the $(n \times n)$ matrix with $u_{ij}^{.k} = \delta_{jk}$ (all i). Let P_σ be the $(n \times n)$ matrix obtained by applying the permutation σ to the columns of the identity matrix. (Premultiplication by P_σ and postmultiplication by P_σ' effect the permutation σ on the rows and columns respectively.)

Conditions (1) - (4) can now be written

(1) $\Gamma_k \Gamma_i = \Gamma_i \Gamma_k$ (all i, k)

(Condition (1) can only be written in this way if condition (2) is already satisfied.)

(2) C_k is symmetric (all k)

(3) $U C_k = U_{.k}$ (all k)

(4) $P_\sigma C_k P_\sigma' = C_{\sigma k}$ (all k, all $\sigma \in G_\sigma$)

or, equivalently, $P_\sigma \Gamma_i P'_\sigma = \Gamma_{\sigma i}$ (all i, all $\sigma \in G_\sigma$).

We show that these conditions are equivalent to the following :-

(a) C_1 is symmetric

(b) $U C_1 = U_{.1}$

(c) $C_{\sigma 1} = P_\sigma C_1 P'_\sigma$ (all $\sigma \in G_\sigma$)

(d) $\Gamma_1(P_\sigma \Gamma_1 P'_\sigma) = (P_\sigma \Gamma_1 P'_\sigma) \Gamma_1$ (all $\sigma \in G_\sigma$).

Clearly (1), (2), (3), (4) imply (a), (b), (c), (d). Assuming (a), (b), (c), (d) we prove (1), (2), (3), (4). Since G_σ is transitive, for any r there is an element σ_r in G_σ which carries 1 to r.

By (c), $C_i = P_{\sigma_i} C_1 P'_{\sigma_i}$.

$$\therefore \quad C'_i = P_{\sigma_i} C'_1 P'_{\sigma_i} = P_{\sigma_i} C_1 P'_{\sigma_i} \quad \text{(by (a))}$$

$$= C_i \qquad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (2)$$

$$U C_k = U P_{\sigma_k} C_1 P'_{\sigma_k} = U C_1 P'_{\sigma_k} = U_{.1} P'_{\sigma_k} \quad \text{(by (b))}$$

$$= U_{.k} \qquad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (3)$$

$$P_\sigma C_k P'_\sigma = P_\sigma P_{\sigma_k} C_1 P'_{\sigma_k} P'_\sigma = P_{\sigma\sigma_k} C_1 P'_{\sigma\sigma_k} = C_{(\sigma\sigma_k)1}$$

$$= C_{\sigma k} \qquad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (4)$$

$P_{\sigma_k} P'_{\sigma_k} = 1$; but $P_{\sigma_k} P_{\sigma_k^{-1}} = 1$, and so $P'_{\sigma_k} = P_{\sigma_k^{-1}}$.

Thus $\Gamma_k \Gamma_i = P_{\sigma_k} \Gamma_1 P'_{\sigma_k} P_{\sigma_i} \Gamma_1 P'_{\sigma_i}$ (from the equivalent form of (4))

$$= P_{\sigma_k} \Gamma_1 P'_{\sigma_k^{-1}} P_{\sigma_i} \Gamma_1 P'_{\sigma_i} P'_{\sigma_k^{-1}} P'_{\sigma_k}$$

$$= P_{\sigma_k} \Gamma_1 (P_{\sigma_k^{-1}\sigma_i} \Gamma_1 P'_{\sigma_k^{-1}\sigma_i}) P'_{\sigma_k}$$

$$= P_{\sigma_k} (P_{\sigma_k^{-1}\sigma_i} \Gamma_1 P'_{\sigma_k^{-1}\sigma_i}) \Gamma_1 P'_{\sigma_k} \quad \text{by (d)}$$

$$= P_{\sigma_i} \Gamma_1 P'_{\sigma_i} P_{\sigma_k} \Gamma_1 P'_{\sigma_k} = \Gamma_i \Gamma_k \ldots\ldots (1).$$

The final condition on Γ is that it must lead to an irreducible polynomial $f(x)$.

If values γ_{ij}^k satisfying conditions (1) ... (4) are known, the coefficients s_r of $f(x)$ can be computed from Γ_1 as follows :-

Let $\sum_i x_i^r = \overline{S}_r = S_r \overline{1}$ (S_r rational, since $\sum_i x_i^r$ is symmetric). Then from the isomorphism between A and the splitting field of $f(x)$ we have $\sum_i \alpha_i^r = S_r$.

We obtain expressions for the values S_r; the values of s_r are then given by Newton's equations.

By repeated application of the multiplication law,

x_i^r can be obtained as $m_{i1}^{(r)} x_1 + \ldots + m_{in}^{(r)} x_n$, where the values $m_{i1}^{(r)}, \ldots, m_{in}^{(r)}$ depend on Γ. Let

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

Hence $(x_i)^{r+1} = (\bar{m}_i^{(r)})'(x_i \bar{x}) = (\bar{m}_i^{(r)})' [\gamma_{ij}^k] \bar{x} = (\bar{m}_i^{(r)})' \Gamma_i \bar{x}$.

Thus $(\bar{m}_i^{(r+1)})' = (\bar{m}_i^{(r)})' \Gamma_i = (\bar{m}_i^{(r-1)})'(\Gamma_i)^2 = \ldots =$ $(\bar{m}_i^{(1)})'(\Gamma_i)^r$, and $(\bar{m}_i^{(r)})' = (\bar{m}_i^{(1)})'(\Gamma_i)^{r-1}$.

But $\Gamma_i = P_{\sigma_i} \Gamma_1 P'_{\sigma_i}$, and $(\Gamma_i)^{r-1} = P_{\sigma_i} (\Gamma_1)^{r-1} P'_{\sigma_i}$;

also $(\bar{m}_i^{(1)})'$ is given by $m_{ij}^{(1)} = \delta_{ij}$.

We have $(\bar{m}_i^{(1)})' P_{\sigma_i} = (\bar{m}_i^{(1)})' P'_{\sigma_i^{-1}} = [1,0,\ldots,0]$; hence $(\bar{m}_i^{(r)})'$ is the result of applying the permutation σ_i to the first row of $(\Gamma_1)^{r-1}$.

Now $S_r \bar{1} = \sum_i x_i^r = \sum_i (\bar{m}_i^{(r)})' \bar{x}$; equating coefficients of x_1, $S_r = \sum_i m_{i1}^{(r)}$.

Let $(\Gamma_1)^{r-1} = \left[c_{i,j}^{(r-1)}\right]$; then $m_{i1}^{(r)} = c_{1,\sigma_i^{-1}1}^{(r-1)}$,

and $S_r = \sum_i c^{(r-1)}_{1,\sigma_i^{-1}1}$. As i runs over 1 to n, $\sigma_i^{-1}1$ also runs over 1 to n; thus $S_r = \sum_i c^{(r-1)}_{1,i}$

i.e. S_r is the sum of the elements in the first row of $(\Gamma_1)^{r-1}$.

2.4 Application.

Theorem 2.2 reduces the problem of finding an equation with given Galois group to that of solving equations (1) ... (4) in R_o in such a way that the resulting polynomial f(x) is irreducible, or, equivalently, of finding a symmetric matrix C_1 satisfying conditions (b), (c), (d), for which f(x) is irreducible. The entries in C_1 can be taken as $\frac{1}{2}n(n+1)$ unknowns in R_o, and the conditions can be expressed as Diophantine equations in these unknowns. For obtaining the equations, the following procedure is convenient :-

(i) Write down C_1 in terms of $\frac{1}{2}n(n+1)$ unknowns.

(ii) Write the conditions $\sum_{i=1}^{n} \gamma^1_{ij} = \delta_{j1}$ (n linear equations).

(iii) Obtain the matrices C_k, using $C_k = P_{\sigma_k} C_1 P'_{\sigma_k}$.

(iv) Write down the matrices Γ_i; Γ_i has for its j^{th} column the i^{th} column of C_j.

(v) Write down the conditions $\sum_m \gamma_{jk}^m \gamma_{im}^l = \sum_m \gamma_{ij}^m \gamma_{mk}^l$ for $i = k+1, \ldots, n-1;\ j = 1, \ldots, n-1;\ k = 1, \ldots, n-2;\ l = 1$

($\frac{(n-1)^2 (n-2)}{2}$ quadratic equations).

We show that if the n equations (ii) hold, and if condition (v) is satisfied for the stated values of i, j, k, l, then it is satisfied for all i, j, k, l.

Assume (ii) and (v) are satisfied; let the relation $\sum_m \gamma_{jk}^m \gamma_{im}^l = \sum_m \gamma_{ij}^m \gamma_{mk}^l$ be denoted by (i, j, k, l). Since $\gamma_{ij}^k = \gamma_{ji}^k$, (i, j, k, l) implies

(k, j, i, l) (all j, l). ..... (1)

(i, j, k, l) is therefore true also for

$i = 1, \ldots, (n-2);\ j = 1, \ldots, (n-1);$

$k = (i+1), \ldots, (n-1);\ l = 1.$

Moreover it is trivially true for i = k ..... (2);

thus it is true for $i = 1, \ldots, (n-1);\ j = 1, \ldots, (n-1);\ k = 1, \ldots, (n-1);\ l = 1.$

Summing (i, j, k, l) over $i = 1, \ldots, n-1$, we have

$$\sum_{i=1}^{n-1} \sum_m \gamma_{jk}^m \gamma_{im}^l = \sum_{i=1}^{n-1} \sum_m \gamma_{ij}^m \gamma_{mk}^l$$

i.e. $$\sum_m \gamma_{jk}^m \left(\sum_{i=1}^{n-1} \gamma_{im}^l\right) = \sum_m \gamma_{mk}^l \left(\sum_{i=1}^{n-1} \gamma_{ij}^m\right)$$

But $\sum_{i=1}^{n} \gamma_{im}^l = \delta_{ml}$, and so $\sum_{i=1}^{n-1} \gamma_{im}^l = \delta_{ml} - \gamma_{nm}^l$;

similarly $\sum_{i=1}^{n-1} \gamma_{ij}^m = \delta_{jm} - \gamma_{nj}^m$.

Thus $$\sum_m \gamma_{jk}^m \left(\delta_{ml} - \gamma_{nm}^l\right) = \sum_m \gamma_{mk}^l \left(\delta_{jm} - \gamma_{nj}^m\right)$$

$$\therefore \gamma_{jk}^l - \sum_m \gamma_{jk}^m \gamma_{nm}^l = \gamma_{jk}^l - \sum_m \gamma_{mk}^l \gamma_{nj}^m$$

$\therefore$ (n, j, k, l) is true.

Hence by (1) (i, j, n, l) is true, and by (2) (n, j, n, l) is true. Similarly, summing (i, j, k, l) over $j = 1, \ldots, n-1$, it can be shown that (i, n, k, l) is true.

Since $\gamma_{ij}^k = \gamma_{\sigma i, \sigma j}^{\sigma k}$, (i, j, k, l) implies $(\sigma i, \sigma j, \sigma k, \sigma l)$. Thus (i, j, k, 1) implies $(\sigma_1 i, \sigma_1 j, \sigma_1 k, \sigma_1 1 = 1)$. But as i, j, k run over $1, \ldots, n$, so do $\sigma_1 i, \sigma_1 j, \sigma_1 k$.

$\therefore$ (i, j, k, 1) (all i, j, k) imply (i, j, k, l) (all i, j, k, l). (i, j, k, l) is therefore true for all i, j, k, l.

In reference 5, Young obtained general solutions of these Diophantine equations for the cyclic groups of orders 3, 4, and 5, and also obtained conditions for

the resulting polynomials to be irreducible; lengthy computations are involved.

Particular solutions for C_1 corresponding to a given group can be obtained, if solutions exist, by programming the Diophantine equations for a computer; $f(x)$ can then be calculated, and the reducibility examined by Kronecker's method.

The discussion preceeding Theorem 2.2 shows that for any group which can be a Galois group over R_o, there is a solution for Γ, and so for C_1, satisfying the required conditions. Thus, for instance, from the work of Šafarevič (reference 4) for any solvable group the method should yield irreducible polynomials $f(x)$. It also shows that for a given group G, every field K for which $\mathcal{G}(K) = G$ occurs as a splitting field of an irreducible polynomial $f(x)$ arising from some solution for C_1.

2.5 Example.

We take as group G the four group. The regular representation is $\sigma_1 = 1$, $\sigma_2 = (12)(34)$, $\sigma_3 = (13)(24)$, $\sigma_4 = (14)(23)$.

Let $C_1 = \begin{bmatrix} a & b & c & d \\ b & c & f & g \\ c & f & h & i \\ d & g & i & j \end{bmatrix}$; the conditions $\sum_i \gamma_{ij}^1 = \delta_{j1}$ give:

$$a + b + c + d = 1$$
$$b + e + f + g = 0$$
$$c + f + h + i = 0$$
$$d + g + i + j = 0.$$

We obtain

$$C_2 = \begin{bmatrix} e & b & g & f \\ b & a & d & c \\ g & d & j & i \\ f & c & i & h \end{bmatrix}, \quad C_3 = \begin{bmatrix} h & i & c & f \\ i & j & d & g \\ c & d & a & b \\ f & g & b & e \end{bmatrix}, \quad C_4 = \begin{bmatrix} j & i & g & d \\ i & h & f & c \\ g & f & e & b \\ d & c & b & a \end{bmatrix}.$$

Thus

$$\Gamma_1 = \begin{bmatrix} a & e & h & j \\ b & b & i & i \\ c & g & c & g \\ d & f & f & d \end{bmatrix}, \quad \Gamma_2 = \begin{bmatrix} b & b & i & i \\ e & a & j & h \\ f & d & d & f \\ g & c & g & c \end{bmatrix},$$

$$\Gamma_3 = \begin{bmatrix} c & g & c & g \\ f & d & d & f \\ h & j & a & e \\ i & i & b & b \end{bmatrix}, \quad \Gamma_4 = \begin{bmatrix} d & f & f & d \\ g & c & g & c \\ i & i & b & b \\ j & h & e & a \end{bmatrix}.$$

Sufficient values for i, j, k, l are :

$k = 1$, $i = 2, 3$; $k = 2$, $i = 3$

$j = 1, 2, 3$ $\qquad$ $j = 1, 2, 3$

$l = 1$ $\qquad$ $l = 1$.

The quadratic equations are therefore :-

$(2\ 1\ 1\ 1)$: $ab + ee + hf + jg = ba + bb + ic + id$

$(2\ 2\ 1\ 1)$: $bb + be + if + ig = ea + ab + jc + hd$

$(2\ 3\ 1\ 1)$: $cb + ge + cf + gg = fa + db + dc + fd$

$(3\ 1\ 1\ 1)$: $ac + ef + hh + ji = ca + gb + cc + gd$

$(3\ 2\ 1\ 1)$: $bc + bf + ih + ii = fa + db + dc + fd$

$(3\ 3\ 1\ 1)$: $cc + gf + ch + gi = ha + jb + ac + ed$

$(3\ 1\ 2\ 1)$: $bc + bf + ih + ii = cb + ge + cf + gg$

$(3\ 2\ 2\ 1)$: $ec + af + jh + hi = fb + de + df + fg$

$(3\ 3\ 2\ 1)$: $fc + df + dh + fi = hb + je + af + eg.$

The nine quadratic equations and the last three linear ones were programmed for a computer, to give integral solutions for the 10 variables a, ..., j. This work was done by Professor W.D. Thorpe, Director of the McGill Computing Centre. A large number of solutions was obtained.

We give a typical solution, obtain the function $f(x)$ from it, and verify its irreducibility.

A solution is : $a = 2$, $b = 2$, $c = -4$, $d = -4$, $e = 1$, $f = -5$, $g = 2$, $h = 5$, $i = 4$, $j = -2$.

For these values $a + b + c + d = -4$; to obtain a solution satisfying all the equations, we therefore divide each value by -4.

We have $$\Gamma_1 = \begin{bmatrix} a & e & h & j \\ b & b & i & i \\ c & g & c & g \\ d & f & f & d \end{bmatrix} = -\frac{1}{4}\begin{bmatrix} 2 & 1 & 5 & -2 \\ 2 & 2 & 4 & 4 \\ -4 & 2 & -4 & 2 \\ -4 & -5 & -5 & -4 \end{bmatrix};$$

thus $\Gamma_1^2 = \frac{1}{16}\begin{bmatrix} -6 & 24 & 4 & 18 \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \end{bmatrix}$

and $\Gamma_1^3 = -\frac{1}{64}\begin{bmatrix} -6 & 24 & 4 & 18 \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \end{bmatrix}\begin{bmatrix} 2 & 1 & 5 & -2 \\ 2 & 2 & 4 & 4 \\ -4 & 2 & -4 & 2 \\ -4 & -5 & -5 & -4 \end{bmatrix}$

$$= -\frac{1}{64}\begin{bmatrix} -52 & -40 & -40 & 44 \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \end{bmatrix} .$$

(We note that, as we require only the elements of the first row of Γ_1^{r-1}, it is necessary only to find the first row of the product at each stage.)

S_r is the sum of the elements in the first row of Γ_1^{r-1}; thus $S_2 = -\frac{3}{2}$, $S_3 = \frac{5}{2}$, $S_4 = \frac{11}{8}$. Also $S_1 = s_1 = 1$.

Newton's equations give

$$S_2 - S_1 s_1 + 2s_2 = 0 \quad : \quad s_2 = \frac{S_1 s_1 - S_2}{2} = \frac{5}{4}$$

$$S_3 - S_2 s_1 + S_1 s_2 - 3s_3 = 0 \quad : \quad s_3 = \frac{S_3 - S_2 s_1 + S_1 s_2}{3} = \frac{7}{4}$$

$$S_4 - S_3 s_1 + S_2 s_2 - S_1 s_3 + 4s_4 = 0 \quad : \quad s_4 = \frac{-S_4 + S_3 s_1 - S_2 s_2 + S_1 s_3}{4} = \frac{19}{16} .$$

Thus $f(x) = x^4 - x^3 + \frac{5}{4}x^2 - \frac{7}{4}x + \frac{19}{16}$, or, with integral

coefficients, $16\,f(x) = 16x^4 - 16x^3 + 20x^2 - 28x + 19$.

Writing $x = \frac{y}{2}$, $F(y) = 16\,f(x) = y^4 - 2y^3 + 5y^2 - 14y + 19$;

we verify the irreducibility of $F(y)$ by Kronecker's method (see, for example, reference 8).

By Gauss' Theorem, if $F(y)$ has factors, then it has factors with integral coefficients. All possible linear factors with integral coefficients are $y - 1$, $y + 1$, $y - 19$, $y + 19$. We have $F(+1) = 9$, $F(-1) = 41$, $F(+19) > 0$, $F(-19) > 0$; thus there are no linear factors with integral coefficients.

Suppose $g(y)$ is a quadratic factor with integral coefficients. We have $F(1) = 9$, $F(-1) = 41$, $F(0) = 19$; thus $g(1)$ can take values ± 1, ± 3, ± 9, $g(-1)$ can take values ± 1, ± 41, and $g(0)$ can take values ± 1, ± 19.

Let $g(y) = y^2 + ay + b$; $g(1) = 1 + a + b$,

$g(-1) = 1 - a + b$,

$g(0) = b$.

$$\therefore\ g(y) = y^2 + \frac{g(1) - g(-1)}{2} + g(0).$$

We need consider only the values ± 1 for $g(0)$; for if there is a factor with $g(0) = \pm 19$, there is also a factor with $g(0) = \pm 1$.

We have $F(2) = 11$; we tabulate the function $g(y)$ for $g(1) = \pm 1$, ± 3, ± 9, $g(-1) = \pm 1$, ± 41, $g(0) = +1$,

g(-1) \ g(1)	+1	-1	+3	-3	+9	-9
+1	y^2+1 $g(2)=5$	y^2-y+1 $g(2)=3$	y^2+y+1 $g(2)=7$	y^2-2y+1 $g(2)=1$	y^2+4y+1 $g(2)=13$	y^2-5y+1 $g(2)=-5$
-1	y^2+y+1 $g(2)=7$	y^2+1 $g(2)=5$	y^2+2y+1 $g(2)=9$	y^2-y+1 $g(2)=3$	y^2+5y+1 $g(2)=15$	y^2-4y+1 $g(2)=-3$
+41	$y^2-20y+1$ $g(2)=-37$	$y^2-21y+1$ $g(2)=-39$	$y^2-19y+1$ $g(2)=-33$	$y^2-22y+1$ $g(2)=-41$	$y^2-16y+1$ $g(2)=-27$	$y^2-25y+1$ $g(2)=-45$
-41	$y^2+21y+1$ $g(2)=47$	$y^2+20y+1$ $g(2)=45$	$y^2+22y+1$ $g(2)=49$	$y^2+19y+1$ $g(2)=43$	$y^2+25y+1$ $g(2)=55$	$y^2+16y+1$ $g(2)=37$

Table 2.

and obtain the corresponding values of $g(2)$ (Table 2). Values of $g(2)$ for $g(0) = -1$ are smaller by $+2$ than the corresponding values for $g(0) = +1$.

For $g(y)$ to be a factor of $F(y)$, $g(2)$ must divide 11. All possible factors are therefore y^2-2y+1, y^2-y-1, y^2+4y-1, y^2-2y-1.

We have $F(3) = 49$; the values of the four possible factors at $y = 3$ are $4, 5, 20, 2$. None of them can therefore be factors, and so $F(y)$ is irreducible.

By Theorem 2.2, $f(x) = 16x^4 - 16x^3 + 20x^2 - 28x + 19$ therefore has Galois group the four group.

[We verify this by obtaining the cubic resolvent of $f(x)$ (see reference 1, p. 252 - 3). This resolvent is $x^3 - \frac{5}{4}x^2 - 3x + \frac{27}{16}$, which has roots $-\frac{3}{2}, \frac{1}{2}, \frac{9}{4}$. Since these are rational, $f(x)$ has Galois group the four group.]

References

1. N. Tschebotaröw and H. Schwerdtfeger, Grundzüge der Galois'schen Theorie, Noordhoff, Groningen, (1950).

2. E. Noether, Gleichungen mit vorgeschriebener Gruppe, Math. Annalen, 78, 1917, pp. 221 - 229.

3. W. Kuyk and P. Mullender, On the Invariants of Finite Abelian Groups, Koninkl. Nederl. Akademie van Wetenschappen, Proceedings, Series A, 66, No. 2.

4. I.R. Šafarevič, Construction of fields of algebraic numbers with given solvable Galois group, Isv. Akad. Nauk S. S. S. R., ser. Mat. 18, 525 - 578 (1954), American Mathematical Society Translations, Series 2, vol. 4, p. 185.

5. L. Young, On certain cyclic extensions of the field of rational numbers, Applied Mathematics and Statistical Laboratories, Stanford University, Technical Report No. 1.

6. Marshall Hall, Jr., The Theory of Groups, Macmillan, New York, (1959).

7. H. Zassenhaus, The Theory of Groups (Second Edition), Chelsea, New York, (1958).

8. B.L. Van der Waerden, Modern Algebra, Vol. 1, Ungar, (1953).

9. A. Loewy, Neue elementare Begründung und Erweiterung der Galoisschen Theorie, Sitz - Ber. d. Heidelberger Akad. d. Wiss., 1925 (7) and 1927 (1).

10. R. Baer, Beitrage zur Galoisschen Theorie, Sitz - Ber. d. Heidelberger Akad. d. Wiss., 1928 (14).

11. E. Artin, Galois Theory, Notre Dame Mathematical Lectures No. 2, 2nd edition, (1959).