ON SOLUBLE IRREDUCIBLE GROUPS OF LINEAR SUBSTITUTIONS IN A PRIME NUMBER OF VARIABLES

BY

W. BURNSIDE

of GREENWICH, England.

It is well known that if a transitive permutation group of prime degree is soluble it must be cyclical or metacyclical; so that if the degree be p, the order of the group is pr, where r is equal to or is a factor of $p-1$.

I propose here to consider the corresponding question for an irreducible group of linear substitutions in a prime number of variables; and in particular to determine the numbers which may be the order of such a group when it is soluble.

1. A group of linear substitutions in p variables is called irreducible when it is impossible to find $q(<p)$ linear functions of the variables which are transformed among themselves by every operation of the group. It has recently been shown by Herr FROBENIUS[1] that if a group G, of finite order, is isomorphic (simply or multiply) with an irreducible group of linear substitutions in p variables, then p must be a factor of the order of G.

A group of linear substitutions in p symbols, which is of finite order and ABELIAN, is always completely reducible[2]; *i. e.*, a set of p independent

[1] Berliner Sitzungsberichte, 1896, p. 1382.

[2] I am not aware whether a separate proof of this statement has been published; but it is contained as a special case in Herr FROBENIUS's investigations in the *Berliner Sitzungsberichte* on the representation of a group by means of linear substitutions.

linear functions of the variables can always be found each of which is changed into a multiple of itself by every operation of the group.

If an irreducible group G in p variables, where p is a prime, has a self-conjugate subgroup H, then H must be either irreducible or ABELIAN. In fact, if H is reducible, new variables may be chosen which are transformed among themselves in sets of $n_1, n_2, \ldots, n_r$ by H, where

$$n_1 + n_2 + \ldots + n_r = p .$$

Since H is a self-conjugate subgroup of G, every operation of G must replace the variables of one of these sets by linear functions either of themselves or of the variables of another set; and since G is irreducible, it must contain operations replacing the variables of any one set by linear functions of those of any other set. Hence $n_1, n_2 \ldots, n_r$ must all be equal, and since p is prime they are all therefore unity; in other words H must be ABELIAN.

2. Suppose now that G is a soluble irreducible group in p variables, where p is a prime. Let I denote the self-conjugate subgroup of G which is constituted of its self-conjugate operations. Every operation of I replaces each variable by the same multiple of itself; and I is therefore necessarily cyclical. If n is its order, any one of its operations may be represented by

$$(\omega z_1, \omega z_2, \ldots, \omega z_p)$$

where ω is an n^{th} root of unity.

Let J be the greatest self-conjugate ABELIAN subgroup of G, so that J contains I, and suppose first that J contains operations which do not belong to I. Choose new variables so that J is represented as completely reduced, and let

$$(\varepsilon_1 z_1, \varepsilon_2 z_2, \ldots, \varepsilon_p z_p)$$

be any operation of J, which does not belong to I; so that $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_p$ are roots of unity which are not all the same. If, for every operation of J,

$$\varepsilon_1 = \varepsilon_2 = \ldots = \varepsilon_r ,$$

while $\varepsilon_{r+s} (s = 1, 2, \ldots p - r)$ is not equal to ε_1 for every operation, then every operation of G must either transform $z_1, z_2, \ldots, z_r$ linearly among themselves, or must change them into linear functions of another distinct

set of r z's. Since p is a prime and G is irreducible, this is impossible if r is greater than unity. Hence no two ε's are the same for every operation of J. There is therefore no linear functions of the z's, except the p z's themselves, which is changed into a multiple of itself by every operation of J. Every operation of G must therefore permute the z's among themselves, at the same time multiplying them by certain constant factors. If S and T are two operations of G which, apart from these factors, give the same permutation of the z's, then ST^{-1} replaces each z by a multiple of itself and therefore belongs to J. Hence the factor group $G|J$ is simply isomorphic with a permutation group of the p z's. Since G is irreducible this permutation group must be transitive; and since G is soluble the permutation group must be soluble. It is therefore a cyclical or a metacyclical group of degree p. If the order of J be m, the order of G is prm, while r is equal to or is a factor of $p-1$.

Also, if G is transformed so that J shall be completely reduced, every operation of G is of the form

$$z_i' = \omega_i z_{ai+b},$$

$$(i = 1, 2, \ldots, p)$$

where the ω's are roots of unity, and the suffixes are reduced, mod. p. A group of linear substitutions in which every operation replaces each symbol by a multiple of itself or of another symbol, I call a permutation group *with factors*. The result of the present section then is that when I is not the greatest self-conjugate ABELIAN subgroup of G, it is possible to represent G as a cyclical or metacyclical permutation group with factors.

3. It remains to consider the case in which the group I, formed of the self-conjugate operations of G, is the greatest ABELIAN self-conjugate subgroup contained in G. Of the self-conjugate subgroups of G which contain I, let H be one whose order is as small as possible. The order of $H|I$ is then a power of a prime. Since by supposition H is not ABELIAN, it must be irreducible. The order of $H|I$ being a power of a prime, it must have self-conjugate operations other than identity. Hence H must have an ABELIAN self-conjugate subgroup containing and of greater order than I. Let J be the subgroup of greatest order of this kind contained in H. The operations of J cannot all multiply each z by the same

factor, for they would then all be self-conjugate in G. Hence the operations of J are not all self-conjugate in H; and therefore H is an actual subgroup of, and is not identical with, G.

Since H is irreducible and has an ABELIAN self-conjugate subgroup J, whose operations are not all self-conjugate, it can be represented as a cyclical or metacyclical permutation group with factors; and since the order of $H \mid I$ is the power of a prime, that of $H \mid J$, which is at once a factor of $p(p-1)$ and of the order of $H \mid I$, must be p. Hence H can be represented as a cyclical permutation group with factors.

Now G can certainly not be so represented. For in such a group the totality of the operations which replace each symbol by a multiple of itself constitute an ABELIAN self-conjugate subgroup; and if every one of these operations replaces each symbol by the same multiple of itself, G would not be irreducible. Hence since H, which is a self-conjugate subgroup of G, can be represented as a permutation group with factors while G cannot, it must be possible to represent H in more than one way as such a group.

Let
$$(\varepsilon_1 z_1, \varepsilon_2 z_2, \ldots, \varepsilon_p z_p)$$
represent any operation P of J which does not belong to I, so that $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_p$ are roots of unity which are not all equal to each other. Further let
$$(\alpha_1 z_2, \alpha_2 z_3, \ldots, \alpha_{p-1} z_p, \alpha_p z_1)$$
be an operation S of H, not belonging to J. It may be assumed without loss of generality that $\alpha_1, \alpha_2, \ldots, \alpha_{p-1}$ are all unity; for this is equivalent to taking $z_1, \alpha_1 z_2, \alpha_1 \alpha_2 z_3, \ldots$ as variables in the place of $z_1, z_2, z_3, \ldots$, and does not affect the form of the operations of J. The operation S may therefore be written in the form
$$(z_2, z_3, \ldots, z_p, \eta z_1).$$

Let
$$\zeta = \beta_1 z_1 + \beta_2 z_2 + \ldots + \beta_p z_p$$
be one of a second set of p linear functions of the z's which are permuted among themselves with factors by H. When the operation P is carried out on the z's, ζ becomes
$$\zeta' = \beta_1 \varepsilon_1 z_1 + \beta_2 \varepsilon_2 z_2 + \ldots + \beta_p \varepsilon_p z_p,$$

and this is not a multiple of ζ. Hence when all the operations of J are carried out on the variables the number of distinct linear functions which arise from ζ, no one of which is a multiple of any other, is equal to the order of $J|I$. This is a power of p in any case, and must be equal to p if, as supposed, H can be represented as a permutation group with factors in the ζ's.

Since the order of $J|I$ is p, the p^{th} power of P must belong to I. Hence P must be of the form

$$(\varepsilon_1 \alpha^{a_1} z_1, \varepsilon_1 \alpha^{a_2} z_2, \ldots, \varepsilon_1 \alpha^{a_p} z_p),$$

where α is a p^{th} root of unity.

Further $P^{-1}S^{-1}PS$ must for the same reason belong to I, and therefore $a_{i+1} - a_i$ is independent of i. The operation P is therefore of the form

$$(\varepsilon_1 z_1, \varepsilon_1 \alpha z_2, \varepsilon_1 \alpha^2 z_3, \ldots, \varepsilon_1 \alpha^{p-1} z_p).$$

The p linear functions that arise from ζ by the operations of J are therefore

$$\sum_{i=1}^{i=p} \beta_i \alpha^{t(i-1)} z_i,$$

$$(t = 0, 1, \ldots, p-1).$$

These must be permuted among themselves with factors by S. They are also permuted by P; and therefore it must be possible to determine m so that SP^m changes one of the ζ's, and therefore all of them, into a multiple of itself. The conditions that ζ may be changed into a multiple of itself by SP^m are

$$\frac{\beta_2}{\beta_1} = \frac{\beta_3}{\beta_2}\alpha^{-m} = \frac{\beta_4}{\beta_3}\alpha^{-2m} = \ldots = \frac{\beta_p}{\beta_{p-1}}\alpha^{2m} = \eta^{-1}\frac{\beta_1}{\beta_p}\alpha^m.$$

When m is assigned these equations determine the ratios of the β's uniquely, and give

$$\frac{\beta_{i+1}}{\beta_1} = \alpha^{\frac{1}{2}mi(i-1)}\eta^{\frac{i}{p}}.$$

Hence if

$$\zeta_{m,n} = \sum_{i=0}^{i=p-1} \alpha^{\frac{1}{2}mi(i-1)+ni} \eta^{\frac{i}{p}} z_{i+1},$$

each of the p sets of p linear functions

$$\zeta_{m,0}, \zeta_{m,1}, \ldots, \zeta_{m,p-1},$$
$$(m = 0, 1, \ldots, p-1)$$

is such that H can be represented as a permutation group with factors in terms of them. Further, these and the z's themselves are the only sets of linear functions of the z's in respect of which H can be so represented. There are therefore just $p+1$ sets of linear functions in terms of which H can be represented as a permutation group with factors.

Since the p^{th} powers of both S and P belong to I, the factor group $H|I$ is a non-cyclical group of order p^2. H has therefore $p+1$ self-conjugate ABELIAN subgroups of index p containing I; and the $p+1$ sets of linear functions give the variables in terms of which each of these subgroups can be represented in completely reduced form.

4. To every operation of G there corresponds an isomorphism of H, and therefore also of $H|I$. The totality of the operations of G, which give the identical isomorphism of $H|I$, constitute a self-conjugate subgroup K of G; and I have shown elsewhere[1] that the order of $K|H$ is a power of p. But J is a self-conjugate subgroup of K, and from § 2 it follows that the order of $K|J$ is equal to or is a factor of $p(p-1)$. Moreover the order of $H|J$ has been shewn to be p. Hence K must be identical with H, and therefore the only operations of G which give the identical isomorphism of $H|I$ are those of H. The factor group $G|H$ is therefore simply isomorphic with a (soluble) subgroup of the group of isomorphisms of a non-cyclical ABELIAN group, order p^2. Moreover this group of isomorphisms can leave no subgroup of order p of the ABELIAN group, order p^2, invariant; for if it did, H would have a subgroup of index p, containing I, and self-conjugate in G, which is not the case. Hence the group of isomorphisms, with which $G|H$ is simply isomorphic, must contain at least one operation which permutes the $p+1$ subgroups

[1] Theory of Groups of finite order (Cambridge), p. 253.

of order p of the ABELIAN group, order p^2, regularly. Now the operations of the group of isomorphisms of a non-cyclical ABELIAN group of order p^2, may be divided into sets which (I) permute the $p+1$ subgroups of order p regularly, (II) leave one such subgroup invariant and permute the remaining p cyclically, (III) leave every operation of one subgroup invariant, change every operation of a second subgroup into a power of itself and permute the remaining subgroups cyclically; and (IV) change every operation into its x^{th} $(x = 1, 2, \ldots, p-1)$ power.

GIERSTER's[1] discussion of the modular group shows that no group containing operations from sets (I) and (II) can be soluble. Hence, since $G|H$ contains operations belonging to (I), it can have none belonging to (II). Suppose now that G has an operation A, given by

$$z_i' = \sum_1^p a_{ij} z_j \qquad (i=1,2,\ldots,p)$$

which gives rise to an isomorphism of $H|I$ belonging to (III). We may then suppose that

$$A^{-1}PA = P^x R,$$

$$A^{-1}SA = SR',$$

where R and R' belong to I. The resulting conditions for the coefficients in A are found to be

$$a_{i,j}(\alpha^{x(i-1)} - k\alpha^j) = 0,$$

$$a_{i,j} - l a_{i+1,j+1} = 0,$$

where k and l are the same for all i's and j's. These conditions are inconsistent, unless x is unity; in which case the isomorphism is the identical isomorphism. Again if A gives rise to an isomorphism belonging to set (IV), we have

$$A^{-1}PA = P^x R,$$

$$A^{-1}SA = S^x R',$$

and the resulting conditions for the $a_{i,j}$'s are

$$a_{i,j}(\alpha^{x(i-1)} - k\alpha^j) = 0,$$

$$a_{i,j} - l a_{i+x,j+1} = 0.$$

[1] Math. Ann. Vol. XVIII, pp. 319—365.

These again are inconsistent unless $x^2 \equiv 1$, mod. p. Hence $G \mid H$ contains no operation of set (III) and the only operation it can contain of set (IV) is the one which replaces every operation by its inverse. Finally therefore every operation of $G \mid H$ must either permute the $p + 1$ subgroups of order p regularly, or must leave them all invariant; and the subgroup of $G \mid H$ which leaves them all invariant consists either of the identical operation only or is of order two. The order of $G \mid H$ is therefore a factor of $2(p + 1)$. The order of G itself is then p^2sn, where s is a factor of $2(p + 1)$ and n is the order of the subgroup constituted by the self-conjugate operations of G. It should be noticed that n is necessarily divisible by p, since $P^{-1}S^{-1}PS$, which multiplies each z by α, belongs to I.

5. (*Summary*). Soluble irreducible groups of linear substitutions in a prime number of variables may, from the preceding investigation, be divided into two classes according as they do or do not contain self-conjugate ABELIAN subgroups other than that formed of their self-conjugate operations.

Those of the first class are multiply isomorphic with a cyclical or metacyclical permutation group of prime degree in respect of the self-conjugate ABELIAN subgroup of greatest order which they contain. The order of such a group is prm, where p is the number of variables, r a factor of $p - 1$ and m the order of the greatest self-conjugate ABELIAN subgroup. It can be represented as a cyclical or metacyclical permutation group with factors. A group with no self-conjugate operations, except identity, necessarily belongs to this class.

Those of the second class are multiply isomorphic, in respect of the subgroup formed of their self-conjugate operations, with a soluble subgroup of the holomorph of a non-cyclical ABELIAN group, order p^2. The order of such a group is p^2sn; where p is the number of variables, s a factor of $2(p + 1)$, and n (which must be divisible by p) is the order of the subgroup formed of the self-conjugate operations. Such a group cannot be represented as a permutation group with factors.