LINEAR GROUPS ANALOGOUS TO PERMUTATION GROUPS

W. J. WONG

(received 25 October 1962)

If G is a finite linear group of degree n, that is, a finite group of automorphisms of an n-dimensional complex vector space (or, equivalently, a finite group of non-singular matrices of order n with complex coefficients), I shall say that G is a *quasi-permutation group* if the trace of every element of G is a non-negative rational integer. The reason for this terminology is that, if G is a permutation group of degree n, its elements, considered as acting on the elements of a basis of an n-dimensional complex vector space V, induce automorphisms of V forming a group isomorphic to G. The trace of the automorphism corresponding to an element x of G is equal to the number of letters left fixed by x, and so is a non-negative integer. Thus, a permutation group of degree n has a representation as a quasi-permutation group of degree n.

It seems reasonable to ask whether properties of permutation groups carry over to quasi-permutation groups. In this note I show the validity for quasi-permutation groups of the following simple properties of permutation groups G of degree n:

(i) The order $|G|$ is a divisor of $n!$

(ii) If p is a prime number exceeding $\sqrt{n}$, then the Sylow p-group of G is of elementary Abelian type.

First, a result on roots of unity.

LEMMA 1. *Suppose that the rational integer s is a sum of n p^a-th roots of* 1, *where p is a prime number. Then,*

(i) *each primitive p-th root of* 1 *occurs the same number of times;*

(ii) *if $s \geqq 0$, then the root* 1 *occurs at least as many times as any primitive p-th root of* 1;

(iii) *the number of roots occurring which are not p-th roots of* 1 *is a multiple of p; and*

(iv) $s \equiv n \pmod{p}$.

PROOF. Let the p^a-th roots of 1 be

$$1, \omega, \omega^2, \cdots, \omega^{p^a-1}.$$

Then, the primitive p-th roots of 1 are $\omega^t, \omega^{2t}, \cdots, \omega^{(p-1)t}$, where $t = p^{a-1}$.

https://doi.org/10.1017/S1446788700027920 Published online by Cambridge University Press

Therefore, the following t linear dependence relations amongst the roots hold:

$$(1)\qquad \omega^k + \omega^{t+k} + \omega^{2t+k} + \cdots + \omega^{(p-1)t+k} = 0 \qquad (k = 0, 1, \cdots, t-1).$$

Now, if Q denotes the rational field, the roots $1, \omega, \omega^2, \cdots$ span $Q(\omega)$ as a vector space over Q. Since this vector space has dimension $p^{a-1}(p-1) = p^a - t$ [2, pp. 112, 162], there can be just t linearly independent linear dependence relations amongst the roots with coefficients in Q. Since the relations (1) are clearly linearly independent, every linear dependence relation amongst the roots, with coefficients in Q, is a linear combination of the relations (1).

Now suppose that

$$s = a_0 + a_1\omega + a_2\omega^2 + \cdots, \sum a_i = n.$$

The dependence relation

$$a_0 - s + a_1\omega + a_2\omega^2 + \cdots = 0$$

must be a linear combination of the relations (1). Hence,

$$a_0 - s = a_t = a_{2t} = \cdots = a_{(p-1)t},$$
$$a_k = a_{t+k} = a_{2t+k} = \cdots = a_{(p-1)t+k} \quad (k = 1, \cdots, t-1).$$

The first string of equations proves (i) and (ii), and the other shows that p divides the sum of all the a_i for which i is not divisible by t, that is, that (iii) holds. For (iv),

$$n = \sum a_i = (a_t + s) + (p-1)a_t + pa_1 + pa_2 + \cdots + pa_{t-1}$$
$$\equiv s \pmod p.$$

THEOREM 1. *The order of a quasi-permutation group G of degree n is a divisor of n!*

PROOF. Let P be a Sylow p-group of G, of order p^a. If $x \in P$, the trace $\chi(x)$ of x is the sum of n p^a-th roots of 1, and so, by Lemma 1 (iv), is of the form $n - rp$, where r is an integer. Since the only p^a-th root of 1 which has real part as large as 1 is 1 itself, $r \geqq 0$, and $r = 0$ only if x is the identity. Since $\chi(x) \geqq 0$, $r \leqq N$, where $N = [n/p]$, the integer part of n/p. For $r = 0, 1, \cdots, N$, let h_r be the number of elements of P with trace $n - rp$. For any non-negative integer q, χ^q is a (possibly reducible) character of P, and so [1, p. 263]

$$\sum_{x \in G} \chi(x)^q \equiv 0 \pmod{p^a},$$

i.e.,

$$\sum_{r=0}^{N} h_r(n - rp)^q \equiv 0 \pmod{p^a} \quad (q = 0, 1, 2, \cdots).$$

https://doi.org/10.1017/S1446788700027920 Published online by Cambridge University Press

This is the case $k = 0$ of the congruences

$$(2) \qquad k!\,p^k \sum_{r=0}^{N-k} \binom{N-r}{k} h_r (n-rp)^q \equiv 0 \pmod{p^a} \quad (q = 0, 1, 2, \cdots).$$

If we suppose that these congruences hold for a particular value of k, then they can be proved for $k+1$ by multiplying (2) by $n-(N-k)p$ and subtracting from the congruence with $q+1$ in place of q. Hence, by induction on k, (2) is valid. The case $k = N$, $q = 0$ gives

$$N!\,p^N \equiv 0 \pmod{p^a},$$

since $h_0 = 1$. But, $N!\,p^N = p \cdot 2p \cdot 3p \cdots Np$ is a divisor of $n!$, since $Np \leqq n$. Hence p^a divides $n!$ Since this holds for all prime divisors p of $|G|$, we have the result.

LEMMA 2. *If P is a Sylow p-group of a quasi-permutation group G of degree n smaller than p^2, then no element of P has order exceeding p.*

PROOF. Suppose if possible that P has an element x of order p^2. The trace $\chi(x)$ is a sum of p^2-th roots of 1. By Lemma 1 (iii), the number of primitive p^2-th roots of 1 occurring is a multiple of p. Hence, the number of primitive p-th roots of 1 occurring in $\chi(x^p)$ is a multiple of p. But, by Lemma 1 (i), the $p-1$ primitive p-th roots of 1 all occur in $\chi(x^p)$ the same number of times. Hence each occurs at least p times. But, by Lemma 1(ii), this implies that the root 1 also occurs at least p times in $\chi(x^p)$, so that the total number of roots occurring is at least p^2, contradicting the assumption that $n < p^2$.

LEMMA 3. *If T is a permutation group of degree n, whose order is a power of a prime number p greater than $\sqrt{n}$, then T contains a permutation*

$$(a_{11} \cdots a_{1p})(a_{21} \cdots a_{2p}) \cdots (a_{m1} \cdots a_{mp})$$

such that every element of T is of the form

$$(3) \qquad (a_{11} \cdots a_{1p})^{r_1}(a_{21} \cdots a_{2p})^{r_2} \cdots (a_{m1} \cdots a_{mp})^{r_m}.$$

In particular, T is of elementary Abelian type.

PROOF. If $N = [n/p]$, then, since $p^2 > n$, the Sylow p-group S_p of the symmetric group of degree n has order p^N. The cycles

$$(kp+1, kp+2, \cdots, (k+1)p) \quad (k = 0, 1, \cdots, N-1)$$

clearly generate an elementary Abelian group of order p^N, which may therefore be taken as S_p. Since T must be similar to a subgroup of S_p, it follows that T is elementary Abelian and that the letters moved by T can be arranged in an order $a_{11}, \cdots, a_{1p}, a_{21}, \cdots, a_{mp}$, such that every element of T is of the form (3).

https://doi.org/10.1017/S1446788700027920 Published online by Cambridge University Press

Suppose that x is an element of T moving as many letters as possible:

$$x = (a_{11} \cdots a_{1p})^{s_1}(a_{21} \cdots a_{2p})^{s_2} \cdots (a_{m1} \cdots a_{mp})^{s_m}.$$

Suppose if possible that $s_1 \equiv 0 \pmod{p}$. There exists an element y of T moving a_{11}:

$$y = (a_{11} \cdots a_{1p})^{t_1}(a_{21} \cdots a_{2p})^{t_2} \cdots (a_{m1} \cdots a_{mp})^{t_m},\ t_1 \not\equiv 0 \pmod{p}.$$

Now, it is possible to choose an integer k such that

$$k \not\equiv 0 \pmod{p}, \quad \text{and}$$
$$s_i + kt_i \not\equiv 0 \pmod{p} \text{ for all } i \text{ such that } s_i \not\equiv 0 \pmod{p}.$$

For, each incongruence is violated by at most one value of $k \pmod{p}$, and there are at most m incongruences. Since $m \leqq n/p < p$, there is a common solution k to all the incongruences. But then xy^k moves more letters than x, a contradiction. Hence $s_1 \not\equiv 0 \pmod{p}$, and similarly $s_i \not\equiv 0 \pmod{p}$, all i. Replacement of $(a_{i1} \cdots a_{ip})$ by $(a_{i1} \cdots a_{ip})^{s_i}$ gives the result.

THEOREM 2. *The Sylow p-group of a quasi-permutation group of degree n smaller than p^2 is of elementary Abelian type.*

PROOF. Let P be the Sylow p-group in question. P may be written as a group of monomial transformations [1, p. 231], that is, there is a basis $e_1, \cdots, e_n$ of the vector space V on which P acts, such that, for x in P, $1 \leqq i \leqq n$,

$$e_i^x = a(i, x)e_j,$$

where $a(i, x)$ is a scalar, and $j = j(i, x)$ is one of the integers $1, \cdots, n$. For a given x, the correspondence $e_i \to e_j$ is a permutation $\bar{x}$ of the basis elements, and the set of all $\bar{x}$ forms a permutation group $\bar{P}$ homomorphic to P. By Lemma 3, the basis elements can be written as

$$e_{11}, \cdots, e_{1p}, e_{21}, \cdots, e_{2p}, \cdots, e_{mp}, e_1, e_2, \cdots, e_r,$$

in such a way that $\bar{P}$ contains the permutation

$$(e_{11} \cdots e_{1p})(e_{21} \cdots e_{2p}) \cdots (e_{m1} \cdots e_{mp}),$$

and every permutation of $\bar{P}$ is of the form

$$(e_{11} \cdots e_{1p})^{r_1}(e_{21} \cdots e_{2p})^{r_2} \cdots (e_{m1} \cdots e_{mp})^{r_m}.$$

This implies that V is the direct sum of subspaces

$$V_1 = \{e_{11}, \cdots, e_{mp}\}, \quad V_2 = \{e_1, \cdots, e_r\},$$

each invariant under P. For $i = 1, 2$, let P_i be the group of transformations of V_i obtained by restricting the transformations in P. Since $\bar{P}$ leaves $e_1, \cdots, e_r$ fixed, P_2 is Abelian.

https://doi.org/10.1017/S1446788700027920 Published online by Cambridge University Press

The restrictions to the basis elements of V_1 of the permutations in $\bar{P}$ form a permutation group $\bar{P}_1$ isomorphic with P_1/N, where N consists of those transformations in P_1 having $e_{11}, \cdots, e_{mp}$ as eigenvectors. Suppose if possible that N is non-trivial. P_1 contains an element x such that

$$e_{ij}^x = a_{ij} e_{i,j+1} \qquad (i = 1, \cdots, m;\ j = 1, \cdots, p),$$

where a_{ij} is a scalar, and $e_{i,p+1} = e_{i1}$. N is obviously Abelian. By Lemma 2, N is elementary Abelian, and thus may be regarded as a vector space over $GF(p)$. x acts as a linear transformation on N, whose minimal polynomial, by Lemma 2, divides $X^p - 1 = (X-1)^p$, and so splits in $GF(p)$. Thus x has an eigenvector in N, that is, x commutes with some non-trivial element y of N. We have

$$e_{ij}^y = b_{ij} e_{ij} \qquad (i = 1, \cdots, m;\ j = 1, \cdots, p).$$

The fact that x commutes with y implies that

$$b_{i1} = b_{i2} = \cdots = b_{ip} \qquad (i = 1, \cdots, m).$$

Thus each eigenvalue of y occurs with multiplicity at least p. But, as in the proof of Lemma 2, no primitive p-th root of 1 can occur more than $p-1$ times. Since the eigenvalues of y must be p-th roots of 1 (by Lemma 2), they must all be 1, and this contradicts the fact that y is non-trivial. Hence N must be trivial, and P_1 is isomorphic with $\bar{P}_1$, which is Abelian, by Lemma 3.

Since P_1 and P_2 are both Abelian, P is itself Abelian, and so elementary Abelian, by Lemma 2.

Theorems 1 and 2 show that any p-group which can be represented as a quasi-permutation group of degree n can also be represented as a permutation group of degree n, provided that $p^2 > n$. The condition is necessary, since, for example, the quaternion group of order 8 has a representation as a quasi-permutation group of degree 4, but none as a permutation group of degree 4. The investigation of Sylow p-groups of quasi-permutation groups, for arbitrary p, seems to be difficult.

References

[1] G. A. Miller, H. F. Blichfeldt and L. E. Dickson, *Theory and Applications of Finite Groups* (New York, 1938).

[2] B. L. van der Waerden, *Modern Algebra*, Vol. 1 (New York, 1949).

University of Otago,
New Zealand.