ON LINEAR p-GROUPS

W. J. WONG

(received 27 August 1963)

A *quasi-permutation group* of degree n was defined in [3] to be a finite group with a faithful representation of degree n whose character has only non-negative rational integral values. If G is such a group, then the following simple properties of permutation groups of degree n were proved to hold also for G:

(i) the order of G is a divisor of the order of the symmetric group S_n of degree n; and

(ii) if G is a p-group and $n < p^2$, then G has exponent at most p and derived length at most 1 (i.e. G is elementary Abelian).

We now generalise (ii) by showing that, if $n < p^{a+1}$, then G has exponent at most p^a and derived length at most a. As a corollary we have the result (i) with the word "order" replaced by the word "exponent". These results are deduced from more general results on the derived length and exponent of a finite p-group with a faithful representation of given degree.

NOTE. Except in the final corollary, we deal only with finite p-groups. All representations will be over a field of characteristic 0, which may be taken without loss of generality to be the complex field, and the term "irreducible" is to be taken as meaning "absolutely irreducible". Of course our results will be valid also for representations over fields of finite characteristic other than p.

Our original proof of the following result was somewhat complicated. The present simple argument is due to Dr. G. E. Wall.

THEOREM 1. *If a p-group G has a faithful representation $\mathscr{X}$ of degree less than p^a, then the derived length of G is at most a.*

PROOF. We proceed by induction on a. If the irreducible components of $\mathscr{X}$ are $\mathscr{X}_1, \cdots, \mathscr{X}_k$, then $\deg \mathscr{X}_i = p^{a_i}$, $a_i < a$. Since G is isomorphic with a subgroup of the direct product of the $\mathscr{X}_i(G)$, it will suffice to show that the $\mathscr{X}_i(G)$ have derived length at most a. In other words, we may assume that $\mathscr{X}$ is irreducible, of degree p^{a-1}. In particular, this proves the result when $a = 1$.

Since G is a p-group, $\mathscr{X}(G)$ may be written as a group of monomial

https://doi.org/10.1017/S1446788700023375 Published online by Cambridge University Press

transformations [2]. This implies that G has a normal Abelian subgroup N (consisting of the elements of G represented by diagonal transformations), such that G/N has a faithful representation as a permutation group of degree p^{a-1}, and thus has a faithful representation of degree $p^{a-1}-1$. By the induction hypothesis, the derived length of G/N is at most $a-1$, so that the derived length of G is at most a.

THEOREM 2. *Suppose that $\mathscr{X}$ is a faithful representation of a p-group G, of degree n, and that the values of the character ζ of $\mathscr{X}$ lie in the field K. If $n < p^a t$, where t is the degree over K of a primitive p-th root of* 1, *then G has derived length at most a. Moreover, if the derived length of G is exactly a, then ζ has an irreducible component χ of degree p^{a-1} whose values generate the field of p-th roots of* 1 *over K.*

PROOF. If $\mathscr{X}$ can be decomposed into representations $\mathscr{X}_1, \cdots, \mathscr{X}_k$, whose characters have values in K, then G is isomorphic to a subgroup of the direct product of the groups $\mathscr{X}_i(G)$, and it will suffice to prove that these have derived length at most a. In other words we may assume that $\mathscr{X}$ cannot be decomposed into representations whose characters have values in K.

Let χ be an irreducible component of ζ, and suppose that the distinct characters algebraically conjugate to χ over K are $\chi_1, \cdots, \chi_r$. We have

$$r = [K(\chi) : K], \tag{1}$$

where $K(\chi)$ is the field generated by the values of χ over K. By the orthogonality relations, each of the χ_i occurs in ζ, and so we may write

$$\zeta = \chi_1 + \cdots + \chi_r + \zeta_1.$$

As $\chi_1 + \cdots + \chi_r$ and ζ_1 both have values in K, we must have $\zeta_1 = 0$, for else $\mathscr{X}$ would be decomposable into parts whose characters have values in K. Taking degrees, we obtain

$$n = rf, \tag{2}$$

where $f = \deg \chi$. The representation $\mathscr{X}$ corresponding to χ is faithful, for if $\chi(x) = f$, then $\chi_i(x) = f$ for all i, so that $\zeta(x) = n$, and x lies in the kernel of $\mathscr{X}$.

Now if x is an element of order p in the centre of G, then, because $\mathscr{X}$ is irreducible, $\mathscr{X}(x)$ is of the form ωI, where ω is a primitive p-th root of 1 and I is the identity transformation. Thus $\chi(x) = f\omega$, and so

$$K(\chi) \supseteqq K(\omega). \tag{3}$$

By (1), this shows that $r \geqq [K(\omega) : K] = t$. Since $n < p^a t$ by assumption, (2) shows that $f < p^a$. By Theorem 1, the derived length of G is at most a.

https://doi.org/10.1017/S1446788700023375 Published online by Cambridge University Press

If the derived length is precisely a, then Theorem 1 shows that $f = p^{a-1}$. If $|G| = p^b$, then $K(\chi)$ is a subfield of $K(\pi)$, where π is a primitive p^b-th root of 1. Since $[K(\pi) : K(\omega)]$ is a power of p, it follows that if equality does not hold in (3), then $[K(\chi) : K(\omega)] \geqq p$, and so, by (1), $r \geqq pt$. But then (2) gives the contradiction $n \geqq p^a t$. Hence $K(\chi) = K(\omega)$, as required.

If p is an odd prime, or if $p = 2$ and the field K contains a square root of -1, we shall say that K is *of finite p-index* if there exists a number s such that K does not contain all the p^s-th roots of 1, and define the *p-index* $m = m_p(K)$ of such a field to be the largest integer such that the field of the p-th roots of 1 over K contains all the p^m-th roots of 1. If $p = 2$ and K does not contain $\sqrt{-1}$, K is defined to be of finite 2-index if and only if $K(\sqrt{-1})$ is of finite 2-index, and then we define $m_2(K) = m_2(K(\sqrt{-1}))-1$. With these definitions, if a is a non-negative integer then the degree over K of a primitive p^{a+m}-th root of 1 is $p^a t$, where t is the degree over K of a primitive p-th root of 1, except in the case when $p = 2$, $a = 0$ and K does not contain $\sqrt{-1}$. We remark that an algebraic number field is of finite p-index for every p.

THEOREM 3. *With the hypotheses of Theorem* 2, *if K is of finite p-index m, then the exponent of G is at most p^{a+m-1}*

PROOF. Since the exponent of G is the maximum of the exponents of the cyclic subgroups of G, we may assume that G is cyclic.

Suppose that $\mathfrak{X}$ is decomposed as much as possible into representations $\mathfrak{X}_i$ whose characters have values in K. Since $\mathfrak{X}$ is faithful, at least one of the $\mathfrak{X}_i$ must be faithful, for else the kernel of $\mathfrak{X}$ would contain the subgroup of G of order p. Thus it suffices to prove the result in the case when $\mathfrak{X}$ cannot be decomposed. As in the proof of Theorem 2, we find an irreducible character χ such that $\zeta = \chi_1 + \cdots + \chi_r$, the sum of the algebraic conjugates of χ over K. If x were an element of order p^{a+m} in G, then consideration of $\chi(x)$ shows that $K(\chi)$ contains the field of the p^{a+m}-th roots of 1 over K. This field has degree $p^a t$ over K. (The exceptional case $p = 2$, $a = 0$ cannot arise since the hypothesis implies that $p^a t > 1$.) Hence $r \geqq p^a t$. As the degree of ζ is less than $p^a t$, this is impossible, and so the exponent of G is at most p^{a+m-1}.

If G is a p-group with a faithful permutation representation of degree less than p^{a+1}, then the derived length of G is at most a, as can be seen by Kaloujnine's construction of the p-Sylow subgroups of the symmetric groups by means of wreath products [1]. (We remark that this fact may be used in place of induction in the proof of Theorem 1 to show that G/N has derived length at most $a-1$). Also, the exponent of G is at most p^a. We now show that the corresponding results are valid for quasi-permutation groups.

THEOREM 4. *If G is a quasi-permutation p-group of degree less than p^{a+1}, then the derived length of G is at most a.*

PROOF. Let $\mathscr{X}$ be a faithful representation of G of degree n less than p^{a+1}, whose character ζ has only non-negative rational integral values. We apply Theorem 2, with K the field of rational numbers. Then, $t = p-1$. Since $n < p^{a+1}(p-1)$, G has derived length at most $a+1$.

Suppose that G has derived length exactly $a+1$. Then, by Theorem 2, ζ has an irreducible component χ of degree p^a whose values generate the field of p-th roots of 1 over K. If the $p-1$ conjugates of χ over K are $\chi_1, \cdots, \chi_{p-1}$, then we have

$$\zeta = \chi_1 + \cdots + \chi_{p-1} + \zeta_1,$$

where $\deg \zeta_1 = n - p^a(p-1) < p^a$. G has an element x for which $\chi(x) = p^a\omega$, where ω is a primitive p-th root of 1. Then we have

$$\zeta(x) = -p^a + \zeta_1(x),$$

so that $\zeta_1(x) \geqq p^a$. But this is impossible, since $\deg \zeta_1 < p^a$. Hence the derived length of G is at most a.

THEOREM 5. *If G is a quasi-permutation p-group of degree less than p^{a+1}, then the exponent of G is at most p^a.*

PROOF. By Theorem 3, since $m = 1$ for the rational field K, the exponent of G is at most p^{a+1}. Suppose that G has a cyclic subgroup H of order p^{a+1}. The restriction ζ' to H of the character ζ of the quasi-permutation representation $\mathscr{X}$ of G splits into components of degree 1. At least one of these, say χ, is faithful, since the restriction of $\mathscr{X}$ to H is faithful. Then, χ has $p^a(p-1)$ conjugates $\chi_1, \cdots, \chi_{p^a(p-1)}$, over K, and we have

$$\zeta' = \chi_1 + \cdots + \chi_{p^a(p-1)} + \zeta_1,$$

where $\deg \zeta_1 = n - p^a(p-1) < p^a$. If x is an element of order p in H, then $\chi(x) = \omega$, a primitive p-th root of 1, and so $\zeta(x) = \zeta'(x) = -p^a + \zeta_1(x)$, giving a contradiction. Thus the exponent of G is at most p^a.

COROLLARY. *If G is a quasi-permutation group of degree n, then the exponent of G is a divisor of the exponent of the symmetric group S_n of degree n.*

PROOF. Theorem 5 shows that the exponent of a Sylow subgroup of G is a divisor of the exponent of the corresponding Sylow subgroup of S_n. Since the exponent of a finite group is the product of the exponents of its Sylow subgroups, the result follows.

https://doi.org/10.1017/S1446788700023375 Published online by Cambridge University Press

References

[1] L. Kaloujnine, La structure des p-groupes de Sylow des groupes symétriques finis, *Ann. sci. École norm. sup.* (3) 65, 239—276 (1948).

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

[3] W. J. Wong, Linear groups analogous to permutation groups, *Jour. Australian Math. Soc.* 3, 180—184 (1963).

University of Otago

https://doi.org/10.1017/S1446788700023375 Published online by Cambridge University Press