PERMUTATION CHARACTERS

FIONA M. ROSS

(Received 11 March 1969; revised 17 December 1970)

Communicated by G. E. Wall

We suppose throughout that G is a finite group with a faithful matrix representation X over the complex field. We suppose that X affords a character π of degree r whose values are rational (hence rational integers). If the matrices in some representation of G affording a character π_0 are all permutation matrices, then π_0 is called a permutation character. Permutation characters have non-negative integral values. In the general case, we consider what properties of permutation characters are true of π, and in particular, under what circumstances π is a permutation character. Note that assuming X to be faithful is equivalent to considering the image group $X(G)$ instead of G.

In Section 1 we obtain some numerical results on π. In Section 2, we show that if π has non-negative values, then the sum of the prime powers dividing the order of an element of G is no greater than $r+1$ (Theorem 2.2). In Section 3, we assume that π has non-negative values and $r = p$ is a prime dividing g, the order of G. If $g \leqq p(p-1)$, then π is a transitive permutation character and G is solvable (results 3.6, 3.7 and 3.8). If $g > p(p-1)$, then G is insolvable and has some properties of doubly transitive permutation groups of degree p. In particular, the commutator subgroup G' is simple and non-cyclic, and is the unique minimal normal subgroup of G (Theorem 3.11). Also G/G' is cyclic of order dividing but less than $p-1$ (Lemma 3.10). In Section 4, with the additional assumption that $\frac{1}{2}(p-1)$ is prime, we have $[G : G'] = 1$ or 2 when $g > p(p-1)$ (Theorem 4.2).

This work was included in a thesis submitted to the University of New South Wales in partial fulfilment of the requirements for an M.Sc. degree in 1967. The work was carried out under the supervision of Dr. John D. Dixon, whose assistance I gratefully acknowledge. In particular, I am indebted to him for simplifications in the proofs of Theorems 1.1 and 2.2.

1

We recall the assumption that the character π afforded by the representation X of G takes only rational values.

1.1. THEOREM. *If $x \in G$ has order n, then for each positive divisor m of n, the*

https://doi.org/10.1017/S1446788700010624 Published online by Cambridge University Press

$\phi(m)$ primitive mth *roots of unity appear with equal multiplicities as eigenvalues of* $X(x)$.

PROOF. Let $f(t)$ be the characteristic polynomial of $X(x)$. Now $X(x)$ is similar to a diagonal matrix whose diagonal entries are its eigenvalues. Thus if $\varepsilon_1, \cdots, \varepsilon_r$ are the eigenvalues of $X(x)$, we can write $\pi(x^i) = \varepsilon_1^i + \cdots + \varepsilon_r^i$ $(i = 1, \cdots, n)$. Since $\pi(x^i)$ $(i = 1, \cdots, n)$ is rational, the elementary symmetric functions of the eigenvalues of $X(x)$ are rational. Thus $f(t)$ has rational coefficients. If ω is a primitive mth root of unity, then the mth cyclotomic polynomial is the polynomial irreducible over the rationals with ω as a root [7, pp. 161–162]. Now the roots of $f(t)$ are nth roots of unity. Thus $f(t)$ is a product of (not necessarily distinct) cyclotomic polynomials. The roots of each cyclotomic polynomial are precisely all the primitive mth roots of unity for some $m|n$ [7, pp. 161–162]. The assertion is now clear.

1.2. LEMMA. *If $x \in G$ and q is prime, then*

$$\pi(x^{q^{\beta-1}}) \equiv \pi(x^{q^\beta}) \pmod{q^\beta}. \tag{1.2.1}$$

for each positive integer β. If the order of x is a power of q, then

$$\pi(x^{q^{\beta-1}}) \equiv r \pmod{q^\beta}. \tag{1.2.2}$$

PROOF. Suppose $x \in G$ has order n. Then by Theorem 1.1, we can write

$$\pi(x^u) = \sum_{m|n} b_m S_m^u \qquad (u = 1, \cdots, n) \tag{1.2.3}$$

where S_m^u is the sum of the uth powers of the primitive mth roots of unity, and the b_m are non-negative integers. To prove (1.2.1) it is sufficient to show that $S_m^{q^{\beta-1}} \equiv S_m^{q^\beta} \pmod{q^\beta}$ for each m.

Let μ be the Möbius function [7, p. 114]. Then $\mu(a)$ is the sum of the primitive ath roots of unity. Now if $d = (m, u)$,

$$S_m^u = \frac{\phi(m)}{\phi(m/d)}\mu(m/d),$$

since the uth powers of primitive mth roots of unity are m/dth roots of unity, and there are $\phi(m)$ primitive mth roots of unity and $\phi(m/d)$ primitive m/dth roots of unity. Hence if $q^\beta \nmid m$, $(m, q^{\beta-1}) = (m, q^\beta)$ and so $S_m^{q^{\beta-1}} = S_m^{q^\beta}$. If $q^\beta | m$, write $m = q^\alpha t$ where $q \nmid t$ and $\alpha \geqq \beta$. Then we must show

$$\frac{\phi(q^\alpha t)}{\phi(q^{\alpha-\beta+1}t)}\mu(q^{\alpha-\beta+1}t) \equiv \frac{\phi(q^\alpha t)}{\phi(q^{\alpha-\beta}t)}\mu(q^{\alpha-\beta}t) \pmod{q^\beta}.$$

Since $\phi(ab) = \phi(a)\phi(b)$ and $\mu(ab) = \mu(a)\mu(b)$ if $(a, b) = 1$, it is sufficient to show that

$$\frac{\phi(q^\alpha)}{\phi(q^{\alpha-\beta+1})}\mu(q^{\alpha-\beta+1}) \equiv \frac{\phi(q^\alpha)}{\phi(q^{\alpha-\beta})}\mu(q^{\alpha-\beta}) \pmod{q^\beta}.$$

This follows because

$$\frac{\phi(q^\alpha)}{\phi(q^\gamma)} = \begin{cases} q^{\alpha-\gamma} & \text{if } 1 \leqq \gamma \leqq \alpha \\ q^{\alpha-1}(q-1) & \text{if } \gamma = 0 \end{cases}$$

and

$$\mu(q^\gamma) = \begin{cases} 0 & \text{if } \gamma > 1 \\ -1 & \text{if } \gamma = 1 \\ 1 & \text{if } \gamma = 0 \end{cases}$$

Thus we have (1.2.1). If n is a power of q the result (1.2.2) follows by induction. (For properties of μ and ϕ see van der Waerden [7, Section 36].)

1.3. *For $x \in G$ of order n, there exist unique integers $u_1, \cdots, u_n$ such that*

$$\pi(x^m) = \sum_{i|m} iu_i \quad (m = 1, \cdots, n). \tag{1.3.1}$$

PROOF. The set of equations (1.3.1) has a unique solution found by solving successively for $u_1, \cdots, u_n$. We show by induction on m that u_m, $1 \leqq m \leqq n$, is an integer. By assumption, $u_1 = \pi(x)$ is an integer. Assume $m > 1$ and u_i is an integer for $1 < i \leqq m$. Put $m = p^\alpha t$ where p is a prime not dividing t, and $\alpha \geqq 1$. Then

$$mu_m = \pi(x^m) - \pi(x^{m/p}) - \sum_s su_s$$

where s runs through the proper divisors of m which are divisible by p^α. Since each u_s is an integer by assumption, we have $mu_m \equiv 0 \pmod{p^\alpha}$ using Lemma 1.2. As this is true for each prime power p^α dividing m, $mu_m \equiv 0 \pmod{m}$ so u_m is an integer. Thus by induction we have that u_m, $1 \leqq m \leqq n$, is an integer.

NOTE. If $X(x)$ is a permutation matrix, u_m is the number of cycles of length m in $X(x)$, so each u_m is a non-negative integer.

We remark that the results of Section 1 are true even if π is not faithful.

2

Throughout this section we assume the following.

(A) G is a finite group with a faithful character π of degree r.

(B) The values of π are non-negative integers.

Let m be a positive integer with distinct prime divisors $p_1, \cdots, p_s$ and suppose $m = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$. For the next theorem we require an estimate of

$$E(p_1, m) = p_1^{\alpha_1}\phi(m/p_1^{\alpha_1}) - \sum_{i=1}^{s} p_i^{\alpha_i}.$$

2.1. LEMMA. $E(p_1, m) \geqq 0$ *except in the cases*

(2.1.1) $\quad E(2,6) = -1, \quad E(3,12) = -1, \quad E(p_1, 2p_1^{\alpha_1}) = -2 \quad (p_1 \text{ odd}).$

Moreover, $E(p_1, m) \geqq 2$ *whenever* m *is odd and not a prime power.*

PROOF. We consider several cases.

(i) If $s = 1$, $E(p_1, p_1^{\alpha_1}) = 0$.

(ii) If $s = 2$, $E(p_1, m) = m(1 - 1/p_2 - 1/p_1^{\alpha_1} - 1/p_2^{\alpha_2})$ so $E(p_1, m) \geqq 0$ except in the cases (2.1.1). However if m is odd, $p_1, p_2 > 2$ and so $E(p_1, m) \geqq 2$.

(iii) If $s \geqq 3$, write $n = m/p_s^{\alpha_s}$. We may suppose $p_2 < p_3 < \cdots < p_s$, so we have $p_s \geqq 3$ in all cases, and $p_s \geqq 5$ if $n = 6$. Now $E(p_1, m) - E(p_1, n) = p_1^{\alpha_1}\phi(n/p_1^{\alpha_1})\{\phi(p_s^{\alpha_s}) - 1\} - p_s^{\alpha_s}$. Thus if $n = 6$, $E(p_1, m) - E(p_1, n) \geqq 3\{\phi(p_s^{\alpha_s}) - 1\} - p_s^{\alpha_s} \geqq 4$, since $p_s \geqq 5$. If $n > 6$, $E(p_1, m) - E(p_1, n) \geqq 5\{\phi(p_s^{\alpha_s}) - 1\} - p_s^{\alpha_s} \geqq 2$, since $p_s \geqq 3$. Thus in either case $E(p_1, m) \geqq E(p_1, n) + 2$.

Collecting these results, we obtain the assertions.

2.2. THEOREM. *Suppose hypotheses (A) and (B) hold. If* $x \in G$ *has order* $n = p_1^{\alpha_1} \cdots p_t^{\alpha_t}$ *where the* p_i *are the distinct prime divisors of* n, *then* $\sum_{i=1}^{t} p_i^{\alpha_i} \leqq r$, *except in the case* $n = 6n'$ *with* $(6, n') = 1$. *In the latter case* $\sum_{i=1}^{t} p_i^{\alpha_i} \leqq r+1$.

NOTE. In the case $n = 6n'$ with $(6, n') = 1$, we shall say n is exceptional.

REMARK 1. This result improves a result of W. J. Wong [9] which shows that under assumptions (A) and (B), the exponent of G divides the exponent of S_r, the symmetric group of degree r i.e. in the above notation, $p_i^{\alpha_i} \leqq r$ $(i = 1, \cdots, t)$.

REMARK 2. For permutation groups of degree r, $\sum_{i=1}^{t} p_i^{\alpha_i} \leqq r$ in all cases. However it will be shown that Theorem 2.2 is the best possible under our weaker assumptions.

PROOF. Using the notation of Section 1, we write $\pi(x) = S_{n_1}^1 + \cdots + S_{n_d}^1$ where $S_{n_i}^1$ is the sum of the $\phi(n_i)$ primitive n_ith roots of unity for some positive divisor n_i of n. Since x has order n, and π is faithful, $n = \text{l.c.m.}\ \{n_1, \cdots, n_d\}$. We can choose a minimal subset A of $\{n_1, \cdots, n_d\}$ such that $n = \text{l.c.m.}\ A$. Reordering if necessary, we may suppose $A = \{n_1, \cdots, n_c\}$ where $1 \leqq c \leqq d$. Clearly each $n_j \in A$ is divisible by at least one prime power $p_i^{\alpha_i}$ which does not divide any other element of A. For each $n_j \in A$ we choose a prime q_j such that $q_j^{\beta_j}$ is equal to some $p_i^{\alpha_i}$ $(i = 1, \cdots, t)$ and $q_j^{\beta_j} | n_j$ but $q_j^{\beta_j} \nmid n_k$ if $n_k \in A$ and $k \neq j$. (For instance we could choose q_j to be the smallest such prime). We can then write $n_j = q_j^{\beta_j} m_j$ $(j = 1, \cdots, c)$. Again in the notation of Lemma 1.2, we have

$$\pi(x^u) = \sum_{j=1}^{d} S_{n_j}^u \quad (u = 1, \cdots, n) \tag{2.2.1}$$

and in particular

$$r = \pi(x^n) = \sum_{j=1}^{d} \phi(n_j). \tag{2.2.2}$$

https://doi.org/10.1017/S1446788700010624 Published online by Cambridge University Press

If $u = n/\prod_{j=1}^{c} q_j$, then $S^u_{n_j} = -\phi(n_j)/(q_j-1)$ $(j = 1, \cdots, c)$ and $S^u_{n_j} \leqq \phi(n_j)$ $(j = c+1, \cdots, d)$. Since $\pi(x^u) \geqq 0$, it follows from (2.2.1) and (2.2.2) that

$$r \geqq r-\pi(x^u) \geqq \sum_{j=1}^{c} \frac{q_j\phi(n_j)}{q_j-1} = \sum_{j=1}^{c} q_j^{\beta_j}\phi(m_j).$$

Thus $r-\sum_{i=1}^{t} p_i^{\alpha_i} \geqq h$ where we define

$$h = h(q_1, \cdots, q_c) = \sum_{j=1}^{c} q_j^{\beta_j}\phi(m_j) - \sum_{i=1}^{t} p_i^{\alpha_i}. \tag{2.2.3}$$

Since $p_1^{\alpha_1} \cdots p_t^{\alpha_t} = \text{l.c.m.}\ \{n_1, \cdots, n_c\}$, we have

$$h \geqq \sum_{j=1}^{c} E(q_j, n_j). \tag{2.2.4}$$

We show that we can choose the q_j $(1 \leqq j \leqq c)$ so that $h \geqq 0$, except in certain cases which are treated differently.

By Lemma 2.1 and (2.2.4), $h \geqq 0$ except when for some values of j, one of the following occurs:

(i) $q_j = 2, n_j = 6$,

(ii) $q_j = 3, n_j = 12$,

(iii) $n_j = 2q_j^{\beta_j}$ (q_j odd).

Suppose (i) occurs for some value, say j_1 of j. Then by definition of q_j, there is no other value of j for which (i) occurs, and neither (ii) nor (iii) can occur for any value of j. If 3 divides some $n_j \in A, j \neq j_1$, then $h \geqq \sum_{j \neq j_1} E(q_j, n_j)+2\phi(3)-2 > 0$. If 3 divides no other $n_j \in A$, then we can choose $q_{j_1} = 3$ instead, and we get case (iii) which is treated later.

If (iii) occurs, suppose the ordering is such that

$$n_j = 2q_j^{\beta_j},\ 1 \leqq j \leqq s, (q_j \text{ odd})$$
$$n_j \neq 2q_j^{\beta_j},\ s < j \leqq c.$$

Then by (2.2.4),

$$h \geqq \sum_{j=s+1}^{c} E(q_j, n_j)-2 \tag{2.2.5}$$

If $4|n$, then by (2.2.3),

$$h \geqq \sum_{j=s+1}^{c} E(q_j, n_j). \tag{2.2.6}$$

Suppose (ii) also occurs, say $n_{s+1} = 12$ and $q_{s+1} = 3$. Then if 4 divides no other $n_j \in A$, we may choose $q_{s+1}^{\beta_{s+1}} = 4$ instead of 3, and get $h \geqq 0$ by (2.2.6). If 4 divides n_j for some $j \neq s+1, n_j \in A$, then by (2.2.3),

$$\begin{aligned} h &\geqq \sum_{s+2}^{c} E(q_j, n_j)+3\phi(4)-3 \\ &> 0. \end{aligned}$$

If (ii) occurs but not (iii), then the same argument applies (with $s = 0$) to give $h > 0$. Hence we may suppose that (iii) occurs, i.e. $s > 0$, but (ii) does not occur. Thus by (2.2.6), if $4|n$, $h \geqq 0$, since none of (i), (ii), (iii) occurs for $j > s$. So suppose $2||n$. If $E(q_j, n_j) \geqq 2$ for some j, $s+1 \leqq j \leqq c$, then by (2.2.5), $h \geqq 0$. Hence assume $E(q_j, n_j) < 2$, $s+1 \leqq j \leqq c$. Then by Lemma 2.1, each n_j, $s+1 \leqq j \leqq c$, is either even or a prime power. But if some n_j, $s+1 \leqq j \leqq c$, is even then by (2.2.3),

$$h \geqq \sum_{s+1}^{c} E(q_j, n_j) \geqq 0.$$

So suppose finally that each n_j, $s+1 \leqq j \leqq c$, is an odd prime power. We have

$$n_1 = 2q_1^{\beta_1}, \cdots, n_s = 2q_s^{\beta_s}, n_{s+1} = q_{s+1}^{\beta_{s+1}}, \cdots, n_c = q_c^{\beta_c}$$

where $1 \leqq s \leqq c$ and q_j is odd $1 \leqq j \leqq c$. Since here $h = -2$, we use another argument. Put $v = n/(2q_{s+1} \cdots q_c)$. Then

$$\begin{aligned} r &\geqq r - \pi(x^v) \\ &\geqq \sum_1^c \phi(q_j^{\beta_j}) + \sum_1^s \phi(q_j^{\beta_j}) + \sum_{s+1}^c q_j^{\beta_j - 1} \\ &= 2\sum_1^s \phi(q_j^{\beta_j}) + \sum_{s+1}^c q_j^{\beta_j}. \end{aligned}$$

So

$$\begin{aligned} r - \sum_{i=1}^t p_i^{\alpha_i} &\geqq 2\sum_{j=1}^s \phi(q_j^{\beta_j}) - \sum_{j=1}^s q_j^{\beta_j} - 2 \\ &\geqq 0 \end{aligned}$$

unless $s = 1$, $q_1^{\beta_1} = 3$, i.e. n is exceptional, and then $r - \sum_{i=1}^t p_i^{\alpha_i} \geqq -1$. Thus the theorem is proved.

We now show that the case $\sum_{i=1}^t p_i^{\alpha_i} = r+1$ actually occurs. Let X be the faithful representation of degree 11 of a cyclic group $\langle x \rangle$ of order 42 such that $X(x)$ is a diagonal matrix whose diagonal entries are: 1, 1, 1, the two primitive 6th roots of unity and the six primitive 7th roots of unity. The values of π, the character afforded by X, are non-negative integers, but the sum of the prime powers dividing the order of x is one larger than the degree of π.

Let 1_G denote the identity character of G, and let

$$\langle \psi, \eta \rangle = 1/g \sum_{x \in G} \psi(x)\eta(x^{-1})$$

(where $g = |G|$) denote the inner product of characters ψ, η of G.

2.3. LEMMA. $\langle \pi, 1_G \rangle \geqq 1$. *Thus if* $G \neq 1$, *then* π *is reducible and* $\pi = 1_G + \chi$ *where* χ *is a faithful character of* G.

PROOF. We have $\langle \pi, 1_G \rangle = 1/g \sum_{x \in G} \pi(x) \geqq 1/g\, \pi(1) > 0$. Then since $\langle \pi, 1_G \rangle$

is an integer, $\langle \pi, 1_G \rangle \geqq 1$. If $G \neq 1$, $\pi \neq 1_G$ since π is faithful and so $\chi = \pi - 1_G$ is a character of G. If x is in the kernel of χ, $\chi(x) = r-1$ and so $\pi(x) = r$, hence $x = 1$. Thus χ is faithful.

2.4. *If $G \neq 1$ and χ is irreducible, then $g \geqq r(r-1)$ and $r-1$ divides g.*

PROOF. Since χ is irreducible and $\chi \neq 1_G$, $\langle \chi, \pi \rangle = \langle \chi, \chi \rangle + \langle \chi, 1_G \rangle = 1$ and so $\sum_{x \in G} \chi(x)\pi(x) = g$. Since $\chi(x)\pi(x) \geqq 0$ for $x \in G, \chi(1)\pi(1) = r(r-1) \leqq g$. Since χ is irreducible of degree $r-1$, $r-1$ divides g [6, p. 332, Theorem 12.2.27].

3

Throughout this section we make the following assumptions.

(A) G is a finite group with a faithful representation X affording a character π.

(B) The values of π are non-negative integers.

(C) The degree $\pi(1)$ of π is a prime p which divides the order g of G.

NOTE 1. If H is a subgroup of G, and $p \mid |H|$, then $\pi|_H$ is a character of H satisfying (A), (B), (C) with H in place of G.

NOTE 2. If G is a transitive permutation group of degree p, then the corresponding permutation character satisfies (A), (B), (C).

3.1. LEMMA. *We have $\langle \pi, 1_G \rangle = 1$ and so $\chi = \pi - 1_G$ is a faithful character of G which does not contain 1_G.*

PROOF. By assumption G contains an element x of order p. As in Section 1, expressing $\pi(x)$ as a sum of the eigenvalues of $X(x)$, we have $\pi(x) = 1 + \varepsilon + \cdots + \varepsilon^{p-1}$ where ε is a primitive pth root of unity. Thus $\pi|_{\langle x \rangle}$ contains the identity character exactly once. Hence $\langle \pi, 1_G \rangle \leqq 1$. Lemma 2.3 now gives the required result.

Let P be a Sylow p-group of G, $N(P) = N_G(P)$ its normalizer in G and $C(P) = C_G(P)$ its centralizer in G.

3.2. LEMMA.

(i) $|P| = p$.

(ii) $C(P) = P$.

(iii) *p divides the number of conjugates of each element not in a Sylow p-group of G.*

(iv) *$N(P)/P$ is cyclic of order dividing $p-1$.*

PROOF. By a result of W. J. Wong [8, Theorem 1], g divides $p!$. This gives (i).

https://doi.org/10.1017/S1446788700010624 Published online by Cambridge University Press

By Theorem 2.2, G contains no element of order pm, $m > 1$. Hence no non-identity element of order prime to p can commute with an element of a Sylow p-group P. Thus since P is cyclic, $C(P) = P$ and we have (ii). If x has order different from 1 and p, then p does not divide the order of its centralizer so p divides the number of conjugates of x. This proves (iii). Finally $N(P)/C(P) = N(P)/P$ is isomorphic to a subgroup of the group of automorphisms of P [6, p. 50] which is cyclic of order $p-1$ [4, p. 86]. Thus $N(P)/P$ is cyclic of order dividing $p-1$ and (iv) is proved.

3.3. Lemma. *There is a unique (normal) Sylow p-group of G if and only if $g \leqq p(p-1)$.*

Proof. Let n_p be the number of Sylow p-groups of G. If $g \leqq p(p-1)$ then $n_p = 1$, since by Sylow's theorems $n_p \equiv 1 \pmod p$ and $n_p | g$. If $g > p(p-1)$, then by Lemma 3.2, $N(P) \neq G$, so $n_p > 1$.

3.4. Theorem. *Suppose assumptions* (A), (B), (C) *of this section are satisfied. Then pn_p divides the order of each normal subgroup $H \neq 1$ of G. If $n_p > 1$, then $|H| > pn_p$.*

Remark 1. This result is known for the case when G is a transitive permutation group of prime degree p. In this case G is primitive [6, p. 269, Theorem 10.5.3] and so each normal subgroup $\neq 1$ is transitive [2, p. 196] and thus its order is divisible by p.

Remark 2. Theorem 3.4 shows that if $1 \neq H \trianglelefteq G$, assumptions (A), (B), (C) are satisfied with H in place of G and $\pi|_H$ in place of π.

Proof. Suppose $1 \neq H \trianglelefteq G$ and $p \nmid |H|$. Then there is an element x of order p in $G \setminus H$. Since $C(x) = \langle x \rangle$ by Lemma 3.2, $C(x) \cap H = 1$. By a result of Feit and Thompson [3, p. 783, Lemma 4.3] since χ is faithful, $\chi(x) = 0$. However by Theorem 1.1, $\chi(x) = -1$ and so we have a contradiction. Thus p divides $|H|$. Since $H \trianglelefteq G$, every Sylow p-group of G is in H and so pn_p divides $|H|$. Suppose $|H| = pn_p$. Then the normalizer of a Sylow p-group P in H has order p and so equals its centralizer. By a theorem of Burnside [6, p. 137, Theorem 6.2.9], H then has a normal subgroup K of order n_p. Applying the above result to H, since $p| \, |H|$, we have $p| \, |K|$ if $K \neq 1$. However $p \nmid n_p$, so $|K| = n_p = 1$. The theorem is now proved.

3.5. Lemma. *If $N(P) = P$ then $g = p$.*

Proof. If $N(P) = P$ then $N(P) = C(P)$ by Lemma 3.2. But then G has a normal subgroup of order g/p [6, p. 137, Theorem 6.2.9]. Now $p \nmid g/p$ (see proof of Lemma 3.2), so by Theorem 3.4, $g/p = 1$.

3.6. Theorem. *We assume* (A), (B), (C) *of this section, and also that $\chi = \pi - 1_G$ is reducible. Then the following are true.*

https://doi.org/10.1017/S1446788700010624 Published online by Cambridge University Press

(i) *The order g of $|G|$ divides but is less than $p(p-1)$.*

(ii) *G is solvable. In fact $G' = P$, the unique Sylow p-group (unless $g = p$ when $G' = 1$), and $G'' = 1$.*

(iii) *G is isomorphic to a transitive permutation group of degree p and π is the corresponding permutation character.*

REMARK. This generalizes a theorem of W. Burnside which states that if a permutation group of degree p is not doubly transitive, then it is solvable of order dividing $p(p-1)$ [6, p. 367, Theorem 12.9.2].

PROOF. By Lemma 3.1., we can write

$$\pi = 1_G + \chi_1 + \cdots + \chi_t$$

where χ_i $(i = 1, \cdots, t)$ are irreducible characters of G different from 1_G. Since χ is assumed reducible, $t \geqq 2$. Let $x \in G$ have order p. As in Section 1, $\pi(x) = 1+\varepsilon+\cdots+\varepsilon^{p-1}$, where ε is a primitive pth root of unity. Let Q be the rational field. For each integer k, $1 \leqq k \leqq p-1$, there is an automorphism of $Q(\varepsilon)$ which sends $\varepsilon \to \varepsilon^k$ and hence the group of all automorphisms permutes the χ_i transitively. Hence each χ_i $(i = 1, \cdots, t)$ has the same degree, namely $(p-1)/t$. We next show that if $y \in G$ has order prime to p, then $\chi_i(y)$ is rational for each i. Otherwise let h be the smallest integer such that $\chi_i(y) \in Q(\omega)$ where ω is a primitive hth root of unity. The smallest cyclotomic extension field of Q containing $\chi_i(x)$ is $Q(\varepsilon)$. Now if q is a prime dividing h, then by a result of Brauer [1, Theorem 2, Corollary 2], G contains elements of order qp. This contradicts Theorem 2.2. Thus $\chi_i(y) \in Q$ if y has order prime to p. Now since the automorphisms of $Q(\varepsilon)$ which send $\varepsilon \to \varepsilon^k$, $1 \leqq k \leqq p-1$, permute the χ_i but fix Q, we have $\chi_i(y) = \chi_j(y)$ for all $1 \leqq i, j \leqq t$. The same argument as in Scott [6, p. 369 equation 3 to end of p. 370] now shows that $\pi(y) = 1$ if $y \neq 1$.

Thus we have

$$\begin{aligned} &\pi(1) = p \\ (3.6.1) \qquad &\pi(x) = 0 \text{ if } x \text{ has order } p \\ &\pi(x) = 1 \text{ if } x \neq 1 \text{ has order prime to } p. \end{aligned}$$

Since by Lemma 3.1, $\sum_{x \in G} \pi(x) = g$, there must be $g-p$ elements such that $\pi(x) = 1$ and p elements such that $\pi(x) \neq 1$. Thus G has a unique Sylow p-group P. By Lemma 3.2., $N(P)/P = G/P$ is cyclic of order dividing $p-1$, so g divides $p(p-1)$. Also $g < p(p-1)$, since otherwise $\langle \chi, \chi \rangle = 1$ and then χ would be irreducible, contrary to assumption. Thus we have result (i).

Since G/P is abelian $G' \leqq P$, so $G' = 1$ or P. If $G' = 1$, G is abelian and $g = p$. Otherwise $G' = P$ and $G'' = 1$. In either case G is solvable and we have result (ii). Result (iii) is clear when $g = p$, so suppose $g > p$.

Put $g = pn$ where $(n, p) = 1$. Since G is solvable, there is a subgroup H of order n, and every element of order prime to p is in a conjugate of H [4, p. 141, Theorem 9.3.1]. There are $(n-1)p$ of these elements, apart from 1, so H has at least p conjugates. However $N(H) \supseteq H$ so H has at most p conjugates. Hence H has exactly p conjugates, and any pair intersect in the identity. Thus G can be faithfully represented as a transitive permutation group of degree p on the cosets of H [4, pp. 57–58, Theorems 5.3.1 and 5.3.2]. Let θ be the character afforded by this representation. Then $\theta(x)$ is the number of conjugates of H containing x, and so (3.6.1) shows that $\theta = \pi$. Hence (iii) is proved. This completes the proof of the theorem.

3.7. Lemma. *If χ is irreducible, then $g = p(p-1)k$ where k divides $(p-2)!$. If $k > 1$, G is insolvable.*

Proof. If χ is irreducible, its degree $p-1$ divides g. Since $g|p!$ (see proof of Lemma 3.2), $g = p(p-1)k$ where $k|(p-2)!$. Suppose G is solvable. Then the derived series has the form

$$G = G^{(0)} \supset G^{(1)} \supset \cdots \supset G^{(n-1)} \supset G^{(n)} = 1$$

for some n. Each group is characteristic in the preceding one, so $G^{(n-1)}$ is characteristic in G. By Theorem 3.4, $p| \, |G^{(n-1)}|$. Now $G^{(n-1)}$ is abelian, and so by Lemma 3.2, $|G^{(n-1)}| = p$. Thus G has a unique Sylow p-group and by Lemma 3.3, $g \leqq p(p-1)$. Hence $k = 1$. Thus G is insolvable if $k > 1$.

3.8. Theorem. *We assume* (A), (B), (C) *of this section, and that $g = p(p-1)$. Then the following are true.*

(i) *G is solvable. In fact $G' = P$, the unique Sylow p-group (except if $p = 2$ when $G' = 1$), and $G'' = 1$.*

(ii) *G is isomorphic to a transitive permutation group of degree p, and π is the corresponding permutation character.*

Proof. If $p = 2$ the results are obvious. Henceforth assume $p > 2$. By Lemma 3.3, G has a unique Sylow p-group P. Thus $N(P) = G$ and by Lemma 3.2, G/P is cyclic and $G' \subseteq P$. Now G is not abelian, since $C(P) = P \neq G$, so $G' = P$ and $G'' = 1$. Thus we have result (i). Since G is solvable and $(p, p-1) = 1$, G has a subgroup H of order $p-1$, and every element of order prime to p is in a conjugate of H [4, p. 141, Theorem 9.3.1]. Now H has p conjugates, and any pair intersect in the identity. Thus G can be represented faithfully as a transitive permutation group of degree p on the cosets of H [4, pp. 57–58, Theorems 5.3.1 and 5.3.2]. The corresponding permutation character θ is given by

$$\begin{aligned} &\theta(1) = p \\ (3.8.1) \qquad &\theta(x) = 0 \text{ if } x \in P \setminus 1 \\ &\theta(x) = 1 \text{ if } x \notin P. \end{aligned}$$

https://doi.org/10.1017/S1446788700010624 Published online by Cambridge University Press

On the other hand, χ is irreducible by Theorem 3.6, so $\sum_{x\in G}\chi(x)^2 = g$. Thus $\sum_{x\notin P}\chi(x)^2 = 0$, since $\chi(1) = p-1$ and $\chi(x) = -1$ if $x \in P\setminus 1$ (see proof of Lemma 3.1). Hence $\chi(x) = 0$ for $x \notin P$. From (3.8.1) we see that $\theta = \chi + 1_G = \pi$ and so π is a permutation character. We now have (ii) and the theorem is proved.

3.9. Lemma. (i) *χ is reducible if and only if $g < p(p-1)$.*

(ii) *G is solvable if and only if $g \leqq p(p-1)$.*

Proof. These assertions follow from results 3.6, 3.7 and 3.8.

3.10. Lemma. *If $H \neq 1$ is a normal subgroup of G, then G/H is cyclic of order dividing $p-1$. Moreover $[G:H] < p-1$ unless $g = p(p-1)$.*

Proof. By Theorem 3.4, H contains all Sylow p-groups of G. Thus $G = H\cdot N(P)$ where P is a Sylow p-group of G [6, p. 136, Theorem 6.24]. Since $H \trianglelefteq G$ and $P \trianglelefteq N(P)$, we have

$$\frac{G}{H} = \frac{H\cdot N(P)}{H} \cong \frac{N(P)}{H\cap N(P)} \cong \frac{N(P)/P}{(H\cap N(P))/P}$$

By Lemma 3.2, the last group is cyclic of order dividing $p-1$. Therefore G/H is cyclic of order dividing $p-1$. Moreover if $H\cap N(P) \neq P$, then G/H has order less than $p-1$. However by Lemma 3.5, $H\cap N(P) = P$ implies $H = P$. Thus $[G:H] < p-1$ except when $g = p(p-1)$.

3.11. Theorem. *Under assumptions* (A), (B), (C) *we have the following results.*

(i) *G has a unique minimal normal subgroup K.*

(ii) *$K = G'$ except when $g = p$.*

(iii) *G' is simple.*

(iv) *G' is non-cyclic if and only if $g > p(p-1)$.*

(v) *Every subnormal subgroup of G is normal in G.*

Remark. This generalizes the result that a transitive permutation group of degree p has a unique minimal normal subgroup. See Burnside [2, p. 202] for the case $g > p(p-1)$, and Scott [6, p. 274, Theorem 10.5.21] for the case $g \leqq p(p-1)$.

Proof. For $g = p$ the results are obvious, so suppose $g > p$. Result (iv) follows from results 3.6, 3.7 and 3.8. Let $H \neq 1$ be a normal subgroup of G. Then by Lemma 3.10, G/H is cyclic and so $G' \subseteq H$. Now $G' \neq 1$, since G is not abelian, so G' is the unique minimal normal subgroup of G and we have (i) and (ii). Since $G'' \trianglelefteq G$, applying these results to G' shows that either $|G'| = p$ and $G'' = 1$ or $G'' = G' \neq 1$; in either case G' is simple so we have (iii). If $1 \neq H \trianglelefteq G$, applying (i) and (ii) to H shows that $H' = G'$ or $H' = 1$. In the latter case, $|H| = p$ and so $G' = H$. In either case, any nonidentity normal subgroup of H contains G' and so is normal in G. By induction every subnormal subgroup of G is normal in G, and (v) is proved.

4

Throughout this section we make the following assumptions.

(A) G is a finite group with a faithful character π.

(B) The values of π are non-negative integers.

(C) The degree of π is a prime p dividing the order g of G.

(D) $q = \frac{1}{2}(p-1)$ is prime.

(E) $g > p(p-1)$, hence by Lemma 3.9, $\chi = \pi - 1_G$ is an irreducible character of G and G is insolvable.

REMARK. If these assumptions are satisfied, and $1 \neq H \trianglelefteq G$ then by Theorem 3.4, $p \mid |H|$. By Lemma 3.10, G/H is cyclic, and since G is insolvable, H is insolvable. Hence by Lemma 3.9, $|H| > p(p-1)$. It follows that the above assumptions are satisfied with H replacing G and $\pi|_H$ replacing π.

4.1. LEMMA. *If G is simple and $p \neq 5$, the order of the normalizer of a Sylow p-group is odd.*

PROOF. Let $P = \langle x \rangle$ be a Sylow p-group of G and suppose that $2 \mid |N(P)|$. Then $N(P)$ contains an element z of order 2 and z does not commute with x (Theorem 2.2). Hence $z^{-1}xz = x^{-1}$. Suppose the matrix representation Y of G affords χ. Then

$$Y(z)^{-1}Y(x)Y(z) = Y(x)^{-1}$$

and with a suitable choice of Y,

$$Y(z)^{-1}\begin{bmatrix} \varepsilon & & & \\ & \ddots & & \\ & & \ddots & \\ & & & \varepsilon^{p-1} \end{bmatrix} Y(z) = \begin{bmatrix} \varepsilon^{-1} & & & \\ & \ddots & & \\ & & \ddots & \\ & & & \varepsilon^{-(p-1)} \end{bmatrix}$$

where ε is a primitive pth root of unity. Put

$$u = \begin{bmatrix} & & & 1 \\ & & \cdot^{\cdot^{\cdot}} & \\ & \cdot^{\cdot^{\cdot}} & & \\ 1 & & & \end{bmatrix}.$$

https://doi.org/10.1017/S1446788700010624 Published online by Cambridge University Press

Then $u^{-1} = u$. (All the matrices are $(p-1)\times(p-1)$). Then

$$(Y(z)u)^{-1}\begin{bmatrix}\varepsilon & & & \\ & \ddots & & \\ & & \ddots & \\ & & & \varepsilon^{p-1}\end{bmatrix} Y(z)u = \begin{bmatrix}\varepsilon & & & \\ & \ddots & & \\ & & \ddots & \\ & & & \varepsilon^{p-1}\end{bmatrix}$$

and so $Y(z)u$ is a diagonal matrix. Put

$$Y(z)u = \begin{bmatrix}a_{11} & & & \\ & \ddots & & \\ & & \ddots & \\ & & & a_{p-1,p-1}\end{bmatrix}$$

then

$$Y(z) = \begin{bmatrix} & & & a_{11} \\ & & \iddots & \\ & \iddots & & \\ a_{p-1,p-1} & & & \end{bmatrix}.$$

Now $\chi(z) = \text{trace } Y(z) = 0$ since $p-1$ is even. As z has order 2, $\chi(z)$ is a sum of $p-1$ terms, each of which is 1 or -1. Suppose s of them are -1. Then $0 = \chi(z) = -s+p-1-s$ and so $s = \frac{1}{2}(p-1) = q$. Since q is odd when $p \neq 5$, $\det Y(z) = (-1)^q = -1$. The homomorphism $x \to \det Y(x)$ of G is an isomorphism since G is simple and $\det Y(z) \neq 1$. Therefore G is abelian, contrary to (E). Thus we conclude that $N(P)$ has odd order.

4.2. THEOREM. *If* (A), (B), (C), (D), (E) *are true, then one of the following occurs.*

(i) $g = p(p-1)k$ *where* $k \neq 1$, $k|(p-2)!$ *and* $k \equiv 1 \pmod p$. *There are* k *Sylow* p*-groups in* G. *The only non-trivial* ($\neq 1, G$) *normal subgroup of* G *is* G' *which is simple of index* 2.

(ii) $g = p(p-1)k$ *where* $k|(p-2)!$ *and* $k \equiv q+1 \pmod p$. G *has* $2k$ *Sylow* p*-groups and* $G = G'$ *is simple.*

If $p = 5$, *then in case* (i) $G \cong A_5$ *the alternating group of degree* 5, *and in case* (ii) $G \cong S_5$, *the symmetric group of degree* 5. *In each case,* π *is the corresponding transitive permutation character.*

PROOF. By Lemma 3.7, $g = p(p-1)k$ where $k|(p-2)!$. By Lemmas 3.2 and 3.5, $|N(P)|$ divides $p(p-1)$ and is greater than p. Thus $|N(P)| = 2p, qp$ or $2qp$, $n_p = qk$, $2k$ or k (respectively), and $k \equiv p-2, q+1$ or $1 \pmod p$ (respectively).

First suppose $p \neq 5$, i.e. q is odd.

(a) Suppose $|N(P)| = 2$p. Then by Lemma 4.1, G is not simple. Thus there is a non-trivial normal subgroup, whose order is divisible by but larger than qpk (Theorem 3.4). This is impossible, since $g = 2qpk$, so this case cannot occur.

https://doi.org/10.1017/S1446788700010624 Published online by Cambridge University Press

(b) Suppose $|N(P)| = qp$. Then G is simple, since any non-trivial normal subgroup would have order divisible by but larger than $2pk$ (Theorem 3.4). Thus we have case (ii).

(c) Suppose $|N(P)| = 2qp$. Then any non-trivial normal subgroup H of G has order $2pk$ or qpk by Theorem 3.4. f $|H| = 2pk$, then since $|N_H(P)| = 2p$, the case (a) above gives a contradiction. By Lemma 4.1, G is not simple, so there must be a normal subgroup of index 2. Theorem 3.11 shows that there is exactly one, namely G', and it is simple. Thus we have case (i).

Now we consider the case $p = 5$. Then $g = 20k$ where $k|6$, $k > 1$ and $k \equiv 1$ or 3 (mod 5). Hence $g = 60$ or 120.

If $g = 60$, then $n_5 = 6$ and G is simple, since any non-trivial normal subgroup would have order exceeding 30 (Theorem 3.4). Thus we have case (ii). Moreover $G \cong A_5$, since up to isomorphism there is only one simple group of order 60 [2, p. 504]. Now A_5 has only one irreducible character of degree 4 [5, pp. 265, 272], so π is the required permutation character.

If $g = 120$, then $n_5 = 6$. Any non-trivial normal subgroup has order 60 (Theorem 3.4). If there is such a subgroup, then by Theorem 3.11, it is unique, equal to G' and simple. Now G can be faithfully represented as a transitive permutation group of degree 6 on its Sylow 5-groups. The subgroups of order 120 of S_6 are all isomorphic to S_5 [2, pp. 208–209], so $G \cong S_5$. Because S_5 has exactly one irreducible character of degree 4 whose values are integers no smaller than -1 [5, p. 265], π is a transitive permutation character. Now S_5 is not simple, hence $[G : G'] = 2$. Thus we have case (i).

The proof of the theorem is now complete.

We conclude by stating some further results without proof.

4.3. *Under the hypotheses of Section* 4, *if* $8 \nmid g$, *then* $G \cong PSL(2, 11)$ *or* $G \cong A_5$.

4.4. THEOREM. *Suppose the hypotheses* (A) and (B) *of Section* 4 *hold and* (E)′

$$\pi - 1_G \textit{ is irreducible.}$$

Suppose the degree p of π *is* 2, 3, 5, *or* 7. *Then the order of G is divisible by p, and* π *is a transitive permutation character.*

REMARK. Here we did not need to assume that $p|g$. However the assumptions imply $\langle \pi, 1_G \rangle = 1$, and perhaps this is equivalent to (C) under (A) and (B).

References

[1] R. Brauer, 'A note on theorems of Burnside and Blichfeldt', *Proc. Amer. Math. Soc.* 15 (1964), 31–34.
[2] W. Burnside, *Theory of groups of finite order* (New York: Dover 1955, 2nd edition 1911).

[3] W. Feit and J. G. Thompson, 'Solvability of groups of odd order', *Pacific J. Math.* 13 (1963), 775–1029.
[4] M. Hall, *The theory of groups* (New York: Macmillan, 1959).
[5] D. E. Littlewood, *The theory of group characters* (Oxford: University Press, 2nd edition 1950).
[6] W. R. Scott, *Group theory* (Englewood Cliffs, N.J.: Prentice-Hall, 1964).
[7] B. L. van der Waerden, *Modern algebra vol.* 1 (New York: Ungar, 1950).
[8] W. J. Wong, 'Linear groups analogous to permutation groups', *Journ. Australian Math. Soc.* 3 (1963), 180–184.
[9] W. J. Wong, 'On linear *p*-groups', *Journ. Australian Math. Soc.* 4 (1964), 174–178.

University of Sydney
Sydney, N.S.W.