PACIFIC JOURNAL OF MATHEMATICS
Vol. 25, No. 3, 1968

ON FINITE GROUPS CONTAINING A CCT-SUBGROUP WITH A CYCLIC SYLOW SUBGROUP

MARCEL HERZOG

Let G be a finite group containing a CCT-subgroup M. M is called a *CCT-subgroup* of G if M contains the centralizer in G of each of its nonunit elements and it is also a trivial-intersection subset of G. In this paper the p-blocks of characters of G of full defect are described in detail, under the additional assumption that the Sylow p-subgroups of M are cyclic and nontrivial. This information yields, under the same conditions, a detailed characterization of the nonexceptional (with respect to M) irreducible characters of G. As an application, it is shown that if G is also perfect, its order is less than $qm(m^2+3m+2)/2$, where m is the order of M and qm is the order of $N_G(M)$, and $N_G(M) \neq M, G$, then G is isomorphic either to $PSL(2, p)$, $m = p > 3$, or to $PSL(2, m-1)$, $m-1 = 2^b$, $b > 1$. These results generalize those of R. Brauer, dealing with the case $m = p$.

We proceed with a precise statement of the results. Quite recently, E. C. Dade [4] obtained a very detailed information about blocks with cyclic defect groups. Using his results, we will prove the following

THEOREM 1. *Let G be a finite group of order g and suppose that G contains a subgroup M of order m, satisfying the following conditions:*

(i) *for all $h \in M^\#$, $C_G(h) \subseteqq M$*

(ii) *a Sylow p-subgroup P of M is cyclic of order p^a, $a \geqq 1$*

(iii) $q = [N_G(M): M] > 1, g > qm$.

Then the nonexceptional (with respect to M) irreducible characters of G, nonvanishing on $M^\#$, are of one of the following two types:

(I) $P_i(i = 1, \cdots, y) - P_i(1) = r_i m + 1, P_i(h) = 1$ *for all* $h \in M^\#$

(II) $Q_i(i = 1, \cdots, q - y) - Q_i(1) = s_i m - 1, Q_i(h) = -1$ *for all* $h \in M^\#$

where $1 \leqq y \leqq q$ and r_i, s_i are nonnegative integers.

The assumptions of Theorem 1 imply that M is a nilpotent Hall subgroup of G, which is a trivial-intersection-subset of G. It follows, hence, that the Sylow p-subgroups of G are cyclic, of order p^a. The situation described in Theorem 1 is similar to that which was summarized by R. Brauer in [1, pp. 59-60], for the case that M satisfies condition (i) and $m = p$.

Theorem 1 follows quite easily from the following proposition, which is of independent interest. Since we are to distinguish between the (irreducible) exceptional characters of G with respect to M (see W. Feit [5]) and those with respect to the cyclic p-group P (in the sense of E. C. Dade [4]), the latter ones will be called p-exceptional. An irreducible character is p-nonexceptional if it is not p-exceptional.

PROPOSITION. Let G and M satisfy the assumptions of Theorem 1. Let t be the number of conjugate classes of G meeting $M^{\#}$ nontrivially. Then the p-blocks of G are listed and described below:

(I) d blocks of defect 0, each containing one ordinary irreducible character and one modular irreducible character.

(II) One block of defect a, containing q modular irreducible characters, q p-nonexceptional characters and $(p^a - 1)/q$ p-exceptional characters.

(III) $(tq + 1 - p^a)/p^a q$ blocks of defect a, each containing one modular irreducible character, one p-nonexceptional character and $p^a - 1$ p-exceptional characters.

As an application of Theorem 1, we will prove the following generalization of the main result of R. Brauer in [1]. Theorem 1 is also needed in a forthcoming paper.

THEOREM 2. *Let G be a finite group of order g and assume that $G = G'$. Suppose that G contains a subgroup M of order m, satisfying conditions* (i)—(iii) *of Theorem* 1.

Then $g = qm(nm + 1)$, where n is a positive integer, and one of the following statements holds:

(I) $n = (muw + u^2 + u + w)/(u + 1)$
where u and w are positive integers.

(II) $n = 1, m = p, q = (p - 1)/2, G \cong PSL(2, p), p > 3$.

(III) $n = (m - 3)/2, q = 2, m = 2^b + 1 > 3, G \cong PSL(2, m - 1)$.

As an immediate corollary we get:

COROLLARY. *Let G and M satisfy the assumptions of Theorem* 2. *If $n < (m + 3)/2$, then G is a simple group either of type* (II) *or of type* (III).

The arguments applied in the proof of Lemma 2.2 are quite similar to those used by *R*. Brauer in his proof of Theorem 7 in [1]. However, for the sake of completeness, the proof is given in full detail.

Most of our notation is standard. If G is a group, then $G^{\#}$ and 1_G denote, respectively, the nonunit elements of G and its principal irreducible character. If p and q are rational integers, then (p, q) denotes the greatest common divisor of p and q, and $p \mid q$ means: p divides q. If u, e, h are elements of the group G, then $n(u)$ is the order of the centralizer of u in G and c_{ueh} is the coefficient of the conjugate class of h in the product of the conjugate classes of u and e.

1. Proof of the Proposition and of Theorem 1. In this proof by blocks we mean p-blocks. Since $q > 1$, M is a nilpotent group and $P \subseteqq Z(M)$. It follows, in view of assumptions (i) and (ii), that G has blocks of defect 0 and a only. The blocks of defect 0 are well known to be of type (I)(see [3], Th. 86.3). Therefore it remains to show that the blocks of defect a are either of type (II) or of type (III), and their number is correct.

If $m = p$, then the Proposition and Theorem 1 follow by Brauer [1,pp.59-60]. In that case G has only one block of defect a, as required. Therefore, from now on, we will assume that $m > p$. Since $N_G(M)$ is a Frobenius group and P is cyclic, it follows that $q \leqq p - 1$ and $q < \sqrt{m - 1}$.

As P is cyclic, the blocks $B_1, \cdots, B_u$ of defect a were described by Dade [4]. Each B_i contains e_i modular irreducible characters, e_i p-nonexceptional characters and $(p^a - 1)/e_i$ p-exceptional characters, where e_i is an integer dividing q.

Let d' be the number of the irreducible characters of G vanishing on $M^\#$. We will show that $d' = d$. Let X be an irreducible character of G vanishing on $M^\#$. Then $m \mid X(1)$, and since m is divisible by the full p-part of $|G|$, X has defect 0. Thus $d' \leqq d$. On the other hand, G and M satisfy the assumptions of Hypothesis A in [6]. By [6], Lemma 3.1.d, $c = 0$. Hence, according to the formulas following Hypothesis A, the degrees of the irreducible characters of G, non-vanishing on $M^\#$, are of one of the following forms:

$$z(fm + q\varepsilon), \; rm + s$$

where f and r are nonnegative integers, $\varepsilon = \pm 1$, s is the value taken on $M^\#$ by the corresponding nonexceptional character, hence a nonzero integer, and z is a degree of an irreducible character of M. Since P is a normal abelian subgroup of M, it follows by Ito (see [3], Corollary 53.18) that z divides $[M: P]$, hence $(z, p) = 1$. As also $(q, p) = 1$, it follows that no character of degree $z(fm + q\varepsilon)$ belongs to a block of defect 0. Since by the definition of T and by [6], Lemma 3.1.b $s \leqq T \leqq q$, it follows that $(s, p) = 1$ and no character of degree $rm + s$ belongs to a block of defect 0. Consequently, $d \leqq d'$ and the equality follows.

It is well known, that the number of the modular irreducible characters of G is equal to the number of (conjugate) classes in G minus the number of p-singular classes in G (see [3], Th. 83.5). In view of the nilpotency of M, the number of the p-singular classes in M is $(p^a - 1)(tq + 1)/p^a$, and the corresponding number for G is $(p^q - 1)(tq + 1)/qp^a$. Let b be the number of the nonexceptional characters of G, nonvanishing on $M^\#$. Then, t being the number of the exceptional characters of G, the number of the conjugate classes in G is $t + b + d$. It follows from the above mentioned equality, remarks and the results of Dade that:

$$\sum e_i + d = t + b + d - (p^a - 1)(tq + 1)/qp^a$$

where the summation is over $i = 1, \cdots, u$. The index of summation i will run over these values throughout this proof. It follows that:

$$\sum e_i = t + b - (p^a - 1)(tq + 1)/qp^a \,. \tag{1}$$

Since the number of the (ordinary) irreducible characters of G is equal to the number of the conjugate classes in G, we get, using once more Dade's results, that after subtraction d from both sides:

$$(p^a - 1) \sum (1/e_i) + \sum e_i = t + b \,. \tag{2}$$

Equations (1) and (2) yield:

$$t = p^a \sum (1/e_i) - (1/q) \tag{3}$$

$$b = \sum e_i - \sum (1/e_i) + (1/q) \,. \tag{4}$$

It is also well known, that the number of blocks of defect a is equal to the number of p-regular conjugate classes of G of defect a (see [3], Th. 86.10). Thus:

$$u = t - (p^a - 1)(tq + 1)/qp^a + 1 = (tq + 1 - p^a)/p^a q + 1 \,. \tag{5}$$

Finally let $q = e_i f_i$. It follows from (3) and (5) that:

$$u = (1/q) \sum f_i - (1/q) + 1$$

$$\sum f_i = uq + 1 - q \,. \tag{6}$$

Suppose that $f_i \neq q$. Then $f_i \leqq q/2$ and it follows from (6) that at most one f_i, say f_1, is unequal to q. Hence:

$$f_1 + (u - 1)q = (u - 1)q + 1$$

and consequently:

$$f_1 = 1, e_1 = q, f_2 = \cdots = f_u = q, e_2 = \cdots = e_u = 1 \,. \tag{7}$$

The Proposition follows from (5), (7) and the results of Dade.

Equations (4) and (7) immediately yield $b = q$. Thus there are q nonexceptional characters nonvanishing on $M^{\#}$ and therefore, in view of [6], Lemma 3.1.b, they are either of type (I) or of type (II). As the principal character is of type (I), $y \geqq 1$. This completes the proof of Theorem 1.

2. Proof of Theorem 2. By [6], Theorem 2.3, $N_G(M) = QM$, where $Q \cap M = 1$ and $g = qm(nm + 1)$. Since $q \neq 1$, M is a nilpotent group with a cyclic Sylow subgroup, hence Q is abelian. As $G = G'$, $n \neq 0$.

If $m = p$, then the theorem holds by Brauer ([1], Th. 10). Therefore, from now on, we will assume that n does not satisfy (I), $m > p$ and will prove that then G satisfies (III). Since P is cyclic, it follows that $1 < q < \sqrt{m} - 1$ and $q \leqq p - 1$.

The groups G and M now satisfy the assumptions of Hypothesis A in [6]. Therefore it follows from Theorem 3.1 there that $c = 0$, and by Thorem 1 of this paper, $c_i = \pm 1$. Consequently, taking into account the formulas preceding Theorem 3.1 in [6], the degrees of the nonprincipal irreducible characters of G, nonvanishing on $M^{\#}$, are:

$$\begin{aligned} &\text{the exceptional characters: } z(bm + q\varepsilon) = (z/v)[(bv + \varepsilon)m - \varepsilon] \\ &\text{the nonexceptional characters: } um \pm 1 \end{aligned} \tag{8}$$

where u is a positive integer, b is a nonnegative integer, $\varepsilon = \pm 1$, $v = (m - 1)/q$ and z is a degree of an irreducible character of M. By Ito ([3], Corollary 53.18) z divides $[M: P]$, hence $z < v$.

We will proceed with a series of lemmas.

LEMMA 2.1. *G is a simple group and m is an odd integer.*

Proof. Let K be a normal complement of $N_G(M)$ in G. Then K is nilpotent and G is solvable, a contradiction. Therefore $N_G(M)$ has no normal complement in G.

Let now K be a nontrivial, proper normal subgroup of G. Then by [6], Theorem 2.3, the order of K is either of the form $wm + 1$, where $wm + 1$ divides $nm + 1$ and $n = ywm + y + w$ for some nonnegative integer y, or it is of the form $q_0m(nm + 1)$, where q_0 divides q. Suppose that the first case occurs. As shown above, $w \neq n$, and hence y is a positive integer. Let $x = (w + 1)y$; then

$$n = (xwm + x + w^2 + w)/(w + 1) ,$$

which has been assumed not to be the case. On the other hand, the order of K could not be $q_0m(nm + 1)$, since that would force the existence of a nonprincipal irreducible character of G of degree less than q, which is not the case. Thus G is a simple group.

If m is even, then it follows from Suzuki ([8]), Theorem 1) and the fact that $q \neq 1$, that M is a Sylow 2-group of G. Hence $p = 2$ and consequently $q = 1$, a contradiction. It follows that m is odd, and the proof of the lemma is complete.

LEMMA 2.2. *The degrees of the nonprincipal irreducible characters of G, nonvanishing on $M^{\#}$, are:*
the exceptional characters: $z(nm+1)/v$
the nonexceptional characters: $m-1$ *or* $nm+1$
where z and v are as described above.
Moreover, $\varepsilon = -1$ *and* $v \mid n+1$.

Proof. In view of (8), it suffices to show that if

$$um + 1 \mid (m-1)(nm+1)$$

then $u = n$, if $um - 1 \mid (m-1)(nm+1)$ and $um - 1 \neq (m-1)(nm+1)$ then $u = 1$, and no irreducible character of G of degree $z(m-1)/v = zq$ exists. Indeed, by (8) each character in question has order of the form $k(um+\delta)$, where k is either 1 or z/v and $\delta = \pm 1$. If $\delta = 1$ then $u = n$, as required. If $\delta = -1$, then either $um - 1 = (m-1)(nm+1)$ or $u = 1$. If $u = 1$, then $k = 1$ and the corresponding character is not an exceptional one. If $um - 1 = (m-1)(nm+1)$, then:

$$k^2(um-1)^2 \geqq (m-1)^2(nm+1)^2/v^2 > qm(nm+1)$$

a contradiction. Thus if $k = z/v$ then $\delta = 1$ and $u = n$; it follows also that $\varepsilon = -1$ and v divides $nm + 1 - n(m-1) = n+1$.

Let $um + 1 = de$, where $d \mid m-1$ and $e \mid nm+1$. Suppose that $n < u$. Then $d \mid u+1$ and $e \mid u-n$. Hence $(u+1)(u-n) = w(um+1)$, where w is a positive integer and:

$$u+1 \mid w(m-1),\ u \leqq wm - w - 1$$

$$u^2 = u(wm + n - 1) + w + n,\ u > wm + n - 1$$

a contradiction. If on the other hand, $n > u$ then $d \mid u+1$ and $e \mid n-u$. It follows that $(u+1)(n-u) = w(um+1)$, where w is a positive integer, and n is of form (I), a contradiction. Thus $u = n$.

Let $um - 1 = de$, where $d \mid m-1$ and $e \mid nm+1$. Suppose that $u > 1$. Then $d \mid u-1$ and $e \mid n+u$. Hence:

$$(u-1)(n+u) = w(um-1) \tag{9}$$

where w is a positive integer, and considering this equation as a quadratic equation for u, we get that the second root $u' = (w - n)/u$ is an integer. Since for $u = 1$ the left hand side of (9) vanishes, while the right hand side is positive, it follows that $u' \leqq 0$. Let $u' = -u''$, and suppose first that $u'' = 0$. Then $w = n$, and (9) yields:

$$u = n(m - 1) + 1, um - 1 = (nm + 1)(m - 1) .$$

Therefore if $um - 1 \neq (nm + 1)(m - 1)$ then u'' is a positive integer and $-u''$ satisfies equation (9). Consequently, n satisfies (I), which is not the case. Thus $u = 1$.

Finally assume that $x = zq$ is a degree of an irreducible character of G. As z is a degree of an irreducible character of $M^\#$, it is well known that $z^2 \leqq [M\colon Z(M)] \leqq m/2p$. It follows that

$$x = zq \leqq \sqrt{m/2p}\sqrt{m} - 1 < (m - 1)/2 .$$

But then, since G is simple, the character of degree x satisfies the assumptions of Theorem 4.2 [7]. This is a contradiction, since the group G does not satisfy any of the conclusions of that theorem. Thus no irreducible character of degree zq exists, and the proof of the lemma is complete.

LEMMA 2.3.

$$g = (m - 1)m[(q - 1)m - q]$$

and no nonexceptional character of G is of degree $nm + 1$.

Proof. Let $h \in M^\#$ and let y have the same meaning as in Theorem 1. Then it follows from Lemma 2.2, Theorem 1 and from the summation formulas of § 3 in [6] that:

$$\begin{aligned} 0 &= \sum X(1)X(h) \\ &= 1 + (fm - q)(-\varepsilon) + (y - 1)(nm + 1) - (q - y)(m - 1) \end{aligned}$$

where the summation ranges over all the irreducible characters of G and $f = (n + 1)/v, fm - q = (mn + 1)/v$. After cancellation, we get:

$$q = f + y(n + 1) - n = (n + 1)/v + y(n + 1) - n .$$

Suppose that $y > 1$; then, as $v \leqq n + 1$:

$$q > (n + 1)/v + n + 1 > v, m - 1 = qv < q^2$$

in contradiction to our assumptions. Therefore $y = 1$ and $n = (q-1)v-1$. Consequently, there are no nonexceptional characters of degree $nm + 1$, and:

$$g = qm[(q - 1)vm - (m - 1)] = (m - 1)m[(q - 1)m - q] .$$

LEMMA 2.4.

$$q = 2 .$$

If u is an involution of $N_G(M)$, then $n(u) = m - 1$.

Proof. By Lemma 2.3,

$$g = (m - 1)mr$$

where $r = (q - 1)m - q$. It is easy to see that the three factors are prime to each other.

Let u, h and e be elements of $G^{\#}$, whose orders divide $m - 1, m$ and r, respectively. Let X, R and D be: an exceptional character of G, a nonprincipal nonexceptional character of G nonvanishing on $M^{\#}$ and an irreducible character of G vanishing on $M^{\#}$, respectively. Let s be a prime divisor of the order of u. Then R, being of degree $m - 1$, belongs to an s-block of defect 0, and consequently $R(u) = 0$ (see [3], Th. 86.3). Similarly, $X(e) = 0$. We, therefore, get the following character table:

	1	u	h	e
1_G	1	1	1	1
X	$z(nm + 1)/v$			0
R	$m - 1$	0	-1	
D	am		0	

By the well known formula for c_{ueh} it follows that:

$$c_{ueh} = g/n(u)n(e) , \qquad n(u)n(e) \mid (m - 1)r .$$

Since e is an arbitrary element of order dividing r, it follows that $n(u) \mid m - 1$.

As m is odd, $m - 1$ is even. Let now u be an involution of G, and let C be the conjugate class of G containing u, of order c. Then:

$$c \geqq g/(m - 1) > g/m - 1$$

and by [2], Theorem (4K), and the trivial intersection property of M, q is even.

Let, finally u be an involution belonging to $N_G(M)$. Then it follows from [2], Theorem (4J), that $n(u) \geqq m - 1$. Since $n(u) \mid m - 1$, $n(u) = m - 1$. The same theorem also yields:

$$g = (m - 1)m(m - q) .$$

Thus, in view of Lemma 2.3, $q = 2$ and the proof of the lemma is complete.

Theorem 2 now follows from Lemma 2.4 and a result of Suzuki [9]. Suzuki has shown, that if Lemma 2.4 holds, then G is of type (III).

REFERENCES

1. R. Brauer, *On permutation groups of prime degree and related classes of groups*, Ann. of Math. **44** (1943), 55-79.
2. R. Brauer, and K. A. Fowler, *On groups of even order*, Ann. of Math. **62** (1955), 565-583.
3. C. W. Curtis, and I. Reiner, *Representation Theory of Finite Groups and Associative Algebras*, Interscience Publishers, 1962.
4. E. C. Dade, *Blocks with cyclic defect groups*, Ann. of Math. **84** (1966), 20-48.
5. W. Feit, *On a class of doubly transitive permutation groups*, Illinois J. Math. **4** (1960), 170-186.
6. M. Herzog, *On finite groups which contain a Frobenius subgroups*, J. Algebra **6** (1967), 192-221.
7. H. S. Leonard, Jr., *On finite groups which contain a Frobenius factor group*, Illinois J. Math. **9** (1965), 47-58.
8. M. Suzuki, *Two characteristic properties of* (ZT)*-groups*, Osaka Math. J. **15** (1963), 143-150.
9. ———, *An abelian subgroup which is the centralizer of its non-identity elements*, Lecture, Midwestern Conference on Group Theory and Number Theory, Columbus, Ohio, 3.30-4.2., 1966.

Received April 24, 1967.

UNIVERSITY OF ILLINOIS
URBANA, ILLINOIS