PACIFIC JOURNAL OF MATHEMATICS
Vol. 109, No. 2, 1983

CHARACTERS VANISHING ON ALL BUT TWO CONJUGACY CLASSES

STEPHEN M. GAGOLA, JR.

If the character table of a group G has a row (corresponding to an irreducible character) with precisely two nonzero entries, then G has a unique minimal normal subgroup N which is necessarily an elementary abelian p-group for some prime p. The group $G/O_p(G)$ is completely determined here. In general, there is no bound on the derived length or nilpotence class of $O_p(G)$.

1. Introduction. An old theorem of Burnside asserts that, for any group G, any irreducible character of degree greater than 1 vanishes at some element of G (for a proof of this fact, see p. 40 of [7]). The extreme case will be considered here, namely, groups G for which a character exists which vanishes on all but two conjugacy classes. Clearly no irreducible character can vanish on all but one conjugacy class (unless $|G| = 1$).

The remaining sections of this paper are devoted to determining the structure of such groups G. Specifically, §2 is devoted to some preliminary lemmas about the action of G on its unique minimal normal subgroup N. The kernel of G on N is $\mathbf{C}_G(N) = O_p(G)$ for some prime p and $G/O_p(G)$ is determined by Theorems 4.2 and 5.6. The subgroup $O_p(G)$ can be quite complicated and this, together with some examples, are discussed in §6.

2. Some preliminary results. As already mentioned in the previous section, if a group G has an irreducible character which does not vanish on only two conjugacy classes, then G has a unique minimal normal subgroup N. The first lemma of this section establishes this, in addition to some properties of the action of G on N.

LEMMA 2.1. *Let G be a group which has an irreducible character χ such that χ does not vanish on exactly two conjugacy classes of G. If $|G| > 2$ then χ is unique and is, moreover, the unique faithful irreducible character of G. In all cases, G contains a unique minimal normal subgroup N which is necessarily an elementary abelian p-group for some prime p. The character χ vanishes on $G - N$ and is nonzero on N. Finally, the action of G by conjugation on N is transitive on $N^{\sharp}$.*

Proof. The conclusion of the theorem is trivial if $|G| = 2$, so assume $|G| > 2$. Clearly χ does not vanish at $1 \in G$. Let $x \in G$ be chosen so that

$x \neq 1$ and $\chi(x) \neq 0$. Now $\chi \neq 1_G$ since $|G| > 2$ and so $(\chi, 1_G) = 0$. Hence $\chi(x) < 0$. If h is the size of the conjugacy class containing x and $\chi(x) = -s$ then $(\chi, 1_G) = 0$ implies $\chi(1) - sh = 0$. Let ψ be any irreducible character of G different from χ. Then $(\chi, \psi) = 0$ and so $\chi(1)\psi(1) - hs\psi(x) = 0$ and hence $\psi(x) = \psi(1)$. Thus x is in the kernel of every irreducible character of G different from χ. Since χ is faithful, it is the unique faithful character of G, and no other character of G can vanish on all but two classes.

Let N be the (normal) subgroup of G generated by the conjugacy class of x. The argument in the preceding paragraph showed that $N \leq \ker \psi$ for every irreducible character ψ different from χ. If there exists a nonidentity element, say y, of N that is not conjugate to x, then the second orthogonality relation applied to the classes containing x and y yields a contradiction.

Thus G is transitive on $N^\#$, $\chi(y) = -s$ for all $y \in N^\#$ and χ vanishes on $G - N$. Since all nonidentity elements of N are conjugate in G, N must be an elementary abelian p-group for some prime p. It remains only to prove that N is the unique minimal normal subgroup of G.

Let M be any normal subgroup of G different from 1, and let $\mathfrak{X}$ be the set of irreducible characters ψ of G with kernel containing M. Since χ is faithful, we know $\chi \notin \mathfrak{X}$. Hence, by the second paragraph of the proof, $N \leq \ker \psi$ for every $\psi \in \mathfrak{X}$ and so

$$M = \bigcap_{\psi \in \mathfrak{X}} \ker \psi \geq N,$$

proving that N is the unique minimal normal subgroup of G. □

LEMMA 2.2. *Let χ be an irreducible character of G and N a normal subgroup of G. Assume χ vanishes on $G - N$ and let λ be an irreducible constituent of χ_N. Define $m = (\chi_N, \lambda)$ and $T = \mathfrak{I}_G(\lambda)$ (the inertia group of λ in G). Then λ^T has a unique irreducible constituent, say θ. Moreover, $\theta^G = \chi$, $\theta|_N = m\lambda$ and $|T : N| = m^2$ so θ is fully ramified over N.*

Proof. If $\lambda = \lambda_1, \lambda_2, \ldots, \lambda_t$ are the distinct G-conjugates of λ then $t = |G : T|$ and $\chi_N = m(\lambda_1 + \lambda_2 + \cdots + \lambda_t)$ by Clifford's Theorem. By that same theorem, there exists a one-to-one correspondence between the irreducible constituents of λ^T and those of λ^G, the correspondence being the induction map. Thus, there exists a unique constituent of λ^T, say θ, which satisfies $\theta^G = \chi$, and $\theta|_N = m\lambda$. Now θ will be the unique irreducible constituent of λ^T if χ is the unique constituent of λ^G.

Suppose χ' is an irreducible constituent of λ^G. Then $\chi'_N = k(\lambda_1 + \cdots + \lambda_t)$ for some positive integer k. As χ vanishes on $G - N$ we have

$$\begin{aligned}(\chi, \chi') &= \frac{1}{|G|} \sum_{g \in N} \chi(g)\overline{\chi'(g)} \\ &= \frac{1}{|G:N|}(m(\lambda_1 + \cdots + \lambda_t), k(\lambda_1 + \cdots + \lambda_t)) = \frac{mkt}{|G:N|}.\end{aligned}$$

Thus $(\chi, \chi') \neq 0$ so $\chi' = \chi$ and hence χ is the unique irreducible constituent of λ^G. As remarked earlier, this means θ is the unique constituent of λ^T. The calculation above also proves $|G: N| = m^2 t$ so $|T: N| = m^2$. Hence θ is fully ramified over N. □

COROLLARY 2.3. *Let χ be an irreducible character of G which vanishes on all but two conjugacy classes of G. If $|G| = 2$ assume χ is the faithful character of G. Then $N = \{x \in G | \chi(x) \neq 0\}$ is the unique minimal normal subgroup of G, and N is an elementary abelian p-group for some prime p. If $x \in N^\#$ and λ is any nonprincipal irreducible character of N, then both $\mathbf{C}_G(x)$ and $T = \mathcal{I}_G(\lambda)$ are Sylow p-subgroups of G. Moreover, T has a unique irreducible character θ which is a constituent of λ^T, and θ is fully ramified over N. Finally, $\chi = \theta^G$.*

Proof. That N is the unique minimal normal subgroup of G follows from Lemma 2.1. Suppose λ is a nonprincipal irreducible character of N. Lemma 2.1 implies G is transitive on $N^\#$ and hence is transitive on the nonprincipal characters of N. As χ is faithful, this implies λ is a constituent of χ_N. Lemma 3.2 now implies $T = \mathcal{I}_G(\lambda)$ has a unique irreducible character θ, such that θ is a constituent of λ^T, and θ is fully ramified over N. That same lemma also implies $\theta^G = \chi$.

Since λ is invariant in T, $\ker\lambda \trianglelefteq T$ and $N/\ker\lambda$ is central in $T/\ker\lambda$. Choose any prime $q \neq p$ and let $Q/\ker\lambda$ be a Sylow q-subgroup of $T/\ker\lambda$. By Lemma 2.2 of [**3**], θ_{NQ} is a multiple of some unique irreducible character of NQ, say ζ, and of course, $\ker\zeta$ contains $\ker\lambda$. Since $N/\ker\lambda$ is central in $T/\ker\lambda$, that same lemma implies ζ_Q is fully ramified over $N \cap Q = \ker\lambda$. Thus $Q/\ker\lambda$ has an irreducible character which is fully ramified over the identity subgroup. This can only happen if $Q/\ker\lambda$ is itself the trivial group. Hence, q does not divide $|T|$ for any prime q different from p, implying that G is a p-group.

Since G is transitive on the nonprincipal irreducible characters of N, $|G: T| = |N| - 1$ is prime to p and hence T is a Sylow p-subgroup of G.

If $x \in N^{\sharp}$, then $|G\colon \mathbf{C}_G(x)| = |N| - 1$ as G is transitive on $N^{\sharp}$, and this proves $\mathbf{C}_G(x)$ is also a Sylow p-subgroup of G. □

LEMMA 2.4. *Let G be a group which acts on an elementary abelian p-group N. Assume G is transitive on $N^{\sharp}$ and the centralizer of any element of $N^{\sharp}$ in G is a Sylow p-subgroup of G. Let S be any normal subgroup of G and P a Sylow p-subgrokup of S. Define $W = \mathbf{C}_N(P)$ and $U = [N, P]$. Then*:

(a) *$\{W^g | g \in G\}$ is a partition of N. In particular, $|N|$ is a power of $|W|$.*

(b) *$\mathbf{N}_G(P) = \mathbf{N}_G(W) = \mathbf{N}_G(U)$, and this subgroup is transitive on the nonidentity elements of both W and N/U. In particular, the order of this subgroup is $(|W| - 1) \cdot |G|_p$, where $|G|_p$ is the p-part of the order of G.*

(c) *$|W| = |N/U|$ and W and U are the unique minimal and maximal subgroups, respectively, of N that are normalized by $\mathbf{N}_G(P)$.*

Proof. Suppose $W \cap W^g$ is nontrivial for some $g \in G$. Then $w_1^g = w \in W^{\sharp}$ for some $w_1 \in W^{\sharp}$. Now $\mathbf{C}(w_1) \cap S$ and $\mathbf{C}(w) \cap S$ are both p-subgroups of S which contain the Sylow p-subgroup P of S. Therefore, $P = \mathbf{C}(w_1) \cap S = \mathbf{C}(w) \cap S$ and hence $g \in \mathbf{N}(P)$. Clearly, $\mathbf{N}(P) \leq \mathbf{N}(W)$ and so $W^g = W$, proving that the distinct conjugates of W intersect trivially. Since G is transitive on $N^{\sharp}$, the conjugates of W cover N and, hence, partition N. The above argument also shows $\mathbf{N}(W) \leq \mathbf{N}(P)$ and, hence, equality holds.

If w_1 and w_2 belong to $W^{\sharp}$ then transitivity of G implies $w_1^g = w_2$ for some $g \in G$. By the preceding paragraph, $g \in \mathbf{N}(P) = \mathbf{N}(W)$ and hence $\mathbf{N}(W)$ is transitive on $W^{\sharp}$. As $\mathbf{C}_G(w) \leq \mathbf{N}(W)$ and $\mathbf{C}_G(w)$ is a Sylow p-subgroup of G for $w \in W^{\sharp}$, the group order formula of part (b) follows. Clearly, W is an irreducible $\mathbf{N}(P)$-submodule of N.

The hypotheses of Lemma 2.4 are satisfied if N is replaced by the dual group $\hat{N}$ (which is the set of irreducible characters of N). Hence $\mathbf{N}(P)$ acts transitively on the nonprincipal characters in $\mathbf{C}_{\hat{N}}(P)$ which is naturally isomorphic to the dual group of N/U. Therefore, $\mathbf{N}(P)$ acts transitively on the nonidentity elements of N/U. Clearly, $\mathbf{N}(P) \leq \mathbf{N}(U)$ and a comparison of their orders shows that equality holds. Clearly $|W| = |N/U|$.

Finally, as any maximal $\mathbf{N}(P)$-submodule of N contains $[N, P] = U$ and any minimal submodule of N is contained in $\mathbf{C}_N(P) = W$, part (c) follows. □

If G is a group which contains an irreducible character which vanishes on all but 2 conjugacy classes, then Lemma 2.4 applies, where N is the unique minimal normal subgroup of G. The special case $S = G$ is worth pointing out. Here, P is a Sylow p-subgroup of G, and $\mathbf{N}_G(P)/[N, P]$ is a group satisfying the same hypothesis that G does.

THEOREM 2.5. *Let G be a group which has an irreducible character χ which vanishes on all but two conjugacy classes of G. Let N be the unique minimal normal subgroup of G guaranteed by Corollary 3.3 so that $N \subseteq O_p(G)$ for some prime p. Finally, let P be a Sylow p-subgroup of G. Then*:

(a) *For every $x \in G - N$, the order of $\mathbf{C}_G(x)$ is the same as the order of $\mathbf{C}_{G/N}(xN)$.*

(b) *$\mathbf{Z}(P) \subseteq N$ and $\mathbf{Z}(P) = N$ if and only if $P \trianglelefteq G$.*

(c) *N is a term of the upper central series of P. In particular, N is a characteristic subgroup of P.*

Proof. (a) is immediate from the second orthogonality relations in G and G/N, as $\chi(x) = 0$.

Suppose $\mathbf{Z}(P) \not\leq N$ and choose $y \in \mathbf{Z}(P) - N$. Then the p-part of the order of $\mathbf{C}_G(y)$ is divisible by $|P|$ and the same must be true of $\mathbf{C}_{G/N}(yN)$ by (a). But $|P|$ does not divide the order of G/N, and this contradiction proves $\mathbf{Z}(P) \leq N$.

If $y \in \mathbf{Z}(P)^{\#}$, then Corollary 3.3 implies $\mathbf{C}_G(y) = P$ so $P = \mathbf{C}_G(\mathbf{Z}(P))$. Thus, if $\mathbf{Z}(P) = N$, then $P = \mathbf{C}_G(N) \trianglelefteq G$. Conversely, if $P \trianglelefteq G$, then $N \leq \mathbf{Z}(P)$ as N is the unique minimal normal subgroup of G, and hence $N = \mathbf{Z}(P)$.

It now remains to prove that N is a term of the upper central series of P. Let $\mathbf{Z}_i(P)$ denote the ith term of the upper central series for P, and choose i so that $\mathbf{Z}_i(P) \leq N$ and $\mathbf{Z}_{i+1}(P) \not\leq N$. From the earlier part of this proof we have $i \geq 1$. Let $y \in \mathbf{Z}_{i+1}(P) - N$. Now the conjugacy class of y in P is entirely contained in $y\mathbf{Z}_i(P)$ so $|P\colon \mathbf{C}_P(y)| \leq |\mathbf{Z}_i(P)|$. Hence, $|\mathbf{C}_P(y)|$ is divisible by $|P/\mathbf{Z}_i(P)|$, so $|P/\mathbf{Z}_i(P)|$ divides the p-part of the order of $\mathbf{C}_G(y)$. Now $|\mathbf{C}_G(y)| = |\mathbf{C}_{G/N}(yN)|$, and a Sylow p-subgroup of G/N has order $|P/N|$. Hence, $|P/\mathbf{Z}_i(P)|$ divides $|P/N|$, proving $|\mathbf{Z}_i(P)| \geq |N|$. This proves $\mathbf{Z}_i(P) = N$, and the proof of Theorem 2.5 is complete. $\square$

3. A digression on doubly-transitive Frobenius groups. The simplest example of a group which possesses an irreducible character vanishing on all but two conjugacy classes is a doubly-transitive Frobenius group. In this case the minimal normal subgroup N is the Frobenius kernel. Using the notation of the introduction, $N = O_p(G) = \mathbf{C}_G(N)$, and of course, $G/O_p(G)$ is isomorphic to the Frobenius complement. It is clear that the determination of $G/O_p(G)$ in the general case will have to involve Frobenius complements of doubly-transitive Frobenius groups.

Although not essential for this paper, the class of doubly-transitive Frobenius groups is in one-to-one correspondence with the finite near-fields. Indeed, if $(K, +, \circ)$ is a near-field, then the multiplicative group of nonzero elements acts by right multiplication as a group of automorphisms of the additive group K, and the resulting semidirect product is a doubly-transitive Frobenius group. Conversely, suppose HK is a doubly-transitive Frobenius group with kernel K and complement H. If $e \in K$ is any nonidentity element of K then $\{e^x = x^{-1}ex | x \in H\}$ is the set of all nonidentity elements of K. Let $+$ denote the group operation within K and 0 the identity element of K. If $\circ$ is defined on K by setting $e^x \circ e^y = e^{xy}$, as well as $0 \circ 0 = 0 \circ e^x = e^x \circ 0 = 0$ for all $x, y \in H$, then $(K, +, \circ)$ is a near-field. (The conjugation action of H on K implies the right distributive law, and the other axioms of a near-field are easy to check.) The correspondence given above allows for the degenerate Frobenius group ($|H| = 1, |K| = 2$) which corresponds to the field GF(2).

The finite near-fields have all been classified by Zassenhaus [**8**], and one possible source for this is [**5**, see especially pp. 182–183].

For convenience we state below the main result on doubly-transitive Frobenius groups (or near-fields) that is needed in this paper. Recall that a group H is *metacyclic* if there exists a normal subgroup L such that both H/L and L are cyclic.

THEOREM 3.1. *Let HK be a doubly-transitive Frobenius group with kernel K and complement H. Then either H is metacyclic, or else $|K| = p^2$ for some prime p and one of the following cases occurs*:

$$\begin{aligned} p &= 5, & H &\simeq \mathrm{SL}(2,3), \\ p &= 7, & H &\simeq \widetilde{\mathrm{GL}}(2,3), \\ p &= 11, & H &\simeq \mathrm{SL}(2,5), \\ p &= 23, & H &\simeq \widetilde{\mathrm{GL}}(2,3) \times C_{11}, \\ p &= 29, & H &\simeq \mathrm{SL}(2,5) \times C_7, \\ p &= 59, & H &\simeq \mathrm{SL}(2,5) \times C_{29}. \end{aligned}$$

We have used the notation $\widetilde{\mathrm{GL}}(2,3)$ to denote a nonsplit cyclic extension of SL(2, 3) by an element of order 4 which acts as an outer automorphism of order 2 on SL(2, 3) and which squares to $-I \in \mathrm{SL}(2,3)$. In the case of $p = 11$ there are actually two inequivalent nontrivial actions of SL(2, 5) on an elementary abelian group of order 121, and this gives rise to two nonisomorphic near-fields of this order.

It is useful to record some information in the metacyclic case which will be used in the next section.

THEOREM 3.2. *Let HK be a doubly-transitive Frobenius group with kernel K and complement H, and let $|K|$ be a power of the prime p. Assume H is metacyclic. Then $|Z(H)| = q - 1$ where q is a power of p and $|H| = q^v$ where v is an integer such that every prime divisor of v divides $q - 1$. Moreover, if $q \equiv 3 \bmod 4$ then 4 does not divide v. If $q \not\equiv 3 \bmod 4$ or $q \equiv 3 \bmod 4$ and v is odd, then a Sylow 2-subgroup of H is cyclic. If $q \equiv 3 \bmod 4$ and v is even, then a Sylow 2-subgroup is generalized quaternion.*

The proof of this result is easily verified following the near-field construction given beginning on p. 182 of [**5**].

4. The solvable case. We saw in §2 that if a group G has an irreducible character that vanishes on all but 2 conjugacy classes, then G contains a unique minimal normal subgroup N which is contained in $O_p(G)$ for some prime p. Clearly, $O_p(G)$ must centralize N as N is minimal normal in G. Moreover, the results of §2 show $\mathbf{C}_G(x)$ is a p-group for $x \in N^\sharp$, and hence $\mathbf{C}_G(N)$ is a normal p-subgroup of G. Therefore, $O_p(G) = \mathbf{C}_G(N)$. In this section, the structure of $G/O_p(G)$ is determined when G is solvable.

LEMMA 4.1. *Let H be a solvable group acting on a vector space V over a field of characteristic p such that H is transitive and faithful on $V^\sharp$ and $\mathbf{C}_H(v)$ is a p-group for every $v \in V^\sharp$. Then H has a normal p-complement which is isomorphic to a Frobenius complement of a doubly-transitive Frobenius group, and a Sylow p-subgroup of H is abelian.*

Proof. Since H is solvable, it contains a p-complement, say H_1. The semidirect product H_1V is a doubly-transitive Frobenius group and it remains to prove $H_1 \trianglelefteq H$ and H/H_1 is abelian.

Let $F = F(H)$, the Fitting subgroup of H. Since H is faithful and irreducible on V, $O_p(H) = 1$ and hence F has order relatively prime to p. The hypotheses imply that F acts Frobeniusly on V, and hence F is cyclic, or a direct product of a characteristic generalized quaternion group Q of order ≥ 8 and a characteristic cyclic subgroup C. If F is cyclic, then H/F is abelian, and the result follows. Otherwise, $F = Q \times C$ and $H/Z(F)$ is isomorphic to a subgroup of $\mathrm{Aut}(Q) \times \mathrm{Aut}(C)$. Notice that $p \neq 2$ in this case. If $p > 3$ or if $|Q| > 8$ then both $\mathrm{Aut}(Q)$ and $\mathrm{Aut}(C)$ have normal p-complements and abelian Sylow p-subgroups, and the result follows.

Suppose then $p = 3$ and $|Q| = 8$. Then $\mathrm{Aut}(Q) \times \mathrm{Aut}(C)$ has a subgroup of index 2 which has a normal 3-complement and abelian Sylow

3-subgroups. Let $L = O_{3'}(H)$. Clearly, $L \leq H_1$ and $|H_1 : L| \leq 2$. It remains only to prove $L = H_1$.

Since $p = 3$, the Frobenius complement H_1 is not one of the exceptional possibilities listed in Theorem 3.1. Hence H_1 is metacyclic. Let q and v be the parameters given by Theorem 3.2 for H_1. As the Sylow 2-subgroups of H_1 are not cyclic, we necessarily have $q \equiv 3 \bmod 4$ and v is twice an odd number. But q is a power of $p = 3$, so q must be an odd power of 3 and $q \equiv 3 \bmod 8$. Thus $q^{v/2} \equiv 3 \bmod 8$, and hence $|H_1| = q^v - 1 = (q^{v/2} - 1)(q^{v/2} - 1) \equiv 8 \bmod 16$. Therefore, the 2-part of the order of H_1 is 8, and as $Q \leq L \leq H_1$, Q must be a Sylow 2-subgroup of H_1. Thus $|H_1 : L|$ is odd, and since $|H_1 : L| \leq 2$ we have $L = H_1$, as desired. □

THEOREM 4.2. *Assume G is a solvable group which has an irreducible character that vanishes on all but 2 conjugacy classes of G. Then there exists a unique prime p for which $O_p(G) \neq 1$. Moreover, $G/O_p(G)$ has a normal p-complement which is isomorphic to the multiplicative group of a near-field, and a Sylow p-subgroup of $G/O_p(G)$ is abelian.*

Proof. By Lemma 2.1, G has a unique minimal normal subgroup N which is an elementary abelian p-group for some prime p. Hence $N \subseteq O_p(G)$ and the uniqueness of N implies p is unique. Moreover, G is transitive on $N^\#$, and by Corollary 2.3, $\mathbf{C}_G(x)$ is a p-subgroup of G for every $x \in N^\#$.

As the kernel of the action of G on N is $O_p(G)$, the hypotheses of Lemma 4.1 are satisfied with $H = G/O_p(G)$ and $V = N$, and we are finished. □

Lemma 4.1 has another immediate application which is not related to the theme of this paper, but which is interesting in its own right.

COROLLARY 4.3. *Let $(K, +, \circ)$ be a finite near-field of characteristic p, and let $G = \mathrm{Gal}(K, +, \circ)$ (the full group of automorphisms of $(K, +, \circ)$). Then a Sylow p-subgroup of G is abelian.*

Proof. Let $P \in \mathrm{Syl}_p(G)$ and let H be the multiplicative group of nonzero elements of K. The natural semidirect product PH may be formed and since P is faithful on H we have $O_p(PH) = 1$. Moreover, P and H separately act on the vector space $V = K$, and these actions are compatible with the action of P on H. Hence PH acts on V and if H is solvable, Lemma 4.1 applies, and P is abelian. If H is not solvable, then K

is an exceptional near-field and $|K| = 11^2$, 29^2 or 59^2. In each case, H does not have an automorphism of order p and so $P = 1$. □

Notice that even though Lemma 4.1 was used to prove Corollary 4.3, the Galois group of a near-field of characteristic p need not have a normal p-complement. For example, if $(K, +, \circ)$ is the unique near-field of order 9 which is not a field, then $\mathrm{Gal}(K, +, \circ)$ is S_3 and so does not have a normal 3-complement.

5. The nonsolvable case. The goal for this section is to obtain the analogue of Theorem 4.2 in the nonsolvable case. The result is Theorem 5.6 below.

It is convenient to begin with some representation theory in characteristic p. If φ is a Brauer character of a group G corresponding to a representation over a field of characteristic p, define $\varphi^{(j)}$ to be the function defined on the p-regular elements of G by setting $\varphi^{(j)}(x) = \varphi(x^{p^j})$. Thus $\varphi^{(0)} = \varphi$, and for all j, $\varphi^{(j)}$ is a Brauer character of G. Moreover, if φ is irreducible, so is $\varphi^{(j)}$ for every j.

THEOREM 5.1. *Let $G = \mathrm{SL}(2, p^a)$ where p is a prime and set $F = \mathrm{GF}(p^a)$. Then G acts naturally on the F-algebra of polynomials in* 2 *variables. Let V_i be the submodule of homogeneous polynomials of degree i, and φ_i the Brauer character afforded by V_i. Then the p^a Brauer characters $\varphi_{i_0}^{(0)}\varphi_{i_1}^{(1)}\cdots\varphi_{i_{a-1}}^{(a-1)}$ for $0 \le i_j \le p-1$ are all distinct, irreducible, and every irreducible Brauer character of G has this form.*

A proof of Theorem 5.1 may be found in [**2**, §30, pp. 588–589].

Let $V = V_1$ (the natural module of $\mathrm{SL}(2, p^a)$). The algebraic conjugates $V^{(j)}$, $0 \le j \le a-1$, are all isomorphic as $\mathrm{GF}(p)[\mathrm{SL}(2, p^a)]$-modules, and any one of these will be referred to as the standard module for $\mathrm{SL}(2, p^a)$. Clearly, the standard module has the property that every element of order p in $\mathrm{SL}(2, p^a)$ has a quadratic minimal polynomial. By examining the complete list of absolutely irreducible modules of $\mathrm{SL}(2, p^a)$ (given by Theorem 5.1) the following converse is easy to check.

COROLLARY 5.2. *Assume p is an odd prime. Let W be an irreducible $\mathrm{GF}(p)[\mathrm{SL}(2, p^a)]$-module in which every element of order p has a quadratic minimal polynomial. Then W is the standard module for* $\mathrm{SL}(2, p^a)$.

The analogue for $p = 2$ of the above corollary is

COROLLARY 5.3. *Assume* $p = 2$ *and* W *is an irreducible* $\mathrm{GF}(2)[\mathrm{SL}(2, 2^a)]$*-module for which* $[W, P] \neq 0$ *and* $[W, P, P] = 0$, *where* P *is a Sylow* 2*-subgroup of* $\mathrm{SL}(2, 2^a)$. *Then* W *is the standard module for* $\mathrm{SL}(2, 2^a)$.

THEOREM 5.4. *Let* p *be an odd prime and assume* H *is a nonsolvable group which acts faithfully on a vector space* V *over a field of characteristic* p. *Assume* H *is transitive on* $V^{\sharp}$ *and* $\mathbf{C}_H(v)$ *is a* p*-group for all* $v \in V^{\sharp}$. *Then one of the following cases holds.*

(i) *There exists* $S \trianglelefteq H$ *with* $S \simeq \mathrm{SL}(2, q)$ *where* q *is a power of* p *and* $\mathbf{C}_H(S) = \mathbf{Z}(S)$. *Moreover,* V *is the standard module for* S, *and* H/S *is a cyclic* p*-group.*

(ii) $p = 3$, $|V| = 3^4$ *and* H *contains a normal subgroup* S *of index* 2 *with* $S \simeq \mathrm{SL}(2, 5)$ *and* $\mathbf{C}_H(S) = \mathbf{Z}(S)$. S *is not split in* H.

(iii) $p = 3, |V| = 3^6$ *and* $H \simeq \mathrm{SL}(2, 13)$.

(iv) $p = 11, |V| = 11^2$ *and* $H \simeq \mathrm{SL}(2, 5)$.

(v) $p = 29, |V| = 29^2$ *and* $H \simeq \mathrm{SL}(2, 5) \times C_7$.

(vi) $p = 59, |V| = 59^2$ *and* $H \simeq \mathrm{SL}(2, 5) \times C_{29}$.

Proof. Let $S = H^{(\infty)}$ be the last term of the derived series of H. By hypothesis, $S > 1$. Define $L = O_{2'}(S)$. By hypothesis, any involution of H must invert V, and hence H has a unique involution, say z. The Sylow 2-subgroups of H and S are necessarily generalized quaternion and so $S/\langle z \rangle L$ has dihedral Sylow 2-subgroups (allowing $C_2 \times C_2$ as a dihedral group). From the classification of groups with dihedral Sylow 2-subgroups ([**4**], or more recently [**1**]) $S/\langle z \rangle L \simeq \mathrm{PSL}(2, r)$ or A_7, where r is an odd prime power. Now S/L is a nontrivial double cover of the perfect group $S/\langle z \rangle L$ and so is a homomorphic image of the unique covering group of $S/\langle z \rangle L$. Hence, $S/L \simeq \mathrm{SL}(2, r)$ or $\hat{A}_7$, where $\hat{A}_7$ is the unique nontrivial double cover of A_7. We shall now prove that $L = 1$.

Let $M = O_{p'}(L)$. As M is a group of odd order acting Frobeniusly on V, M is necessarily a $\mathbf{Z}$-group. Hence, $H/\mathbf{C}_H(M)$ is solvable and this implies $M \leq \mathbf{Z}(S)$. Now H is irreducible on V as it is transitive on $V^{\sharp}$, and since H is faithful on V we have $O_p(H) = 1$. Hence $O_p(L) = 1$. As L is solvable and $M = O_{p'}(L)$ is central in L we must have $M = L$. Now $L \leq \mathbf{Z}(S) \cap S'$ so L is isomorphic to a subgroup of the Schur multiplier of S/L. If $L \neq 1$ then $|L| = 3$ and S/L is either $\mathrm{SL}(2, 9)$ or $\hat{A}_7$. In either of these cases, a Sylow 3-subgroup of S is noncyclic. As every p'-subgroup of H acts Frobeniusly on V we must have $p = 3$. But then $L \leq O_3(H) = 1$, a contradiction.

Hence $L = 1$ and $S \simeq \mathrm{SL}(2, r)$ or $\hat{A}_7$. We now show S is not isomorphic to $\hat{A}_7$.

Suppose $S \simeq \hat{A}_7$. Recall S acts on V in such a way that the subgroups of p' order act Frobeniusly. Since a Sylow 3-subgroup of $\hat{A}_7$ is not cyclic, this means $p = 3$. Let θ be any irreducible constituent of the Brauer character of S afforded by V. Then 1 does not appear as an eigenvalue under the action of any $3'$-element of S in the representation affording θ. This condition on θ remains valid for $\theta|_X$ for all subgroups X of S. A contradiction will be reached by showing $\hat{A}_7$ has no irreducible Brauer character satisfying the requirements of θ.

Notice that $\hat{A}_6 \simeq \mathrm{SL}(2, 9)$ embeds as a subgroup of $\hat{A}_7$. Using the notation of Theorem 5.1, the irreducible Brauer characters of $\mathrm{SL}(2, 9)$ for $p = 3$ are $\varphi_i^{(0)}\varphi_j^{(1)}$, $0 \leq i, j \leq 2$. The only irreducible Brauer characters of $\mathrm{SL}(2, 9)$ satisfying the same condition as θ are $\varphi_1^{(0)}$ and $\varphi_1^{(1)}$. For ease of notation, denote these two characters by φ and $\tilde{\varphi}$. Hence, $\theta|_{\hat{A}_6}$ is an integral combination of φ and $\tilde{\varphi}$. By standard properties of characters (the Nakayama relations), θ must be a constituent of either $\varphi^{\hat{A}_7}$ or $\tilde{\varphi}^{\hat{A}_7}$. Now

$$\varphi^{\hat{A}_7}|_{\hat{A}_6} = 2\varphi + 2\tilde{\varphi} + \varphi\varphi_2^{(1)}$$

and

$$\tilde{\varphi}^{\hat{A}_7}|_{\hat{A}_6} = 2\varphi + 2\tilde{\varphi} + \tilde{\varphi}\varphi_2^{(0)}.$$

This implies $\theta|_{\hat{A}_6}$ is a subcharacter of $2\varphi + 2\tilde{\varphi}$, and in particular, $\theta(1) \leq 8$ and $\theta(1)$ is even.

Let X be the Frobenius group of order 21. Then X embeds as a subgroup of $\hat{A}_7$. Moreover, X has exactly 3 irreducible Brauer characters for $p = 3$, namely the principal Brauer character, and two others of degree 3. As $\theta|_X$ cannot contain the principal character, we have $3|\theta(1)$. Combining this with the above, we have $\theta(1) = 6$.

Now let X be a Sylow 5-normalizer in $\hat{A}_7$. Then X contains the central involution z, and $X/\langle z \rangle$ is the Frobenius group of order 20. As $3 \nmid |X|$, $\theta|_X$ is an ordinary character of X. The eigenvalue condition on θ implies that $\theta|_X$ is a multiple of the unique faithful character of X and so $4|\theta(1) = 6$. This contradiction eliminates $\hat{A}_7$ and shows $S \simeq \mathrm{SL}(2, r)$, where r is an odd prime power.

Case 1. $p \nmid |\mathrm{SL}(2, r)|$.

By definition of S, H/S is solvable and so has a p-complement H_1/S. Then H_1 is a p-complement in H. Moreover, H_1 is transitive on $V^\#$ and so H_1V is a doubly transitive Frobenius group. Theorem 3.1 implies, since H_1 is nonsolvable, that one of the following three possibilities holds:

$$\begin{aligned} |V| &= 11^2, & H_1 &\simeq \mathrm{SL}(2,5), \\ |V| &= 29^2, & H_1 &\simeq \mathrm{SL}(2,5) \times C_7, \\ |V| &= 59^2, & H_1 &\simeq \mathrm{SL}(2,5) \times C_{29}. \end{aligned}$$

Thus, $S \simeq \mathrm{SL}(2,5)$ in this case, and since S has no automorphism of order p, $H = S\mathbf{C}_H(S)$. The group $\mathbf{C}_H(S)$ is necessarily p-closed and as $O_p(H) = 1$ we have $H = H_1$. Thus, Case 1 leads to one of the last three possibilities of Theorem 5.4.

Case 2. $p \mid |\mathrm{SL}(2, r)|$ but $p \nmid r$.

Since $p \mid (r^3 - r)$ we have $p \mid (r + \varepsilon)$ for $\varepsilon = 1$ or -1. Let p^a be the full power of p dividing $r + \varepsilon$, and let l be the p'-part of the index $|H : S|$. Since the normalizer in S of a Sylow p-subgroup, say P, has order $2(r + \varepsilon)$, Lemma 2.4(b) and the Frattini argument imply

$$2(r + \varepsilon)l/p^a = p^\alpha - 1,$$

where $p^\alpha = |\mathbf{C}_V(P)|$. By Lemma 2.4(a), $|V|$ is a power of p^α, say $p^{\alpha\beta}$, and hence

$$(r - \varepsilon)r\frac{r + \varepsilon}{p^a}l = p^{\alpha\beta} - 1$$

follows by the hypotheses of Theorem 5.4. Dividing this by the first equation yields

$$r^2 - \varepsilon r = 2\sigma \quad \text{where } \sigma = (p^\alpha)^{\beta - 1} + \cdots + p^\alpha + 1.$$

Hence,

$$r = \tfrac{1}{2}\left(\sqrt{8\sigma + 1} + \varepsilon\right) \quad \text{and} \quad r + \varepsilon = \tfrac{1}{2}\left(\sqrt{8\sigma + 1} + 3\varepsilon\right).$$

Now p^a divides $r + \varepsilon$ so p^a divides $(\sqrt{8\sigma + 1} - 3\varepsilon)(\sqrt{8\sigma + 1} + 3\varepsilon) = 8(\sigma - 1)$ so $a \leq \alpha$.

Suppose $\beta \geq 5$. Then

$$r = \tfrac{1}{2}\left(\sqrt{8\sigma + 1} + \varepsilon\right) \geq \tfrac{1}{2}2p^{2\alpha} = p^{2\alpha}$$

and hence, as $p \nmid r$, $r + \varepsilon \geq p^{2\alpha}$. Therefore,

$$p^{\alpha} - 1 = 2(r + \varepsilon)l/p^{a} \geq 2p^{2\alpha}l/p^{a} > p^{\alpha},$$

as $\alpha \geq a$. This is a contradiction, so we must have $\beta \leq 4$.

Subcase $\varepsilon = -1$. As all p'-subgroups of H act Frobeniusly on V, r must be a prime. Moreover, in the subcase we are in ($\varepsilon = -1$), the Sylow p-subgroup P of S normalizes some Sylow r-subgroup of S, say R, and PR is a Frobenius group. Since PR acts on V with $\mathbf{C}_V(R) = \{0\}$, P must act semiregularly on a basis for V. Hence

$$\dim V = p^{a} \dim \mathbf{C}_V(P) = p^{a}\alpha.$$

Hence, $\beta = p^{a}$ and, since p is odd and $\beta \leq 4$, we must have $\beta = 3$, $p = 3$ and $a = 1$. If $l > 1$ then

$$p^{\alpha} - 1 = 2(r - 1)l/3 > (r - 1)$$

and, hence, $r < p^{\alpha}$ so $r + 1 \leq p^{\alpha}$. Then

$$\begin{aligned} p^{3\alpha} - 1 &= (r + 1)r\frac{(r - 1)l}{3} = \frac{(r + 1)r}{2} \cdot \frac{2(r - 1)l}{3} \\ &< \tfrac{1}{2}p^{\alpha}p^{\alpha} \cdot (p^{\alpha} - 1) < \tfrac{1}{2}p^{3\alpha}. \end{aligned}$$

This forces the contradiction $p^{3\alpha} < 2$ and so in fact l must be 1. We now have

$$2(r - 1)/3 = 3^{\alpha} - 1 \quad \text{and} \quad r^2 + r = 2(3^{2\alpha} + 3^{\alpha} + 1).$$

Solving for r and 3^{α} we have $r = 13$ and $3^{\alpha} = 9$. Hence, $S \simeq \mathrm{SL}(2, 13)$ and $|V| = p^{\alpha\beta} = 3^6$. Also, H/S is a 3-group (as $l = 1$). Since all automorphisms of S of order 3 are inner, and $O_3(H) = 1$, we have $H = S$. Hence, this subcase leads to possibility (iii) of Theorem 5.4.

Subcase $\varepsilon = +1$. In this case, r is still a prime. If $r - 1$ is divisible by an odd prime, say t, then S contains a Frobenius subgroup of order tr. This is impossible as the p'-elements of S act fixed point freely on V. Thus, $r - 1$ is a power of 2 and r is a Fermat prime.

We also have $(r - 1)/2 \cdot r = (p^{\alpha})^{\beta - 1} + \cdots + p^{\alpha} + 1$, where $2 \leq \beta \leq 4$.

If $\beta = 4$ then

$$(r - 1)/2 \cdot r = (p^{\alpha} + 1)(p^{2\alpha} + 1).$$

As $p^{2\alpha} + 1 \equiv 2 \bmod 4$, and r is the unique odd prime factor on the left side of the equation, we must have

$$r = \frac{p^{2\alpha} + 1}{2} \quad \text{and} \quad \frac{r-1}{2} = 2(p^{\alpha} + 1).$$

Solving for r and p^{α} we have $r = 41$ and $p^{\alpha} = 9$. Hence $p = 3$ and $a = 1$. However $2(r+1)/p^{a} = p^{\alpha} - 1$ implies the contradiction $28l = 8$.

If $\beta = 3$ then $(r-1)/2 \cdot r = p^{2\alpha} + p^{\alpha} + 1$. As the right side is odd, this implies $(r-1)/2 = 1$ and $p^{\alpha} = 1$, a contradiction.

This leads to $\beta = 2$ and $(r-1)r/2 = p^{\alpha} + 1$. Now $2(r+1)l/p^{a} = p^{\alpha} - 1$ implies $p^{\alpha} \equiv 1 \bmod 4$ so $(r-1)r/2 = p^{\alpha} + 1 \equiv 2 \bmod 4$. Hence $(r-1)/2 = 2$ and this leads to $r = 5$, $p = 3$, $\alpha = 2$, $a = 1$, $l = 2$ and $\beta = 2$. Thus $|V| = p^{\alpha\beta} = 3^4$ and $S \simeq \mathrm{SL}(2,5)$ has index in H equal to twice a power of 3. As in the other subcase, all automorphisms of S of order 3 are inner, and as $O_3(H) = 1$ we have $|H : S| = 2$. A Sylow 2-subgroup of H must be generalized quaternion and so S is not split in H. This is possibility (ii) of Theorem 5.4.

Case 3. $S \simeq \mathrm{SL}(2, r)$ where r is a power of p.

Let P be a Sylow p-subgroup of S and let l be the p'-part of $|H : S|$. By (a) and (b) of Lemma 2.4 again, we have

$$(r-1)l = q - 1 \quad \text{and} \quad (r+1)(r-1)l = q^{\beta} - 1,$$

where $q = |\mathbf{C}_V(P)|$ and $|V| = q^{\beta}$. Thus $r + 1 = q^{\beta-1} + q^{\beta-2} + \cdots + q + 1$. Now r and q are powers of the same prime p, and so by uniqueness of representation in base p we have $\beta = 2$ and $r = q$. This also implies $l = 1$ and so H/S is a p-group. As $O_p(H) = 1$, we have $\mathbf{C}_H(S) = \mathbf{Z}(S)$. The outer automorphism group of S is well known so H/S is cyclic. It remains to prove V is the standard module for S.

By Lemma 2.4(c) we have $|V/[V, P]| = |\mathbf{C}_V(P)| = q$ and as $\beta = 2$ we must have $[V, P] = \mathbf{C}_V(P)$. Hence, every element of order p in S has a quadratic minimal polynomial in its action on V and Corollary 5.2 implies V is the standard module for S.

This completes the entire proof of Theorem 5.4. □

It is possible to show that each of the exceptional cases mentioned in Theorem 5.4 actually occurs. This is certainly true for the possibilities (iv)–(vi) since these cases correspond to near-fields. If $H = \mathrm{SL}(2, 13)$ then H has an ordinary complex character of degree 6 which remains irreducible mod 3 (since the defect is zero). Moreover, all character values lie in

GF(3) so that, as Schur indices are trivial in characteristic p, H acts on a vector space V of size 3^6. The character of this representation shows that the elements of order prime to 3 act fixed point freely, and hence, $\mathbf{C}_H(v)$ is a 3-group for all $v \in V^\sharp$. The transitivity of H easily follows from this.

If H is the nonsplit extension of $S = \mathrm{SL}(2,5)$ by a cyclic group of order 2 then either of the two faithful characters of degree 2 of S induces to an irreducible character of degree 4 of H, which is irreducible mod 3. Again, all character values lie in GF(3) so H acts on a vector space V of order 3^4. No element of order prime to 3 fixes any vector in $V^\sharp$ and this easily implies the transitivity of H on $V^\sharp$.

THEOREM 5.5. *Assume the hypotheses of Theorem* 5.4 *except that in this case assume* $p = 2$. *Then there exists* $S \trianglelefteq H$ *with* $S \simeq \mathrm{SL}(2, q)$ *where* q *is a power of* 2 *and* $q > 2$. *Moreover,* H/S *is a cyclic* 2-*group,* $\mathbf{C}_H(S) = 1$, *and* V *is the standard module for* S.

Proof. As in the odd prime case, let $S = H^{(\infty)}$ be the last term in the derived series of H, and let L be a minimal normal subgroup of H contained in S. As H is nonsolvable, $S > 1$ so that L exists. Every subgroup of H of odd order acts Frobeniusly on V and hence is metacyclic. If $|L|$ is odd, then $H/\mathbf{C}_H(L)$ is solvable so $L \le \mathbf{Z}(S) \cap S'$. However, all Sylow l-subgroups of S/L are cyclic for all odd primes l, so the Schur multiplier of S/L is a 2-group. This implies the contradiction $L = 1$, and hence $|L|$ must be even. As $O_2(H) = 1$, L cannot be a 2-group and hence L is a direct product of isomorphic nonabelian simple groups. As the Sylow l-subgroups of L are cyclic for odd primes l, we must have that L is in fact simple.

The simple groups having cyclic Sylow subgroups for all odd primes are $\mathrm{SL}(2, 2^n)$ $(n \ge 2)$, $\mathrm{Sz}(2^{2n+1})$ $(n \ge 1)$ and $Ja = J_{11}$. The group J_{11} is quickly eliminated as J_{11} contains a nonabelian subgroup of order 21 which then cannot act fixed point freely on V.

Suppose $L \simeq \mathrm{Sz}(q)$ where $q = 2^{2n+1}$. Let $P \in \mathrm{Syl}_2(L)$ so $|\mathbf{N}_L(P)| = (q-1)q^2$. By Lemma 2.4(a) and (b) we have

$$(q-1)l = 2^\alpha - 1 \quad \text{and} \quad (q^2+1)(q-1)l = 2^{\alpha\beta} - 1,$$

where $2^\alpha = |\mathbf{C}_V(P)|$, $|V| = (2^\alpha)^\beta$, and l is the odd part of $|H : L|$.

Dividing the second equation by the first yields

$$q^2 + 1 = (2^\alpha)^{\beta-1} + \cdots + 2^\alpha + 1.$$

By uniqueness of representation in base 2 we have $\beta = 2$ and $q^2 = 2^\alpha$. Hence $l = q + 1$, $|\mathbf{C}_V(P)| = q^2$ and $|V| = q^4$.

By Lemma 2.4(c), $V > [V, P] = \mathbf{C}_V(P) > \{0\}$ is an $\mathbf{N}(P)$-composition series for V, and hence $[V, P, P]$ is trivial. This implies P' centralizes V, which is a contradiction as a Sylow 2-subgroup of $\mathrm{Sz}(q)$ is nonabelian.

This leads to $L \simeq \mathrm{SL}(2, q)$ where q is a power of 2 and $q \geq 4$. Again with $P \in \mathrm{Syl}_2(L)$ and l equal to the odd part of $|H : L|$:

$$(q-1)l = 2^\alpha - 1 \quad \text{and} \quad (q+1)(q-1)l = (2^\alpha)^\beta - 1,$$

where $2^\alpha = |\mathbf{C}_V(P)|$ and $2^{\alpha\beta} = |V|$. This leads to $\beta = 2$, $q = 2^\alpha$ and $l = 1$. Also $[V, P] = \mathbf{C}_V(P)$ so Corollary 5.3 applies, and V is the standard module for L. As $l = 1$ we have $L = S$ and H/S is a power of 2. Also, $O_2(H) = 1$ so $\mathbf{C}_H(S) = 1$. As in the odd prime case, H/S is cyclic and the proof of Theorem 5.5 is complete. □

An immediate consequence of the last two theorems together with the results of §2 is the following extension of Theorem 4.2 to the nonsolvable case.

THEOREM 5.6. *Let G be a nonsolvable group which has an irreducible character which vanishes on all but two conjugacy classes of G. Then $O_p(G) \neq 1$ for some unique prime p. Moreover, the group $H = G/O_p(G)$ has one of the following forms*:

(i) *There exists $S \trianglelefteq H$ with $S \simeq \mathrm{SL}(2, q)$ where $q > 2$ is a power of p, H/S is a cyclic p-group and $\mathbf{C}_H(S) = Z(S)$.*

(ii) *$p = 3$, H contains a normal subgroup S of index 2 with $S \simeq \mathrm{SL}(2,5)$ and $\mathbf{C}_H(S) = Z(S)$. S is not split in H.*

(iii) *$p = 3$ and $H \simeq \mathrm{SL}(2, 13)$.*

(iv) *$p = 11$ and $H \simeq \mathrm{SL}(2, 5)$.*

(v) *$p = 29$ and $H \simeq \mathrm{SL}(2, 5) \times C_7$.*

(vi) *$p = 59$ and $H \simeq \mathrm{SL}(2, 5) \times C_{29}$.*

6. The subgroup $O_p(G)$. Under the hypothesis of Theorems 4.2 or 5.6, the group $G/O_p(G)$ was characterized. In this section some attention will be paid to $O_p(G)$. The group $O_p(G)$ need not be a Sylow p-subgroup of G, however, the remarks following Lemma 2.4 show that a "small" homomorphic image of a Sylow p-normalizer always satisfies the same hypothesis as G. In this subgroup, of course, a Sylow p-subgroup is normal.

In this special case (that $O_p(G)$ is a Sylow p-subgroup of G) the structure of $O_p(G)$ can be quite complicated. Theorem 6.3 below shows that no bound can be placed on the derived length, or nilpotence class of $O_p(G)$. The proof of this result generalizes a construction given in [**3**].

On the positive side, Theorem 6.2 completely characterizes G when $O_p(G)$ is minimal normal in G.

LEMMA 6.1. *Let C be a cyclic p-group acting on a vector space V over a field of characteristic p. Let r be a power of p such that $|V| \geq r^{|C|}$. Then $|\mathbf{C}_V(C)| \geq r$.*

Proof. We may assume that the underlying field is $\mathrm{GF}(p)$. Each indecomposable summand of V has size at most $p^{|C|}$, or equivalently, the size of any Jordan block in the Jordan decomposition for a generator of C is at most $|C| \times |C|$. Hence, there are at least $\log_p r$ indecomposable summands. As there is a one-dimensional subspace of vectors centralized by C in each such summand, we have $|\mathbf{C}_V(C)| \geq p^{\log_p r} = r$. □

THEOREM 6.2. *Suppose G has an irreducible character which vanishes on all but 2 conjugacy classes of G, and let N denote the unique minimal normal elementary abelian p-subgroup as guaranteed by Lemma 2.1. Then $N = O_p(G)$ if and only if G is a doubly transitive Frobenius group, or $|G| = 2$.*

Proof. If G is a doubly transitive Frobenius group, or $|G| = 2$ (which may be regarded as a degenerate Frobenius group) then the Frobenius kernel is N and the result $N = O_p(G)$ follows.

Assume now $N = O_p(G)$ and let $P \in \mathrm{Syl}_p(G)$. If N is complemented in G by a subgroup H say, then the group N is complemented in P by $P \cap H$. Now $[N, P \cap H] < N$, and any linear character λ with kernel containing $[N, P \cap H]$ is extendible to P. However, by Corollary 2.3, λ^P has a unique irreducible constituent, and this constituent vanishes on $P - N$. This implies that P must equal N. Thus, H has order prime to p and is transitive and regular on the nonidentity elements of N. If $H \neq 1$ then $G = NH$ is a doubly transitive Frobenius group, while if $H = 1$ then G is cyclic of order 2. Thus, the theorem is valid if N is complemented in G.

Assume first that G/N is solvable. By Theorem 4.2, G/N has a normal p-complement, say G_0/N, and N is complemented in G_0 by a subgroup, say H. The Frattini argument yields $G = N \cdot \mathbf{N}_G(H)$ and $N \cap \mathbf{N}_G(H)$ is centralized by H. Thus, for $H \neq 1$, $\mathbf{N}_N(H) = 1$ and N is complemented in G, which implies by the preceding paragraph that we are finished. If $H = 1$ then $|N| = 2$ and G is a 2-group. Hence $N = O_2(G) = G$ and so $|G| = 2$, completing the solvable case.

Suppose then that G/N is nonsolvable. If $p > 2$ then any involution u in G must invert N and hence $u\mathbf{C}_G(N)$ is the unique involution of $G/\mathbf{C}_G(N)$. Now $\mathbf{C}_G(N) = O_p(G) = N$, so uN is the unique involution of G/N. By the Frattini argument again, $G = N \cdot \mathbf{C}_G(u)$ and since u inverts

N, $N \cap \mathbf{C}_G(u) = \mathbf{C}_N(u) = 1$. N is complemented by $\mathbf{C}_G(u)$ and we are finished.

This leads to the case that G/N is nonsolvable, and $p = 2$. Using $N = O_2(G)$ and Theorem 5.6, G/N has a normal subgroup S/N isomorphic to $\mathrm{SL}(2, q)$ where q is a power of 2, and N is the standard module for S/N. In particular $|N/[N, P_0]| = |\mathbf{C}_N(P_0)| = q$ where $P_0 = P \cap S$ is a Sylow 2-subgroup of S.

Suppose first that $G = S$. Then $\mathbf{N}_G(P) = PH$ where $|H| = q - 1$ and H acts fixed point freely on the groups P/N, $N/[N, P]$ and $\mathbf{C}_N(P)$. Let $x \in P - N$. By Theorem 2.5(a) we have $q = |\mathbf{C}_{G/N}(x)| = |\mathbf{C}_G(x)|$. However, $\mathbf{C}_G(x) \supseteq \langle x, \mathbf{C}_N(P)\rangle$ and so has order $> q$. This contradiction shows that $G > S$.

Let $l = |G : S|$. By Theorem 5.6, l is a power of 2 so $G = SP$, and $\mathbf{C}_{G/N}(S/N) = \bar{1}$. Hence G/N is isomorphic to a subgroup of $\mathrm{Aut}(S/N)$ which contains $\mathrm{Inn}(S/N)$. In particular, P_0/N splits in P/N, say by C/N, and the action of C/N on P_0/N is that of a Galois group on a field. We may write $q = q_0^l$ and identify the action of C/N on P_0/N with that of $\mathrm{Gal}(\mathrm{GF}(q_0^l)/\mathrm{GF}(q_0))$ on $\mathrm{GF}(q_0^l)$. In particular, C/N acts semiregularly on a basis of P/N viewed as a vector space over GF(2), and $\mathbf{C}_{P/N}(C/N)$ has order q_0. It follows that the 2-part of the order of $\mathbf{C}_{G/N}(C/N)$ has order $q_0 l$. By Lemma 6.1 applied to the group C/N acting on N, where $|N| = q_0^{2l}$ and $r = q_0^2$, we have $|\mathbf{C}_N(C/N)| \geq q_0^2$ (in fact equality holds, but we won't need this). Let c be a generator for $C \bmod N$. Then $|\mathbf{C}_N(c)| \geq q_0^2$ and as $\mathbf{C}_C(c) \geq \langle c, \mathbf{C}_N(c)\rangle$, the order of $\mathbf{C}_G(c)$ is divisible by lq_0^2. However, we already saw that the 2-part of the order of $\mathbf{C}_{G/N}(cN)$ was $q_0 l$, and this contradicts Theorem 2.5(a). This completes the proof of Theorem 7.2. $\square$

THEOREM 6.3. *Let Q be any p-group and let $a > 0$ be any integer. Then a group G exists satisfying the following conditions*:

(a) *G has an irreducible character which vanishes on all but two conjugacy classes.*

(b) *$G = PH$ where $P \trianglelefteq G$ is a Sylow p-subgroup and H is cyclic of order $p^a - 1$.*

(c) *$\mathbf{Z}(P)H$ is a doubly transitive Frobenius group of order $p^a(p^a - 1)$.*

(d) *Q is isomorphic to a subgroup of $P/\mathbf{Z}(P)$.*

Proof. The result is clear if $Q = 1$. Let Q_0 be a maximal (and hence normal) subgroup of Q. By induction, assume a group of the form $P_0 H$ exists satisfying (a)–(d) above for Q_0. Let E be a group written additively which is H-isomorphic to $\mathbf{Z}(P_0)$ and set $\hat{E} = \hom_H(E, \mathbf{Z}(P_0))$. Since multiplicative notation is retained in $\mathbf{Z}(P_0)$ we have $(f+h)(e) = f(e)h(e)$ and $f(e_1 + e_2) = f(e_1)f(e_2)$ for $e, e_1, e_2 \in E$ and $f, h \in \hat{E}$. Let $P_0^{\hat{E}} = \{x | x\colon \hat{E} \to P_0\}$ so that $P_0^{\hat{E}}$ is a group under pointwise multiplication of functions, and $P_0^{\hat{E}}$ is isomorphic to a direct product of $|\hat{E}|$ copies of P_0. Let

$$W = \left\{ x \in P_0^{\hat{E}} | x(f) \in \mathbf{Z}(P_0) \text{ for every } f \in \hat{E} \text{ and } \prod_{f \in \hat{E}} x(f) = 1 \right\}$$

and set $U = P_0^{\hat{E}}/W \times E$.

If $x \in P_0^{\hat{E}}$, $e \in E$ and $f \in \hat{E}$ define $x_{e,f} \in P_0^{\hat{E}}$ by setting $x_{e,f}(h) = x(h-f)$ for $h \neq 0$, while $x_{e,f}(0) = f(e)x(-f)$. For $(xW, e) \in U$ and $f \in \hat{E}$ define

$$(xW, e)^f = (x_{e,f}W, e).$$

This is well defined since for x, $y \in P_0^{\hat{E}}$ and $w \in W$ with $x = yw$ we have $x_{e,f} = y_{e,f}\tilde{w}$ where $\tilde{w}(h) = w(h-f)$ for all $h \in \hat{E}$. Hence $\tilde{w} \in W$, and so $x_{e,f}$ and $y_{e,f}$ lie in the same coset of W. The requirement that $f \in \hom_H(E, \mathbf{Z}(P_0))$ implies that the function $u \mapsto u^f$ is an automorphism of U. Moreover, for $e \in E$ and $f, g \in \hat{E}$ we have $x_{e,f+g} \equiv (x_{e,f})_{e,g} \bmod W$, and hence the function $(u, f) \mapsto u^f$ is an action of $\hat{E}$ on U.

By the preceding paragraph, we have an action of $\hat{E}$ on $U = P_0^{\hat{E}}/W \times E$ by automorphisms. Let $P = \hat{E} \ltimes U$ denote the resulting semidirect product using the action. Notice that since H acts on P_0 (by conjugation), H acts naturally on $P_0^{\hat{E}}$ by automorphisms (via $(x^h)(f) = x(f)^h$ for $f \in \hat{E}$) and W is stabilized by H. Hence, we may define an action of H on P by setting

$$(f, (xW, e))^h = (f, (x^hW, e^h))$$

where we have used the action of H on E, but not the action of H on $\hat{E}$.

The equation

$$(x_{e,f})^h = (x^h)_{e^h,f}$$

for $x \in P_0^{\hat{E}}$, $e \in E$, $f \in \hat{E}$ and $h \in H$, is readily verified, and this implies that the action of H on P is an action by automorphisms. Let G denote the semidirect product $H \ltimes P$ with respect to this action. It remains to check that G satisfies (a) — (d) of Theorem 6.3.

Let λ be any nonprincipal irreducible character of $\mathbf{Z}(P_0)$ and let ζ be the unique irreducible constituent of λ^{P_0} (thus, ζ^{P_0H} is the character of P_0H

which vanishes on all but 2 conjugacy classes of $P_0 H$). The character $\eta = \zeta \# \zeta \# \cdots \# \zeta$ is an irreducible character of $P_0^{\hat{E}}$ with kernel containing W, and hence we may regard η as a character of $P_0^{\hat{E}}/W$. Let $\tilde{\eta} = \eta \# 1_E$ so that η is an extension of η to $U = P_0^{\hat{E}}/W \times E$. To prove that $\theta = \tilde{\eta}^P$ is irreducible, it is enough to verify that $\mathcal{I}_{\hat{E}}(\tilde{\eta}) = \{0\}$.

Let $f \in I_{\hat{E}}(\tilde{\eta})$. Then $\tilde{\eta}^{-f}(xW, e) = \tilde{\eta}(xW, e)$ for all $(xW, e) \in U$, and so $\tilde{\eta}(x_{e,f}W, e) = \tilde{\eta}(xW, e)$ or $\eta(x_{e,f}W) = \eta(xW)$. Dropping the W and then restricting the equation to the subgroup $\mathbf{Z}(P_0)^{\hat{E}}$ of $P_0^{\hat{E}}$ yields

$$\zeta(1)^{|\hat{E}|}\tilde{\lambda}(x_{e,f}) = \zeta(1)^{|\hat{E}|}\tilde{\lambda}(x)$$

for all $e \in E$ and $x \in \mathbf{Z}(P_0)^{\hat{E}}$, where $\tilde{\lambda} = \lambda \# \lambda \# \cdots \# \lambda$ ($\tilde{\lambda}$ is the unique irreducible constituent of $\eta|_{\mathbf{Z}(P_0)^{\hat{E}}}$). Now let $x\colon \hat{E} \to \mathbf{Z}(P_0)$ be the trivial map. Then dropping the factor of $\zeta(1)^{|\hat{E}|}$ we have

$$\tilde{\lambda}(x_{e,f}) = 1 \quad \text{for all } e \in E.$$

But $x_{e,f}(h) = 1$ for $h \neq 0$ and $x_{e,f}(0) = f(e)$, so the equation above implies

$$\lambda(f(e)) = 1 \quad \text{for all } e \in E.$$

Thus $f(E) \leq \ker \lambda$. Now, if $f \neq 0$ then f is surjective so $f(E) = \mathbf{Z}(P_0) \leq$ | $\ker \lambda$. Thus, f is necessarily 0 and this proves that $\mathcal{I}_{\hat{E}}(\tilde{\eta}) = \{0\}$.

As $|\hat{E}| = |E|$ (an easy consequence of H being abelian) we have $\theta(1)^2 = |P\colon \mathbf{Z}(P_0)^{\hat{E}}/W|$ and so θ is fully ramified over $\mathbf{Z}(P_0)^{\hat{E}}/W$. Hence, θ vanishes on $P - \mathbf{Z}(P_0)^{\hat{E}}/W$. As θ corresponds uniquely to $\tilde{\lambda}$, and $\tilde{\lambda}$ is in a regular orbit under the action of H on the irreducible characters of $\mathbf{Z}(P_0)^{\hat{E}}/W$, we have $\mathcal{I}_G(\theta) = P$ and hence $\chi = \theta^G$ is irreducible.

This implies that $\mathbf{Z}(P) = \mathbf{Z}(P_0)^{\hat{E}}/W$ and that χ vanishes on $G - \mathbf{Z}(P)$. Clearly

$$\chi(g) = -|P\colon \mathbf{Z}(P)|^{1/2} \quad \text{for } g \in \mathbf{Z}(P)^{\#}$$

and

$$\chi(1) = (p^a - 1)|P\colon \mathbf{Z}(P)|^{1/2}.$$

Thus χ is the required character of G, and conditions (b) and (c) of the theorem are evident from the construction of G. It remains to prove (d).

From the construction of P, $P/\mathbf{Z}(P)$ is isomorphic to a group of the form $\hat{E} \ltimes ((P_0/\mathbf{Z}(P_0))^{\hat{E}} \times E)$ where $(P_0/\mathbf{Z}(P_0))^{\hat{E}}$ is stabilized by the action of $\hat{E}$, and this action itself is that of a wreath product. Thus, $P/\mathbf{Z}(P)$ contains a subgroup isomorphic to the wreath product $(P_0/\mathbf{Z}(P_0)) \wr \hat{E}$ which in turn contains $(P_0/\mathbf{Z}(P_0)) \wr C_p$ where C_p is the cyclic group of order p. Now Q is isomorphic to a subgroup of $Q_0 \wr (Q/Q_0) = Q_0 \wr C_p$ and this completes the proof. (Elementary properties of the wreath product which were used may be found in [6]. See especially pp. 98–99.) $\square$

The hypothesis that H is isomorphic to the multiplicative group of a field (rather than a general near-field) was used only once in the proof given above (namely to prove $|\hat{E}| = |E|$). It may be interesting to find an analogue of Theorem 6.3 which applies to general near-fields.

The examples that Theorem 6.3 generates are all p-closed. It is not hard to produce examples of this directly. Indeed, if F is any finite field, say $|F| = s$ where s is a power of some prime p, then let

$$G = \left\{ \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & d \end{pmatrix} \middle| \, a, b, c, d \in F, d \neq 0 \right\}.$$

Then

$$P = \left\{ \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \middle| \, a, b, c \in F \right\}$$

is normal in G, $\mathbf{Z}(P)^\#$ is a single conjugacy class of G and χ defined by $\chi(1) = s(s-1)$, $\chi(g) = -s$ for $g \in \mathbf{Z}(P)^\#$ and $\chi(x) = 0$ for $x \in G - \mathbf{Z}(P)$ is an irreducible character of G.

We close this section with two examples which are not p-closed.

Let p and q be the primes 2 and 3 in some order and let R be the ring $\mathbf{Z}/p^2\mathbf{Z}$. The natural map $\mathrm{SL}(2, R) \to \mathrm{SL}(2, p)$ is surjective, and the kernel K is elementary abelian of order p^3. Since p is 2 or 3, the group $\mathrm{SL}(2, p)$ has a normal p-complement which is a Sylow q-subgroup, and hence, $\mathrm{SL}(2, R) = K \cdot \mathbf{N}_{\mathrm{SL}(2,R)}(Q)$ where Q is a Sylow q-subgroup of $\mathrm{SL}(2, R)$.

If $p = 2$ then the group $S = \mathbf{N}_{\mathrm{SL}(2,R)}(Q)$ intersects K in $\langle -I \rangle$ and S itself is the semidirect product of a cyclic group of order 4 with a cyclic group of order 3. (For example, Q may be generated by $\left(\begin{smallmatrix} 0 & 1 \\ -1 & -1 \end{smallmatrix}\right)$. Then $\left(\begin{smallmatrix} 1 & -1 \\ 2 & -1 \end{smallmatrix}\right)$ has order 4 and inverts Q. The entries are taken mod 4 of course.) Let $M = R \oplus R$ so that $\mathrm{SL}(2, R)$, and hence S, acts naturally on M, and let G denote the semidirect product $S \ltimes M$ of S with M under this action. Now let $N = \Omega_1(M)$ (the subgroup of M generated by the involutions of M). The subgroup S transitively permutes the nonprincipal characters of N. Let λ be one of these and set $P = \mathcal{I}_G(\lambda)$. Then P is a Sylow 2-subgroup of G. Notice that λ extends to M as M is abelian. If $\tilde{\lambda}$ is an extension of λ to M then $\tilde{\lambda}$ is necessarily complex valued, and so $\tilde{\lambda}$ is not fixed by $-I$.

Hence, $\mathfrak{I}_P(\tilde{\lambda}) = M$ and $\psi = \tilde{\lambda}^P$ is an irreducible character of P, fully ramified over N and uniquely corresponds with λ. As $\mathfrak{I}_G(\lambda) = P$ we have $\chi = \psi^G$ an irreducible character of G. By construction, χ vanishes on $G - N$.

Suppose now $p = 3$. For this case Q is the quaternion group of order 8, and $\mathbf{N}_{\mathrm{SL}(2,R)}(Q)$ is a complement for K in $\mathrm{SL}(2, R)$, and hence is isomorphic to $\mathrm{SL}(2,3)$. Let $S = \langle 4I \rangle \times \mathbf{N}_{\mathrm{SL}(2,R)}(Q) \leq \mathrm{GL}(2, R)$, and as before, let $M = R \oplus R$, $N = \Omega_1(M)$ and $G = S \ltimes M$.

The group $\mathbf{N}_{\mathrm{SL}(2,R)}(Q)$ contains an element of order 3, say g, which maps onto $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ under the natural map to $\mathrm{SL}(2,3)$. As $\det g = 1$ and $g^3 = I$, g must have the form

$$g = \begin{pmatrix} 1+\alpha & 1+\beta \\ 6 & 7-\alpha \end{pmatrix}$$

where $\alpha, \beta \in 3R$.

Let $P = \langle g \rangle$ and $C = \langle 4I \rangle$ so that $PC = P \times C$ is a Sylow 3-subgroup of S, and PCM is a Sylow 3-subgroup of G. Let λ be an irreducible character of N with kernel $0 \oplus 3R$. Then λ has an extension to a character $\tilde{\lambda}$ of M with kernel $0 \oplus R$. Notice that $\tilde{\lambda}$ has order 9. As $\mathfrak{I}_G(\tilde{\lambda})$ normalizes $\ker \tilde{\lambda} = 0 \oplus R$ we have $\mathfrak{I}_{PC}(\tilde{\lambda}) \leq \mathbf{N}_{PC}(0 \oplus R) = C$. Moreover, C permutes fixed point freely the characters of M having order 9, so $\mathfrak{I}_{PC}(\tilde{\lambda}) = 1$ and hence $\mathfrak{I}_{PCM}(\tilde{\lambda}) = M$. Thus, $\theta = \tilde{\lambda}^{PCM}$ is irreducible, and as in the last case, $\chi = \theta^G$ is an irreducible character of G vanishing on $G - N$.

In each of the two examples above, $O_p(G)$ is not a Sylow p-subgroup of G. However, $G/O_p(G)$ does have a normal p-complement, in accordance with Theorem 4.2.

7. Concluding remarks. If G is a group which has an irreducible character that vanishes on all but two conjugacy classes then $O_p(G) \neq 1$ for some unique prime p, and the group $H = G/O_p(G)$ is determined by Theorems 4.2 (in the solvable case) and 5.6 (in the nonsolvable case). The author, however, has no examples to illustrate that the first three cases of Theorem 5.6 actually occur. The last three cases arise as examples in a doubly-transitive Frobenius group.

If $O_p(G)$ is a Sylow p-subgroup of G and $G/O_p(G)$ is cyclic, then Theorem 6.3 shows that $O_p(G)$ can be arbitrarily complicated. When $G/O_p(G)$ is noncyclic (in particular, when it is nonsolvable) the argument in Theorem 6.3 breaks down. It may be possible to classify $O_p(G)$ in this case.

Finally, when $O_p(G)$ is not a Sylow p-subgroup, then $N < O_p(G)$ necessarily holds where N is the unique minimal normal subgroup of G

(Theorem 6.2). It is natural to ask if $O_p(G)$ can be arbitrarily complicated in this case. In the last two examples given in §6, $O_p(G)$ is nonabelian of class 2. As already mentioned in the first paragraph, the author is not aware of any nonsolvable examples in this case.

I would like to take this opportunity to thank the referee for simplifying the proof of Lemma 4.1.

REFERENCES

[1] H. Bender, *Finite groups with dihedral Sylow 2-subgroups*, J. Algebra, **70** (1981), 216–228.

[2] R. Brauer and C. Nesbitt, *On the modular characters of groups*, Annals of Math., **42** (1941), 556–590.

[3] S. M. Gagola, Jr., *Characters fully ramified over a normal subgroup*, Pacific J. Math., **55** (1974), 107–126.

[4] D. Gorenstein and J. Walter, *The characterization of finite groups with dihedral Sylow 2-subgroups I, II, III*, J. Algebra, **2** (1965), 85–151, 218–270, 334–393.

[5] Marshall Hall, Jr., *Combinatorial Theory*, Blaisdell, Waltham, Massachusetts, 1967.

[6] B. Huppert, *Endliche Gruppen I*, Springer-Verlag, Berlin/Heidelberg/New York, 1967.

[7] I. Martin Isaacs, *Character Theory of Finite Groups*, Academic Press, New York, 1976.

[8] H. Zassenhaus, *Uber Endliche Fastkörper*, Abh. Math. Sem. Hamburg, **11** (1936), 187–220.

Received January 5, 1982 and in revised form January 24, 1983.

KENT STATE UNIVERSITY
KENT, OH 44242