View metadata, citation and similar papers at core.ac.uk brought to you by CORE
provided by Elsevier - Publisher Connector

JOURNAL OF ALGEBRA 30, 496–506 (1974)

On Finite Linear Groups II

WALTER FEIT*

Department of Mathematics, Yale University, New Haven, Connecticut 06520

Communicated by the Editors

Received April 12, 1973

1. INTRODUCTION

The primary purpose of this paper is to study the following situation.

(i) *G is a finite group. p is an odd prime and P is a Sylow p-group of G with $|P| = q$.*

(ii) *$G = G'$. $\mathbf{Z}(G)$ is cyclic and $G/\mathbf{Z}(G)$ is simple.*

(iii) *P is abelian. If $x \in G - \mathbf{N}_G(P)$ then $P \cap x^{-1}Px = \langle 1 \rangle$.*

(iv) *$\mathbf{C}_G(P) = P \times \mathbf{Z}(G)$ and $|\mathbf{N}_G(P) : \mathbf{C}_G(P)| = 2$.* $\qquad (*)$

The main result of this paper follows.

THEOREM 1. *Suppose that $(*)$ is satisfied with $q \geqslant 7$. Let χ be a faithful irreducible character of G with $\chi(1) \not\equiv 0 \pmod p$. Then one of the following holds.*

(I) $\mathbf{Z}(G) = \langle 1 \rangle$.

(II) $|\mathbf{Z}(G)| = 2$. *$2q \pm 1$ is a prime power and $G/\mathbf{Z}(G) \approx PSL_2(2q \pm 1)$.*

(III) *$|\mathbf{Z}(G)|$ is even and G contains exactly one conjugate class of non-central involutions.*

(IV) *For $q \geqslant 19$, $\chi(1) \geqslant q((q-7)/4) - 2$ if $q \equiv 3 \pmod 4$. $\chi(1) \geqslant q((q-9)/4) - 2$ if $q \equiv 1 \pmod 4$. Furthermore if $q = 7$ or 11 then $\chi(1) \geqslant 2q - 2$. If $q = 13$ or 17 then $\chi(1) > q - 2$.*

The following result which was announced previously [9, Theorem 8.3.4(iii)] is a consequence of Theorem 1.

THEOREM 2. *Let G be a finite group. Let $p > 5$ be a prime and let P be a Sylow p-group of G. Assume that G has a faithful complex irreducible represen-*

* The work on this paper was partially supported by NSF Contract No. GP-33591.

Copyright © 1974 by Academic Press, Inc.
All rights of reproduction in any form reserved.

tation of degree $p-2$. *Then either* $P \lhd G$ *or* $p-1=2^a$ *and* $G \approx SL_2(p-1) \times A$ *where* A *is an abelian group.*

In case $p=5$ Theorems 1 and 2 are both false since there exists a group G with a center Z of order 3 and $G/Z \approx \mathfrak{A}_6$ which has a faithful three-dimensional complex irreducible representation. As all three-dimensional complex groups are known it can be seen by inspection that up to an abelian factor the above mentioned group is the only counterexample for $p=5$.

Theorem 2 is proved by using Theorem 1 to reduce to the case where the center of G has order 1. In this case the result is an immediate consequence of [8, Theorem 2]. The main result of [6] is used to reduce to the case that P has order p. The argument here is quite straightforward and is similar to that used in [8].

Section 5 contains a proof of the following result which is handled by similar methods and is occasionally useful.

THEOREM 3. *Let* G *be a finite group with* $G = G'$. *Let* p *be an odd prime. Suppose* G *has an abelian Sylow* p*-group* P *which satisfies the following conditions*

(i) *If* $x \in G - \mathbf{N}_G(P)$ *then* $x^{-1}Px \cap \mathbf{N}_G(P) = \langle 1 \rangle$.

(ii) *There exists a subgroup* H *of* G *such that* $\mathbf{C}_G(P) = \mathbf{C}_G(u) = P \times H$ *for all* $u \in P$, $u \neq 1$.

(iii) $|\mathbf{N}_G(P) : \mathbf{C}_G(P)| = 3$.

Then if λ *is a nonprincipal linear character of* $P \times H/H$

$$(1_{P\times H} - \lambda)^G = 1_G + \theta - \zeta - \eta$$

where θ, ζ, η *are irreducible characters of* G *and* $\theta(1)\,\zeta(1)\,\eta(1)$ *is the square of a rational integer.*

As an immediate corollary of Theorem 3 one gets the following theorem.

THEOREM 4. *Suppose that* G *has a Sylow* p*-group* P *of order* $p > 3$. *Assume that* $G = G'$ *and* $|\mathbf{N}_G(P) : \mathbf{C}_G(P)| = 3$. *Let* $1_G, \theta, \eta, \chi_1, \ldots, \chi_{(p-1)/3}$ *be all the irreducible characters in the principal* p*-block of* G *where* $\chi_1, \ldots, \chi_{(p-1)/3}$ *are exceptional. Then* $\theta(1)\,\eta(1)\,\chi_1(1)$ *is the square of a rational integer.*

The situation described in Theorem 3 occurs infinitely often. For instance let $G_1(q) = PSL_3(q)$ and let $G_{-1}(q) = PSU_3(q)$. Then for $\epsilon = \pm 1$, $G_\epsilon(q)$ contains a subgroup $A = P \times H$ which satisfies the assumptions of Theorem 3 of order $(q^2+\epsilon q+1)/(q^2+\epsilon q+1, 3)$. The degrees of the given characters are q^3, $q^2+\epsilon q$, and $(q^2-1)(q-\epsilon)$.

The notation used is standard and is the same as that used in [8] except that the gothic letters have been replaced by ordinary capital letters.

2. Some Consequences of Condition (*)

Throughout this section it will be assumed that condition $(*)$ *is satisfied.*

Lemma 2.1. *P is cyclic.*

Proof. This follows from [11].

The results of [11] are not really necessary for this paper since the results of [2] yield sufficient information about the characters of G for what is needed here. However in view of Lemma 2.1 the theory of blocks with a cyclic defect group becomes available and can be used to simplify some of the arguments.

Let $Z = \mathbf{Z}(G)$. Let $|Z| = m$ and let $\mu_1 = 1_Z, \ldots, \mu_m$ be all the irreducible characters of Z. For $i = 1, \ldots, m$ let B_i be the p-block of G corresponding to μ_i.

Let $P = \langle y \rangle$.

Lemma 2.2. *Any two involutions in* G/Z *are conjugate.*

Proof. Since G/Z satisfies $(*)$ it may be assumed after a change of notation that $Z = \langle 1 \rangle$ and $G = G/Z$. Since $|\mathbf{N}_G(P) : P| = 2$ it follows that $\mathbf{N}_G(P)$ contains exactly one conjugate class of involutions. Suppose that x is an involution in G which is not conjugate to any element of $\mathbf{N}_G(P)$. Then y is not the product of two conjugates of x. Therefore

$$\sum \frac{\xi(x)^2\, \xi(y)}{\xi(1)} = \sum \frac{\xi(x)\, \xi(1)\, \xi(y)}{\xi(1)} = \sum \frac{\xi(1)^2\, \xi(y)}{\xi(1)} = 0, \qquad (2.3)$$

where ξ ranges over all the irreducible characters of G. Since $\xi(y) = 0$ unless ξ is in B_1 the same equations hold if ξ runs over the irreducible characters in B_1. Let

$$\underset{1}{\circ} \text{———} \underset{\eta}{\circ} \text{———} \underset{\zeta}{\circ}$$

be the tree corresponding to B_1. Then (2.3) implies that

$$1 + \frac{\zeta(1)^2}{\zeta(1)} - \frac{\eta(1)^2}{\eta(1)} = 1 + \frac{\zeta(1)\, \zeta(x)}{\zeta(1)} - \frac{\eta(1)\, \eta(x)}{\eta(1)}$$
$$= 1 + \frac{\zeta(x)^2}{\zeta(1)} - \frac{\eta(x)^2}{\eta(1)} = 0.$$

Hence the vectors $(1, \zeta(1), \eta(1))$, $(1, \zeta(x), \eta(x))$ lie in an isotropic subspace for the diagonal quadratic form $(1, \zeta(1)^{-1}, -\eta(1)^{-1})$. Since this is a non-degenerate form an isotropic subspace has dimension at most 1. Thus the two vectors are proportional and so $\zeta(x) = \zeta(1)$. Hence x is in the kernel of ζ contrary to the simplicity of G.

LEMMA 2.3. *One of the following holds*

(i) *Condition* (I), (II), *or* (III) *of Theorem* 1 *is satisfied.*

(ii) *There exists an involution w in $\mathbf{N}_G(P) - \mathbf{C}_G(P)$ which is not conjugate in G to any element of the form wz with z in Z, $z \neq 1$.*

Proof. Suppose that $\mathbf{N}_G(P) - \mathbf{C}_G(P)$ contains no involutions. Then there exists a unique involution z in $\mathbf{N}_G(P)$ and $z \in Z$. Then by Lemma 2.2 z is the unique involution in G. This implies that a Sylow 2-group of G is a generalized quaternion group. Thus a Sylow 2-group of G/Z is a dihedral group. Therefore the main result of [4] implies that G/Z is either isomorphic or $\mathfrak{A}_7$ or $PSL_2(r)$ for some prime power r. It is easily seen that $\mathfrak{A}_7$ does not satisfy $(*)$ for any prime p. Furthermore if $PSL_2(r)$ satisfies $(*)$ for p then $|P| = (r \pm 1)/2$. Since $q \geqslant 7$, $PSL_2(2q \pm 1)$ has a Schur multiplier of order 2. Thus either condition (I) or (II) of Theorem 1 is satisfied.

Suppose that w is an involution in $\mathbf{N}_G(P) - \mathbf{C}_G(P)$ and condition (ii) of the Lemma does not hold. Let z be an element in Z, $z \neq 1$, such that w is conjugate to wz in G. Then clearly z is an involution. Since every involution in $\mathbf{N}_G(P)$ is conjugate to w, wz or z in $\mathbf{N}_G(P)$ it follows from Lemma 2.2 that every involution in G is conjugate to w or z. Thus condition (III) of Theorem 1 is satisfied and the Lemma is proved.

Suppose that condition (ii) of Lemma 2.3 is satisfied. For $i = 1,..., m$ define

$$f_i = \sum_{\xi \text{ in } B_i} \frac{\xi(w)^2 \, \xi(y)}{\xi(1)} .$$

LEMMA 2.4. *Suppose that condition* (ii) *of Lemma* 2.3 *is satisfied. Then $f_i = f_1$ for $i = 1,..., m$.*

Proof. Induction on m. If $m = 1$ the result is clear.

Let H be any subgroup of Z. Let $\bar{G} = G/H$ and let $\bar{x}$ be the image of x in $\bar{G}$. The group $\bar{G}$ clearly satisfies condition $(*)$. If $H \neq \langle 1 \rangle$ and $\bar{x} = \overline{wz}$ for some element z in Z with $\bar{z} \neq 1$ then x has order at least 4. Thus w is not conjugate to x. Hence $\bar{G}$ also satisfies condition (ii) of Lemma 2.3.

Let n_H be the number of ordered pairs of involutions x_1, x_2 in $\bar{G}$ with $\bar{y} = x_1 x_2$ and x_1, x_2 conjugate to $\bar{w}$ in $\bar{G}$. Then $x_1, x_2 \in \mathbf{N}_{\bar{G}}(\bar{P})$. Hence condition (ii) of Lemma 2.3 implies that $n_H = p$. Furthermore

$|\mathbf{C}_{\bar{G}}(x_1)|\,|H| = |\mathbf{C}_G(w)|$. Thus

$$\frac{|G|}{|\mathbf{C}_G(w)|^2}\sum_{i=1}^{m} f_i = n_{\langle 1\rangle} = p = n_H = \frac{|G:H|}{|\mathbf{C}_G(x_1)|^2}\sum_{H \text{ in kernel of } \mu_i} f_i\,.$$

Consequently

$$\sum_{i=1}^{m} f_i = |H| \sum_{H \text{ in kernel of } \mu_i} f_i\,. \tag{2.6}$$

By induction $f_i = f_1$ if μ_i is not a faithful character of Z. There are $\phi(m)$ faithful characters of Z and they are all algebraically conjugate. Since f_i is rational for all i this implies that if μ_m is a faithful character of Z then $f_j = f_m$ for any faithful character μ_j of Z. Hence (2.6) with $H = Z$ yields that

$$mf_1 = \sum_{i=1}^{m} f_i = \{m - \phi(m)\}f_1 + \phi(m)f_m\,.$$

Consequently $f_m = f_1$ and the result is proved.

3. Proof of Theorem 1

Throughout this section the following will be assumed.

Condition $(*)$ *and condition* (ii) *of Lemma* 2.3 *are both satisfied with* $q \geqslant 7$.

$\mathbf{Z}(G) \neq \langle 1\rangle$.

χ *is a faithful irreducible character of* G *with* $\chi(1) \not\equiv 0 \pmod{p}$.

The notation of Section 2 will be used without change and $W = \langle w\rangle$.

In view of Lemma 2.3 the proof of Theorem 1 will be complete once it is shown that the above mentioned hypotheses imply that condition (IV) of Theorem 1 holds. This will be done in a series of Lemmas in this section.

Lemma 3.1. *Let* ξ *be an irreducible character of* G *with* $\xi(1) \not\equiv 0 \pmod{p}$. *Then*

(i) $\xi(1) = kq \pm 1$ *or* $kq \pm 2$ *for some integer* k.

(ii) *If* $\xi(1) = kq + 1$ *then* $|\xi(w)| \leqslant k + 1$. *If* $\xi(1) = kq - 2$ *then* $|\xi(w)| \leqslant k$. *Furthermore*

$$\frac{|\xi(w)|}{\xi(1)} \leqslant \frac{1}{q} + \frac{1}{\xi(1)}\,.$$

(iii) *If* $\xi(1) = q + 1$ *then* $\xi(w) = \pm\{1 - (-1)^{(q+1)/2}\}$. *If* $\xi(1) = q - 2$ *then* $\xi(w) = (-1)^{(q+1)/2}$.

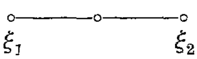
Proof. By [3] (i) is an immediate consequence of Lemma 2.1.

$$\xi_{PW} = \lambda + \sum_{i=1}^{k} \gamma_i \qquad \text{or} \qquad \gamma_k - \lambda + \sum_{i=1}^{k-1} \gamma_i$$

where each γ_i is a character of PW which vanishes on $P - \langle 1 \rangle$. λ is an irreducible character of PW and in the second case λ is a constituent of γ_k. This is easily seen to imply that $\gamma_i = \alpha_i^{PW}$ is the character of PW induced by the linear character α_i of W. Thus $\gamma_i(w) = \pm 1$ for all i and γ_i has a unique linear irreducible constituent. Furthermore every nonlinear irreducible character of PW vanishes on w. If $\xi(1) = kq + 1$ this implies that $|\xi(w)| = |\lambda(w) + \sum_{i=1}^{k} \gamma_i(w)| \leqslant k + 1$. If $\xi(1) = kq - 2$ then $\lambda(w) = 0$ and so $|\xi(w)| = |\sum_{i=1}^{k} \gamma_i(w)| \leqslant k$. The last statement in (ii) follows by inspection.

Let $M(w)$ be the linear transformation corresponding to w in the representation which affords ξ. All the characteristic roots of $M(w)$ are ± 1 and the determinant of $M(w) = 1$. Thus -1 occurs as a characteristic root with even multiplicity. Since the trace of $M(w)$ is $\xi(w)$ condition (iii) is a direct consequence of condition (ii).

Lemma 3.2. *Let*



be the tree corresponding to the block $B = B_i$. *Then after possibly interchanging* ξ_1 *and* ξ_2 *it follows that* $\xi_1(1) = 1 \pmod q$ *and*

$$f_i = \left\{ \frac{\xi_1(w)}{\xi_1(1)} - \frac{\xi_2(w)}{\xi_2(1)} \right\}^2 \left\{ \frac{1}{\xi_1(1)} + \frac{1}{\xi_2(1)} \right\}^{-1}.$$

Proof. It may be assumed that $\xi_1(1) \equiv \epsilon \pmod q$ for $\epsilon = \pm 1$. By definition

$$f_i = \frac{\xi_1(w)^2}{\xi_1(1)} \epsilon + \frac{\xi_2(w)^2}{\xi_2(1)} \epsilon - \frac{\{\xi_1(w) + \xi_2(w)\}^2}{\xi_1(1) + \xi_2(1)} \epsilon.$$

Direct computation shows that ϵf_i is equal to the expression in the statement of the lemma. Since $f_i = f_1 \geqslant 0$ this implies that $\epsilon = 1$.

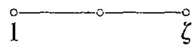
Lemma 3.3. *For* a, t *real let* $g(t) = (a + t)^2 t^{-1}$. *Then* $g(t)$ *is monotonic increasing for* $|t| > |a|$ *and* $g(t)$ *is monotonic decreasing for* $0 < |t| < |a|$.

Proof. Elementary calculus.

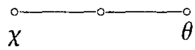
Throughout the rest of this section the following notation will be used.

$B = B_i$ is the block containing χ. $f = f_i$. Since χ is faithful and $Z \neq \langle 1 \rangle$ it follows that $B \neq B_1$. Thus every irreducible character in B is faithful on Z and hence faithful on G.

Let



be the tree corresponding to B_1 and let $\zeta(1) = c$. Let



be the tree corresponding to B and let $\chi(1) = d$, $\theta(1) = e$. Choose the notation so that $d \leqslant e$.

LEMMA 3.4. (i) $f_1 > 1 - 5/q$.

(ii) *If* $d = q - 2$ *then* $f < 9/2q$.

(iii) *If* $d > q - 2$ *then*

$$f \leqslant \frac{4}{q^2} d + \frac{4}{q} + \frac{1}{d}.$$

Proof (i). Suppose that $c = q - 2$. By Lemma 3.1(iii) and Lemma 3.2

$$f_1 \geqslant \left(1 - \frac{1}{q-2}\right)^2 \left(1 + \frac{1}{q-2}\right)^{-1} = \frac{(q-3)^2}{(q-2)(q-1)}$$

$$= 1 - \frac{(3q-7)}{q^2 - 3q + 2} > 1 - \frac{5}{q}.$$

Suppose that $c > q - 2$. By Lemma 3.2 $c > q$. Let $g_1(t) = (1/q - 2 + t)^2 t^{-1}$. Then $f_1 \geqslant g_1(1 + 1/c)$. Since $1 + 1/c < 2 - 1/q$. Lemma 3.3 implies that

$$f_1 \geqslant g_1\left(1 + \frac{1}{q}\right) = \left(1 - \frac{2}{q}\right)^2 \left(1 + \frac{1}{q}\right)^{-1} = \frac{(q-2)^2}{q(q+1)}$$

$$= 1 - \frac{(5q-4)}{q^2 + q} > 1 - \frac{5}{q}.$$

(ii) If $e = q - 2$ then Lemma 3.1(iii) and Lemma 3.2 imply that $f = 0$. If $e = q + 1$ then by Lemma 3.1(iii)

$$f \leqslant \left(\frac{1}{q-2} + \frac{2}{q+1}\right)^2 \left(\frac{1}{q-2} + \frac{1}{q+1}\right)^{-1}$$

$$= \frac{9(q-1)^2}{(2q-1)(q-2)(q+1)} < \frac{9}{2q}$$

for $q \geqslant 7$.

Suppose that $e > q+1$. Then $e \geqslant 2q-2$ by Lemma 3.2 and so $1/q < 1/d + 1/e < 2/q$. Let $g(t) = (1/q + t)^2 t^{-1}$. Then $f \leqslant g(1/d + 1/e)$. Hence by Lemma 3.3

$$f \leqslant g\left(\frac{2}{q}\right) = \left(\frac{3}{q}\right)^2 \frac{q}{2} = \frac{9}{2q}.$$

(iii) Let $g(t) = (2/q + t)^2 t^{-1}$. Then $f \leqslant g(1/d + 1/e)$. Since $1/d < 1/d + 1/e < 2/q$ it follows from Lemma 3.3 that

$$f \leqslant g\left(\frac{1}{d}\right) = \left(\frac{2}{q} + \frac{1}{d}\right)^2 d = \frac{4}{q^2} d + \frac{4}{q} - \frac{1}{d}.$$

LEMMA 3.5. *Condition* (IV) *of the theorem holds for* $q \geqslant 13$.

Proof. Suppose that $q \geqslant 13$. By Lemma 2.4 and 3.4 $1 - 5/q < f_1 = f$. If $d = q-2$ then Lemma 3.4 implies that $1 - 5/q < 9/2q$ and so $2q < 19$ which is not the case. Suppose that $d > q-2$. Thus it may be assumed that $q \geqslant 19$. Then Lemma 3.4 implies that

$$1 - \frac{5}{q} < \frac{4}{q^2} d + \frac{4}{q} + \frac{1}{d}.$$

Therefore $0 < 4d^2 - (q^2 - 9q)d + q^2$. Hence one of the following possibilities must occur.

$$8d \leqslant q^2 - 9q - q(q^2 - 18q + 65)^{1/2} < q\{(q-9) - (q-10)\} = q,$$

$$8d \geqslant q^2 - 9q + q(q^2 - 18q + 65)^{1/2} > q\{(q-9) + (q-10)\} = q(2q-19).$$

Since $d \geqslant q-2$ the first possibility cannot occur. Therefore $d > q(2q-19)/8$. If $q \equiv 3 \pmod 4$ this implies that $d > q((q-7)/4) - (3/8)q$. Since $d \equiv 1$ or $-2 \pmod q$ this implies that $d \geqslant q((q-7)/4) - 2$. If $q = 1 \pmod 4$ then $d > q((q-9)/4) - 5q/8$. Hence $d \geqslant q((q-9)/4) - 2$ in this case. The last statement in Condition (IV) is an immediate consequence as $q \geqslant 13$ and the lemma is proved.

To complete the proof of condition (IV) of Theorem 1 it is now sufficient to consider the cases where $q = 7$ or $q = 11$ and $d = q+1$ or $q-2$.

Suppose that $d = q+1$. By Lemma 3.1(iii) $\chi(w) = 0$ for $q = 7$ or 11. If $e = q+1$ then $f = 0$ by Lemma 3.1(iii). Then by Lemmas 2.4 and 3.4 $0 = f_1 > 1 - 5/q$ which is not the case. If $e > q+1$ then $e \geqslant 2q-2$. Lemmas 3.1(ii) and 3.2 imply that if $g(t) = ((1/q(q+1)) + t)^2 t^{-1}$ then

$$f \leqslant g\left(\frac{1}{e} + \frac{1}{q+1}\right) \leqslant g\left(\frac{1}{2q-2} + \frac{1}{q+1}\right) = \frac{(3q-2)^2 (q+1)}{2q^2(q-1)(3q-1)}.$$

If $q = 7$ or 11 this implies by direct computation that $f < 1 - 5/q$ contrary to Lemmas 2.5 and 3.4.

Suppose that $d = q - 2$. Then Lemmas 2.4 and 3.4 yield that $1 - 5/q < 9/2q$ and so $2q < 19$. Thus $q \neq 11$ and so $q = 7$. Hence $d = 5$. If χ is a monomial character then $P \lhd G$ contrary to assumption. If χ is not monomial then G is one of the groups listed in [1]. It can be seen by inspection that 7 does not divide $|G|$. Hence this case cannot occur. The proof of Theorem 1 is complete.

4. Proof of Theorem 2

Lemma 4.1. *Let G be a minimal counterexample to Theorem 2. Then G satisfies condition $(*)$ with $|P| = p$.*

Proof. Since G is a counterexample to Theorem 2 $P \ntriangleleft G$. The main result of [6] yields the existence of a subgroup P_0 of P with $|P : P_0| = p$ and $P_0 \lhd G$. Since G has a faithful representation of degree $p - 2 < p$ it follows that P is abelian. Hence $P \subseteq \mathbf{C}_G(P_0) \lhd G$. Let G_0 be the subgroup of G generated by all elements of order p. Thus $G_0 \lhd G$ and $G_0 \subseteq \mathbf{C}_G(P_0)$. Hence Burnside's transfer theorem implies that $G_0 = G_1 \times P_0$ for some characteristic subgroup G_1 of G_0. Therefore $G_1 \lhd G$. Let $P_1 = P \cap G_1$. Thus $|P_1| = p$ and $P_1 \ntriangleleft G_1$.

Suppose that $G_1 \neq G$. The minimality of G implies that $p = 2^a + 1$ and $G_1 = G_2 \times A$ where $G_2 \approx SL_2(p-1)$ and A is abelian. The smallest degree of a faithful irreducible character of $SL_2(p-1)$ is $p - 2$ and no outer automorphism of $SL_2(p-1)$ stabilizes a character of degree $p - 2$. Thus χ_{G_2} is irreducible and $G = G_2\mathbf{C}_G(G_2) = G_2 \times \mathbf{C}_G(G_2)$ with $\mathbf{C}_G(G_2)$ abelian contrary to the fact that G is a counterexample to Theorem 1.

Therefore $G_1 = G$. Hence $P_1 = P$ and $G = G_0$ is generated by all elements of order p. Thus $G = G'$. Since G has a faithful irreducible character $\mathbf{Z}(G)$ is cyclic.

Let H be a normal p'-subgroup of G. Then PH is a p-solvable group which has a faithful complex representation of degree $p - 2$. Thus by a result of Ito $P \lhd PH$. See e.g. [5, (24.6)]. Hence $P \subseteq \mathbf{C}_G(H) \lhd G$. Since G is generated by its p-elements this implies that $H \subseteq \mathbf{Z}(G)$. Thus $G/\mathbf{Z}(G)$ is simple and condition (ii) of $(*)$ is satisfied.

Condition (iii) of $(*)$ is satisfied as $|P| = p$. By [7, Theorem 1] $\mathbf{C}_G(P) = P \times \mathbf{Z}(G)$. Thus by [3] $|\mathbf{N}_G(P) : \mathbf{C}_G(P)| = 2$. Hence also condition (iv) of $(*)$ is satisfied.

Theorem 2 can now be proved.

Let G be a minimal counterexample to Theorem 2. By Lemma 4.1 $(*)$ is satisfied with $|P| = p$. Thus Theorem 1 can be applied. Since $\chi(1) = p - 2$

is odd it follows that $|\mathbf{Z}(G)|$ is odd. Therefore (II), (III), or (IV) of Theorem 1 cannot hold. Consequently by Theorem 1 $|\mathbf{Z}(G)| = 1$. Theorem 2 now follows directly from [8, Theorem 2].

5. Proof of Theorem 3

Suppose that G satisfies the hypotheses of Theorem 3. Let $N = \mathbf{N}_G(P)$. Let $\lambda = \lambda_1, \lambda_2, \ldots$ be all the nonprincipal irreducible characters of $(P \times H)/H$. Let $\tilde{\lambda}_i$ be the character of N induced by λ_i. Then each $\tilde{\lambda}_i$ is an irreducible character of N and after relabeling it may be assumed that $\tilde{\lambda}_1, \ldots, \tilde{\lambda}_n$ are all the distinct irreducible characters of N in the principal p-block which do not contain P in their kernel where $n = (|P| - 1)/3$.

There exists a sign $\epsilon = \pm 1$ and irreducible characters $\chi_1, \ldots, \chi_n$ of G with $(\tilde{\lambda}_i - \tilde{\lambda}_j)^G = \epsilon(\chi_i - \chi_j)$. See for instance [2]. Furthermore

$$\|(1_{P\times H} - \lambda)^G\|^2 = 4 \qquad \text{and} \qquad (1_{P\times H} - \lambda)^G = 1_G + \epsilon\chi_1 + \delta_1\theta_1 + \delta_2\theta_2,$$

where $\theta_1 \neq \theta_2$ are irreducible characters distinct from 1 and each χ_i, and $\delta_j = \pm 1$ for $j = 1, 2$.

Let y be an element of $P - \langle 1 \rangle$. Since $|N : \mathbf{C}_G(P)| = 3$ it follows that no p-singular element of G is the product of two involutions. Thus if B denotes the principal p-block of G then

$$\sum_{\xi \text{ in } B} \frac{\xi(x_1)\, \xi(x_2)\, \xi(y)}{\xi(1)} = 0 \tag{5.1}$$

for $x_1^2 = x_2^2 = 1$.

By the results of [2] it follows that $\{1_G, \theta_1, \theta_2, \chi_1, \ldots, \chi_n\}$ is precisely the set of all irreducible characters in the principal p-block. Furthermore $\chi_i(y) = -\epsilon\tilde{\lambda}_i(y)$ and $\theta_i(y) = \delta_i$ for $i = 1, 2$. Thus (5.1) becomes

$$1 + \epsilon\frac{\chi_1(x_1)\,\chi_1(x_2)}{\chi_1(x)} + \frac{\delta_1\theta_1(x_1)\,\theta_1(x_2)}{\theta_1(1)} + \frac{\delta_2\theta_2(x_1)\,\theta_2(x_2)}{\theta_2(1)} = 0 \tag{5.2}$$

for $x_1^2 = x_2^2 = 1$.

Let V be a four-dimensional rational vector space. Define the symmetric bilinear from B on V by

$$B(u, v) = u_1v_1 + \frac{\epsilon}{\chi_1(1)}u_2v_2 + \frac{\delta_1}{\theta_1(1)}u_3v_3 + \frac{\delta_2}{\theta_2(1)}u_4v_4 .$$

It suffices to show that V has a two-dimensional isotropic subspace because in that case exactly one of $\epsilon, \delta_1, \delta_2$ is $+1$ and V is the orthogonal sum of two hyperbolic planes. See for instance [10, Chapter XIV]. Thus the discriminant of B is a square. Since the discriminant of B is $\{\chi_1(1)\,\theta_1(1)\,\theta_2(1)\}^{-1}$ Theorem 2 is proved.

By (5.2) $u = (1, \chi_1(1), \theta_1(1), \theta_2(1))$ is an isotropic vector in V. Since $G = G'$ there exists an involution x in G which is not in $\mathbf{O}_{p'}(G)$ and so is not in the kernel of χ_1, θ_1, and θ_2. Let $v = (1, \chi_1(x), \theta_1(x), \theta_2(x))$. Thus u and v are linearly independent vectors. By (4.2)

$$B(u, u) = B(u, v) = B(v, v) = 0.$$

Hence the two-dimensional subspace of V which is spanned by u and v is isotropic as required.

References

1. R. Brauer, Über endliche lineare Gruppen von Primzahlgrad, *Math. Ann.* **169** (1967), 73–96.
2. R. Brauer and H. S. Leonard, Jr., On finite groups with an abelian Sylow group, *Canad. J. Math.* **14** (1962), 436–450.
3. E. C. Dade, Blocks with cyclic defect groups, *Ann. of Math.* **84** (1966), 20–48.
4. D. Gorenstein and J. Walter, The Characterization of finite groups with dihedral Sylow 2-subgroups, *J. Algebra* **2** (1965), 85–151, 218–270, 354–393.
5. W. Feit, "Characters of Finite Groups," W. A. Benjamin, New York, 1967.
6. W. Feit, Groups which have a faithful representation of degree less than $p - 1$, *Trans. Amer. Math. Soc.* **112** (1964), 287–303.
7. W. Feit, Groups with a cyclic Sylow subgroup, *Nagoya Math. J.* **27** (1966), 571–584.
8. W. Feit, On finite linear groups, *J. Algebra* **5** (1967), 378–400.
9. W. Feit, The Current Situation in the Theory of Finite Simple Groups, Actes du Congres International des Mathematiciens 1970, Paris, 1971, pp. 55–93.
10. S. Lang, "Algebra," Addison-Wesley, Reading, MA, 1965.
11. S. D. Smith and A. P. Tyrer, On Finite Groups with a certain Sylow Normalizer I, II, *J. Algebra* **26** (1973), 343–365.