TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 282, Number 1, March 1984

BRAUER'S HEIGHT CONJECTURE FOR p-SOLVABLE GROUPS

BY

DAVID GLUCK AND THOMAS R. WOLF

ABSTRACT. We complete the proof of the height conjecture for p-solvable groups, using the classification of finite simple groups.

Introduction. The height conjecture is the statement that a p-block of a finite group has an abelian defect group if and only if all ordinary irreducible characters in the block have height zero.

While a proof of this conjecture for general finite groups seems remote, considerable progress has been made toward proving it for p-solvable groups. Fong [**5**] proved that all characters in a block with abelian defect group have height zero in a p-solvable group, and he proved the converse direction for the principal block [**5**] and for solvable groups in the case that p is the largest prime divisor of the group order [**6**].

Recently [**24**, **8**], the converse direction has been established for all solvable groups. In this paper we prove the converse direction for all p-solvable groups, assuming the classification of finite simple groups.

In its general outline this paper resembles [**8**], where we proved the height conjecture for solvable groups. The reader is assumed to have some familiarity with [**8**].

Now we state our main results, the analogs of the main results of [**8**].

THEOREM A. *Suppose that $N \lhd G$, that G/N is p-solvable, that $\varphi \in \mathrm{Irr}(N)$, and that $p \nmid (\chi(1)/\varphi(1))$ for all $\chi \in \mathrm{Irr}(G \mid \varphi)$. Then the p-Sylow subgroups of G/N are abelian.*

THEOREM B. *Let B be a p-block of a p-solvable group with defect group D. If every ordinary irreducible character in B has height zero, then D is abelian.*

THEOREM C. *Suppose that $N \lhd G$, that G/N is p-solvable, and that $\varphi \in \mathrm{Irr}(N)$. Suppose that e is an integer such that p^{e+1} does not divide $\chi(1)/\varphi(1)$ for all $\chi \in \mathrm{Irr}(G \mid \varphi)$. Then the derived length of a p-Sylow subgroup of G/N is at most $2e+1$.*

THEOREM D. *Let B and D be as in Theorem* B. *If every ordinary irreducible character in B has height at most e, then the derived length of D is at most $2e+1$.*

Received by the editors January 10, 1983.
1980 *Mathematics Subject Classification.* Primary 20C20, 20C15.

0002-9947/84 $1.00 + $.25 per page

Theorems B, C and D follow from Theorem A as in [**8**], so the rest of this paper is devoted to the proof of Theorem A.

The next proposition, essentially proved by Fong [**6**], describes the minimal counterexample to Theorem A. Note that N and φ in the statement of Theorem A correspond to Z and λ in the statement of Proposition 0, and that N in the statement of Proposition 0 does not correspond to any subgroup in the statement of Theorem A.

PROPOSITION 0. *Let G be a minimal counterexample to Theorem* A. *Then G has normal subgroups $Z \leqslant N \leqslant K$, and Z has a faithful linear character λ, such that the following conditions are satisfied*:

(1) $Z = O_{p'}(G)$ *is cyclic and central in* G.

(2) N/Z *is a self-centralizing p-chief factor of* G.

(3) $p \nmid |K : N|$ *and* $|G : K| = p$.

(4) $G = O^{p'}(G)$.

(5) *If* $V = \mathrm{Irr}(N/Z)$, *the irreducible* $GF(p)[G/N]$-*module dual to* N/Z, *then every element of V is centralized by some p-Sylow subgroup of* G/N.

(6) $p \nmid \chi(1)$ *for all* $\chi \in \mathrm{Irr}(G|\lambda)$.

PROOF. This follows as in Steps 1–4 of the proof of [**8**, Theorem 4.4]. The assumption in that theorem, that $p = 3$, is irrelevant in Steps 1–4, as is the assumption that G/Z is solvable rather than merely p-solvable.

The notation of Proposition 0 is used in the following summary of the contents of this paper.

After some preliminary lemmas on simple groups in §1, we consider in §2 the case that V is an imprimitive $GF(p)[G/N]$-module. We use a variety of facts about permutation groups and character degrees of groups of Lie type to show that G must be solvable.

In §3 we consider the case that V is a primitive $GF(p)[G/N]$-module and $F(G/N) = F^*(G/N)$, where F and F^* denote the Fitting and generalized Fitting subgroups. We use a variant of the estimation technique in [**8**, §2] to show that G must be solvable.

In §4 we examine the remaining case that V is primitive and $F(G/N) \neq F^*(G/N)$. We use standard facts about orders, automorphisms, and multipliers of groups of Lie type and a result on permutation groups from §2 to show that $\mathrm{Irr}(G|\lambda)$ contains a character of degree divisible by p. This contradicts condition (6) in Proposition 0 and so completes the proof of Theorem A.

1. This section contains some general lemmas which are useful in working with nonsolvable p-solvable groups.

LEMMA 1.1. *Let p be a prime number and let n be a positive integer. Suppose that neither of the following situations occurs*:

(i) $n = 6$ *and* $p = 2$.

(ii) $n = 2$ *and p is a Mersenne prime.*

Then there is a prime number r such that $r \mid p^n - 1$ and $r \nmid p^m - 1$ for $0 < m < n$. Such a prime number r is called a primitive divisor of $p^n - 1$.

PROOF. See [**8**, Lemma 3.3].

LEMMA 1.2. *Let S be a simple adjoint group of Lie type. Let $d = |Z(G)|$, where G is the universal group of the same type as S. Then*:

(i) $d \,\|\, |S|$.

(ii) *If p is a prime number and $p \nmid |S|$, then $p > d$.*

(iii) *There exists a prime number $r > 3$ such that $r \,\|\, |S|$, $r \nmid d$, and r is greater than the order l of the group of field automorphisms of S.*

PROOF. To prove (i) and (ii) we may assume that $G = A_n(q)$ or $G = {}^2A_n(q)$ (see [**9**, p. 491]). Then $d = (n + 1, q \pm 1)$, and we may assume that $n \geqslant 3$. Since $q^j - 1$ divides $|G|$ whenever j is even and $j \leqslant n + 1$, it follows that $(q^4 - 1)(q^2 - 1)$ divides $|G|$ and $n + 1 \leqslant p - 1$. Then $d^2 \,\|\, |G|$, $d \,\|\, |G/Z(G)|$, and $p > n + 1 \geqslant d$. This proves (i) and (ii).

To prove (iii), write $q = q_0^l$ for a prime number q_0 and a positive integer l. If G is not $A_n(q)$ or ${}^2A_n(q)$, there is an integer $m \geqslant 2$ such that $(q^m + 1) \,\|\, |G|$. If $G = {}^2A_n(q)$, there is an integer $m \geqslant 3$ such that $m \geqslant n$ and $(q^m + 1) \,\|\, |G|$. In either case, let r be a primitive divisor of $q^{2m} - 1 = q_0^{2ml} - 1$, allowing $r = 7$ if $q^{2m} = 2^6$. Then $r \,\|\, |G|$, $2ml \leqslant r - 1$, and $r \geqslant 5$. Then $r \,\|\, |S|$ by (i), and $r > l$, the order of the group of field automorphisms of S. Also $r \geqslant 5 > d$ if $G \not\cong {}^2A_n(q)$ and $r > 2m \geqslant n + 1 \geqslant d$ if $G \cong {}^2A_n(q)$.

Thus, we may assume that $G \cong A_n(q)$, so that $q^{n+1} - 1$ divides $|G|$. If $l(n + 1) \geqslant 3$, let r be a primitive divisor of $q^{n+1} - 1 = q_0^{l(n+1)} - 1$. Then $l(n + 1) \leqslant r - 1$, $r \geqslant 5$, $r > l$, and $r > n + 1 \geqslant d$. If $l(n + 1) \leqslant 3$, then $d \leqslant 3$ and $l \leqslant 3$, so we can let r be any prime greater than 3 which divides $|S|$.

LEMMA 1.3. *Let S be a nonabelian simple group which admits a coprime automorphism of prime order p. Then S is an adjoint group of Lie type, S admits a field automorphism of order p, and* $\mathrm{Out}(S)$ *has a cyclic and central p-Sylow subgroup.*

PROOF. By [**10**, p. 169] the sporadic and alternating groups have no coprime automorphisms. By [**12**] the simple group ${}^2F_4(2)'$ has no coprime automorphism. Thus S is an adjoint group of Lie type. If S is a Suzuki or Ree group then $\mathrm{Aut}(S)$ is generated by the inner and field automorphisms of S (see [**23**, **18**, **19**]). Thus, we may assume that S is not a Suzuki or Ree group. In particular, $p > 3$.

By [**20**, p. 608], we have $D \lhd F \lhd \mathrm{Out}(S)$, where D is the image in $\mathrm{Out}(S)$ of the group of diagonal automorphisms of S, and F is the image in $\mathrm{Out}(S)$ of the group generated by the diagonal and field automorphisms of S. Moreover $|D| = d$, where d is as in Lemma 1.2, and $\mathrm{Out}(S)/F$ is isomorphic to the group of graph automorphisms of S, a $\{2, 3\}$-group.

Since $p > 3$ and $p > d$ by Lemma 1.2(ii), it follows that S admits a field automorphism of order p. Since graph and field automorphisms commute [**10**, p. 169] and since $D \lhd F$ and $p > d$, the rest of Lemma 1.3 follows.

COROLLARY 1.4. *Let S be a nonabelian simple group with Schur multiplier M. Then there is a prime number r such that $r \mid |S|$, $r \nmid |M|$, and $r \nmid |\mathrm{Out}(S)|$.*

PROOF. This is clear if S is sporadic, alternating, or ${}^2F_4(2)'$, since then both M and $\mathrm{Out}(S)$ are $\{2,3\}$-groups.

Otherwise, S is an adjoint group of Lie type. By [**11**, p. 280], any prime divisor of $|M|$ is 2, 3, or a divisor of d. Thus the result follows from Lemma 1.2 and the description of $\mathrm{Out}(S)$ in the proof of Lemma 1.3.

LEMMA 1.5. *Let G be a finite group. Let $F(G)$ and $F^*(G)$ denote the Fitting and generalized Fitting subgroups of G. If L/W is a chief factor of G such that $L = L'$ and $W = Z(L)$ then $L \leqslant F^*(G)$. Conversely, if $F^*(G) \neq F(G)$, then $F^*(G)$ contains a perfect subgroup L such that $L/Z(L)$ is a chief factor of G.*

PROOF. See [**3**, p. 128].

2. In this section we show that the $GF(p)[G/N]$-module V of Proposition 0 must be primitive. We first record several lemmas which will be needed in the proof of Theorem 2.5, the main result of this section.

LEMMA 2.1. *Let G be a nonsolvable group which acts faithfully on a finite vector space V. Suppose G acts transitively on $V - \{0\}$. Then the (unique) nonsolvable composition factor of G is not a Suzuki group.*

PROOF. See the discussion preceding [**13**, Proposition 5.1].

LEMMA 2.2. *Let G be a transitive permutation group on a set Ω of n points, and let $P \in \mathrm{Syl}_p(G)$ for some prime p dividing $|G|$. If P has f fixed points on Ω, then $f \leqslant (n-1)/2$.*

PROOF. This follows from [**14**, Corollary 2].

LEMMA 2.3. *Let G be a primitive permutation group on Ω, with degree n and socle N. Then one of the following occurs*:

(i) *N is elementary abelian of order p^d and regular*; *$n = p^d$ where p is prime.*

(ii) *$N = T_1 \times \cdots \times T_m$, where $T_1, \ldots, T_m$ are isomorphic to a fixed simple group T. Moreover, either*

(a) *T is the socle of a primitive group G_0 of degree n_0 and $G \leqslant G_0 \operatorname{Wr} S_m$ (with the product action), where $n = n_0^m$, or*

(b) *$m = kl$ and $n = |T|^{(k-1)l}$. The permutation group induced by G on $\{T_1, \ldots, T_m\}$ has $\{T_1, \ldots, T_k\}$ as a block of imprimitivity. The group induced on the set of blocks is transitive.*

PROOF. See Theorem 4.1 and Remark 2 following Theorem 4.1 in [**4**]. In (ii)(a) the statement that $G_0 \operatorname{Wr} S_m$ acts with the product action means that $G_0 \operatorname{Wr} S_m$ acts on $\Omega = \Omega_0^m$, where $|\Omega_0| = n_0$. The base group of the wreath product acts componentwise on Ω_0^m, while S_m acts by permuting coordinates. See [**4**, p. 5] for a formal definition of "product action".

The following impressive result does not depend on the classification of simple groups.

LEMMA 2.4. *Let G be a uniprimitive permutation group of degree n. Then*

$$|G| < \exp\left(4\sqrt{n}\log^2 n\right).$$

PROOF. This is [**2**, Corollary 3.3].

Another important ingredient in the proof of Theorem 2.5 will be the lower bounds found by Landazuri and Seitz for the smallest degree of a nontrivial projective representation of a simple group of Lie type. Their results are tabulated in [**17**, p. 419]. We will not reproduce their table here, except to note a misprint; the bound for $PSO(2n+1, q)'$, $q > 5$, should read $q^{2(n-1)} - 1$, as in [**17**, Lemma 3.3].

DEFINITION. In this paper J denotes the affine semilinear group over $GF(8)$. Thus J is a solvable group of order 168, which acts 2-transitively on 8 points.

THEOREM 2.5. *Let G be a transitive permutation group on a finite set Ω. Suppose $|G : O_{p'}(G)| = p$ and $G = O^{p'}(G)$ for an odd prime p. Suppose each subset of Ω is stabilized by an element of order p in G. Then $p = 3$, $|\Omega| = 8$, and $G \cong J$.*

PROOF. Let G be a counterexample to the theorem. The proof will be carried out in a series of steps.

Step 1. G is primitive on Ω.

PROOF. We write Ω as a disjoint union of blocks so that G acts as a primitive group on the set of blocks. We may assume that each block contains more than one point.

By induction on $|\Omega|$, the conclusion of the theorem is valid for the action of G on the set of blocks. Thus $p = 3$, we may write $\Omega = B_1 \cup \cdots \cup B_8$, and G acts as J on the set of blocks. Choose $\Delta \leqslant \Omega$ to consist of 2 points from B_1, one point from B_2, and one point from B_3. Any element of order 3 in G which stabilizes Δ must stabilize B_1, B_2 and B_3. This contradicts the fact that elements of order 3 in J have only two fixed points in the action of J on 8 points.

Step 2. Let $|\Omega| = n$. Then:

(i) $2^{n/3} < |\mathrm{Syl}_p(G)|$.

(ii) $2^{.4n} < |\mathrm{Syl}_p(G)|$ if $p > 3$.

(iii) If G is not 2-transitive on Ω, then $n \leqslant 10^8$.

PROOF. By Lemma 2.2, an element of order p in G fixes less than $n/2$ points of Ω. Thus, an element of order p in G has at most $2n/3$ cycles on Ω if $p = 3$ and at most $.6n$ cycles on Ω if $p > 3$. It follows that the number of ordered pairs $(\langle g \rangle, \Delta)$, such that $\langle g \rangle \in \mathrm{Syl}_p(G)$, $\Delta \leqslant \Omega$, and g fixes Δ, is at most $2^{2n/3}|\mathrm{Syl}_p(G)|$ if $p = 3$ and at most $2^{.6n}|\mathrm{Syl}_p(G)|$ if $p > 3$. Since the number of such ordered pairs must exceed the number of subsets of Ω, parts (i) and (ii) follow.

If G is not 2-transitive, then part (i) and Lemma 2.4 imply (iii).

Step 3. G does not have an elementary abelian regular normal subgroup.

PROOF. Assume first that G is not solvable. Let $n = q^m$ for a prime number q. Since $|GL(m, q)| < q^{m^2}$, Step 2 yields $2^{q^m/3} < q^{m^2+m}$, or

$$(*) \qquad (\log 2/3)q^m < (m^2 + m)\log q.$$

Since G is nonsolvable, $m \geqslant 2$, and it is easy to see that $(*)$ holds only if q^m is 3^2, 3^3, 3^4, 5^2, 7^2 or 2^m for some $m \leqslant 7$. In none of these cases is $|GL(m, q)|$ divisible by the cube of the order of a simple group or by the order of a simple group which admits a coprime automorphism. Thus $G = O^{p'}(G)$ can't have a nonsolvable chief factor.

Hence G is solvable and [**8**, Lemma 3.1] implies that $p = 3$, $n = 8$ and $G \cong J$.

Step 4. G has a simple socle.

We adopt the notation of Lemma 2.3. Assume G does not have a simple socle. By Step 3, G falls under case (ii)(a) of Lemma 2.3 for $m > 1$, or under case (ii)(b) of Lemma 2.3.

Suppose first that G falls under case (ii)(a) with $m > 1$. Let Ω_0 be the set permuted by G_0, so that Ω may be identified with the cartesian product Ω_0^m. Let α and β be distinct points in Ω_0. For $\Delta \leqslant \{1, 2, \ldots, m\}$, define $\omega \in \Omega$ by the condition that $\omega_i = \alpha$ for $i \in \Delta$ and $\omega_i = \beta$ for $i \notin \Delta$. Define $\eta \in \Omega$ by the condition that $\eta_i = \alpha$ for all $i \leqslant m$. Choose $x \in G$ such that x has order p and x stabilizes the subset $\{\omega, \eta\}$ of Ω. Then x must stabilize Δ in its action on $\{1, 2, \ldots, m\}$.

Since G acts transitively on $\{T_1, \ldots, T_m\}$, the action of G on $\{T_1, \ldots, T_m\}$ satisfies the hypotheses of Theorem 2.5. By induction on n, it follows that $m = 8$ and $p = 3$. Thus T is a Suzuki group. The classification of the maximal subgroups of the Suzuki groups [**23**, Theorem 9] yields that $n_0 \geqslant 8^2 + 1 = 65$. Thus $n > 10^8$, contradicting Step 2(iii).

Next suppose (ii)(b) of Lemma 2.3 holds. It is possible that T admits a coprime automorphism of order p. In this case $|T| \geqslant |\mathrm{Sz}(8)| = 29{,}120$ and $|T|^2 > 10^8$. By Step 2, $n = |T|^{(k-1)l} < 10^8$, so $k = 2$, $l = 1$, and $\mathrm{Soc}(G) = T_1 \times T_2$. Then $G \leqslant O^{p'}(\mathrm{Aut}(T_1 \times T_2)) \leqslant \mathrm{Aut}\, T_1 \times \mathrm{Aut}\, T_2$. Since $O^{p'}(G) = G$, Lemma 1.3 implies that $|G| = p|T|^2$ and $|\mathrm{Syl}_p(G)| < |T|^2$. Since $|T| \geqslant 29{,}120$, this contradicts Step 2(i).

Thus we assume that T does not admit a coprime automorphism of order p. If $l > 1$, our assumption that $O^{p'}(G) = G$ implies that an element of order p in G permutes the l blocks $T_1 \times \cdots \times T_k, \ldots, T_{k(l-1)+1} \times \cdots \times T_{kl}$ nontrivially. Hence $l \geqslant p$. If $l = 1$, an element of order p in G permutes $\{T_1, \ldots, T_k\}$ nontrivially, since $O^{p'}(G) = G$ and T does not admit a coprime automorphism of order p. Hence $k \geqslant p$. In either case $(k-1)l \geqslant p - 1$.

If $p \geqslant 7$, then $n = |T|^{(k-1)l} \geqslant 60^6 > 10^8$. If $p = 5$, then $|T| \neq 60$ and so $n = |T|^{(k-1)l} \geqslant |T|^4 > 10^8$. If $p = 3$, then $|T| \geqslant |\mathrm{Sz}(8)| = 29{,}120$ and $n = |T|^{(k-1)l} \geqslant |T|^2 > 10^8$. Hence, $n > 10^8$ and we are done by Step 2(iii).

Step 5. Conclusion.

By Lemmas 2.3 and 1.2, $|G| = p|T|$ and T admits a field automorphism of order p.

First suppose $T = \mathrm{Sz}(q)$ for an odd power q of 2. Let $\alpha \in \Omega$. Then $n = |G : G_\alpha| = |T : T_\alpha|$. By [**23**, Theorem 9], $n = |T : T_\alpha| \geqslant q^2 + 1$, so Step 2(i) yields a contradiction. Hence, for the rest of this step we suppose $T \neq \mathrm{Sz}(q)$ and, in particular, $p > 3$.

Let $L(T)$ be the lower bound for the smallest degree of a nontrivial projective representation of T given in [**17**, p. 419]. Thus in the notation of [**17**], $L(T) \leqslant l(T, p)$ and $L(T)$ is the number which actually appears in the table in [**17**, p. 419]. Let $T = \mathbf{G}(q)$ be an adjoint group of type $\mathbf{G}$ over the field of q elements. Since $p > 3$,

$q \geqslant 32$ and $q \geqslant 243$ if T has type ${}^2G_2$. If $\mathbf{G}$ is of exceptional Lie type then $L(T) \geqslant 10^4$ and $|T| \leqslant L(T)^{10}$. Thus $2^{.4L(T)} > |T|$, which contradicts Step 2(ii).

Hence, T is a classical group. If T is of type A_m, B_m, C_m, D_m, ${}^2A_m$ or ${}^2D_m$ for $m \geqslant 2$, then it is immediate from [**17**, p. 419] that $n > L(T) \geqslant (q^m - 1)/2 > 500$. As $q \geqslant 32$, this implies that $\log(2n) > m \log q > 3m$. By the order formulas,

$$|T| \leqslant |B_m(q)| \leqslant q^{4m^2} = (q^m)^{4m} \leqslant (3n)^{4m} \leqslant 3n^{2\log(3n)}.$$

By Step 2, $|T| > 2^{.4n}$. Thus $3n^{2\log(3n)} > 2^{.4n}$, contradicting $n > 500$.

Thus $T = PSL(2, q)$. If q is odd then $q \geqslant 243$ and $2^{.4L(T)} > |T|$. If q is even then $2^{.4L(T)} = 2^{.4(q-1)} > |T|$ for $q > 32$. Thus $T = SL_2(32)$. Since G is primitive on Ω, $T \lhd G$ is transitive on Ω. If T were not doubly transitive on Ω, then $n > 2(q-1) > 60$. Since $2^{.4(60)} > |T|$, T must be doubly transitive on Ω. By [**4**, Theorem 5.3], $n = 33$.

Now let $x \in G = \mathrm{Aut}(SL_2(32))$ have order $p = 5$. Since $5 \nmid |T|$ and T is transitive on Ω, it follows from [**16**, Lemma 13.8] that the fixed points of x in Ω form a single orbit under $C_T(x) \cong S_3$. Since the number of fixed points of x is congruent to $3 \bmod 5$, x has 3 fixed points in Ω. Then no set of size 4 in Ω is stabilized by an element of order 5 in G. This contradiction completes the proof of Theorem 2.5.

COROLLARY 2.6. *Suppose $|G : O_{p'}(G)| = p$ and $G = O^{p'}(G)$ for an odd prime p. Suppose G acts faithfully and imprimitively on a finite vector space V of characteristic p so that each $v \in V$ is centralized by a p-Sylow subgroup of G. Then G is solvable.*

PROOF. Let $V = V_1 \oplus \cdots \oplus V_n$ be an imprimitivity decomposition for the action of G. Let G_1 be the stabilizer in G of V_1 and let $C = \mathrm{Core}_G(G_1)$. Let $\Omega = \{1, 2, \ldots, n\}$. Let $\Delta \leqslant \Omega$. By choosing a vector whose nonzero components correspond to Δ, we see that $(G/C, \Omega)$ satisfies the hypotheses of Theorem 2.5. As in [**8**, Lemma 3.2] C acts transitively on $V_1 - \{0\}$. By Lemma 2.1, C is solvable. Thus G is solvable.

3. Let G and N be as in Proposition 0. Suppose that $F^*(G/N) = F(G/N)$. Theorem 3.1 below shows that G must be solvable. The groups G and K below correspond to G/N and K/N in Proposition 0.

THEOREM 3.1. *Let $|G : O_{p'}(G)| = p$ and $G = O^{p'}(G)$ for an odd prime p. Suppose that V is a faithful irreducible primitive $GF(p)[G]$-module. Suppose $p \,||\, C_G(x)|$ for all $x \in V$. If $F^*(G) = F(G)$, then G is solvable.*

PROOF. Let $K = G'$. The hypotheses imply that K is the unique maximal normal subgroup of G. The proof is carried out in a series of steps.

Step 1. There is a unique maximal normal abelian subgroup Z of G. Furthermore, Z is cyclic and $Z = Z(K)$.

Proof. As in Step 2 of [**8**, Theorem 2.3].

Step 2. Let E/Z be a chief factor of G, let $B = C_G(E)$ and let $C = C_G(E/Z)$. Then:

(i) E/Z is an elementary abelian q-group for a prime q and $E \leqslant K$.

(ii) $BE = C \leqslant K$ and $B \cap E = Z$.

(iii) $|E/Z| = q^{2n}$ for an integer n.

(iv) K/C is isomorphic to a subgroup of the symplectic group $\mathrm{Sp}(2n, q)$.

(v) If $P \leqslant C_G(Z)$, then G/C is isomorphic to a subgroup of $\mathrm{Sp}(2n, q)$.

PROOF. If $Z = K$, the conclusion of the theorem is satisfied, so we assume $Z < K$. Since K is the unique maximal normal subgroup of G, $E \leqslant K$. Since E/Z is a chief factor of G and $Z \leqslant Z(K)$, E is nilpotent or E/Z is a direct sum of isomorphic nonabelian simple groups. In either case $E \leqslant F^*(G)$ by Lemma 1.5. The hypotheses and Step 1 yield that E is nilpotent but nonabelian. The rest of the proof follows that of Step 4 in [**8**, Theorem 2.3].

Step 3. There exist $E_1, \ldots, E_m \leqslant G$ such that:

(i) E_i/Z is a chief factor of G for each i.

(ii) $[E_i, E_j] = 1$ when $i \neq j$.

(iii) $M/Z = E_1/Z \times \cdots \times E_m/Z$, where M is defined to be $E_1 E_2 \cdots E_m$.

(iv) $C_G(M) = Z$ and $C_{G/Z}(M/Z) = M/Z$.

PROOF. As in Step 6 of [**24**, Theorem 3.3]. We remark that $M = F(G)$.

Step 4. Let $W \neq 0$ be an irreducible Z-submodule of V and let $e = |M : Z|^{1/2}$. Then $\dim V = te(\dim W)$ for an integer t.

PROOF. As in Step 6 of [**8**, Theorem 2.3].

Step 5. Let W be as in Step 4 and let q_i be the prime divisor of E_i/Z. Then:

(i) $|Z| \mid (|W| - 1)$.

(ii) $q_i \mid (|W| - 1)$ for each i.

PROOF. As in Step 14 of [**24**, Theorem 3.3].

Step 6. $|E/Z| = 4$ if and only if $C = K$. In this situation, $p = 3$.

PROOF. As in Step 7 of [**24**, Theorem 3.3].

Step 7. Assume that $|E/Z| \neq 4$. Let $P \in \mathrm{Syl}_p(G)$. Then:

(i) If s is a prime divisor of $|F(G/C)|$, then $s \mid q^{2n} - 1$.

(ii) If $1 \neq S \in \mathrm{Syl}_s(F(G/C))$ and if $C_S(P) = 1$, then $\dim C_{E/Z}(P) = 2n/p$.

(iii) If G/C is solvable, then $1 \neq C_{G/C}(F(G/C)) \leqslant F(G/C) \leqslant K/C$.

(iv) If $F(G/C)$ is cyclic and G/C is solvable, then $F(G/C) = K/C$ and $\dim C_{E/Z}(P) = 2n/p$.

PROOF. As in Step 11 of [**24**, Theorem 3.3].

Step 8. Let $P \in \mathrm{Syl}_p(G)$. Then:

(i) $|\mathrm{Syl}_p(G)||C_V(P)| \geqslant |V|$.

(ii) $|\mathrm{Syl}_p(G)| > |V|^{1/2}$.

PROOF. As in Step 7 of [**8**, Theorem 2.3]. Note that we may replace the $\geqslant$ sign in (ii) by a $>$ sign, since $|V|^{1/2}$ is not a p'-integer.

Step 9. Let $q = 2, p = 3, n \neq 1$. Then:

(i) $n \geqslant 6$.

(ii) If $n \leqslant 7$ and K/C is nonsolvable, then $|K/C| \leqslant 2^{28}$.

PROOF. We first assume that K/C is solvable. Suppose that $n = 5$. Since $p = 3$ and $|\mathrm{Sp}(10, 2)| = 3^6 \cdot 5^2 \cdot 7 \cdot 11 \cdot 17 \cdot 31 \cdot 2^{25}$, it follows from Steps 2(iv) and 7(i),(iv) that $|F(G/C)| \mid 11 \cdot 31$ and $3 \mid 10$. Thus, $n \neq 5$ and similarly, $n \neq 2$. If $n = 4$, then $|F(G/C)| \mid 5^2 \cdot 17$ by Steps 2(iv) and 7(i). Since $C_{G/C}(F(G/C)) \leqslant K/C$, a 3-Sylow subgroup of G must act nontrivially on the 5-Sylow subgroup of $F(G/C)$. Then Step

7(iii) yields a contradiction. Thus $n \neq 4$. If $n = 3$, then Step 7 yields that $F(G/C) = K/C$ is cyclic of order 7 and G/C is a Frobenius group of order 21. It is easy to see that G/C has exactly two nonisomorphic faithful irreducible representations over $GF(2)$, both of degree 3. Thus, E/Z is not an irreducible G/C-module and not a chief factor of G, a contradiction.

Thus, we may assume that K/C is nonsolvable and $2 \leqslant n \leqslant 7$. There exists an integer d, and a chief factor R/T of G/C such that R/T is isomorphic to the direct product of d copies of a nonabelian simple group. Since $|K/C|$ divides $|\mathrm{Sp}(14,2)|$ and $3 \nmid |K/C|$, it follows that $|K/C|$ divides $2^{49} \cdot 5^3 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 43 \cdot 127$. Hence, $d \leqslant 2$ and since $O^{3'}(G/C) = G/C$ we have $d = 1$. Hence R/T is isomorphic to a Suzuki group which admits an automorphism of order 3. By the order formulas for the Suzuki groups and the bound on $|K/C|$ above, it follows that $R/T \cong \mathrm{Sz}(8)$ and K/R and T/C are both solvable. Since $|\mathrm{Out}(\mathrm{Sz}(8))| = 3$, we may replace R and T by K and $C_G(R/T)$, respectively, so that $K/T \cong \mathrm{Sz}(8)$ and T/C is solvable.

Since $13 \nmid |\mathrm{Sp}(2n,2)|$ for $n \leqslant 5$, it follows that $n \geqslant 6$. By the preceding paragraph T/C divides $2^{43} \cdot 5^2 \cdot 7 \cdot 11 \cdot 17 \cdot 31 \cdot 43 \cdot 127$. By Step 7(i), $|F(T/C)|$ divides $5^2 \cdot 7$ if $n = 6$ and $|F(T/C)|$ divides $43 \cdot 127$ if $n = 7$. A cyclic Sylow subgroup of $F(T/C)$ is central in $(G/C)' = K/C$ and in T/C. Since $C_{T/C}F(T/C) = F(T/C)$, it follows that $|T/C|$ divides $2^3 \cdot 5^2 \cdot 7$ if $n = 6$ and $|T/C|$ divides $43 \cdot 127$ if $n = 7$. In either case $|T/C| \leqslant 2^{13}$ and so $|K/C| = |\mathrm{Sz}(8)||T/C| \leqslant 2^{28}$.

Step 10. Let $q = 2, p \neq 3$ and $n \neq 1$. Then:

(i) $n \geqslant 4$.

(ii) If $n = 4$, then K/C is solvable.

(iii) If $n = 5$ and K/C is nonsolvable, then $p = 5$ and $K/C \cong SL_2(32)$.

PROOF. First suppose that $n = 3$. Since $|K/C|$ divides $|\mathrm{Sp}(6,2)| = 2^9 \cdot 3^4 \cdot 5 \cdot 7$, the order formulas [**9**, p. 491] and Lemma 1.2 show that K/C involves no simple group which admits a coprime automorphism. Since $G = O^{p'}(G)$, it follows that K/C has no nonabelian simple chief factor. As $G = O^{p'}(G)$ and $|K/C|$ is not divisible by the fifth power of the order of a nonabelian simple group, every chief factor of K/C must be solvable, so K/C is solvable. As $p \,\|\, |\mathrm{Aut}(E/Z)|$ and $p \neq 3$, p must be 5, 7 or 31. By Step 7(i),(iii), $O_3(G/C)$ is elementary abelian of order 3^4 and $p = 5$. Hence, an element of order p in G has no fixed points on $O_3(G/C)$. By Step 7(ii), $5 \mid 6$, a contradiction. Thus $n \neq 3$. Similarly $n \neq 2$.

If $n = 4$, the arguments of the preceding paragraph show that K/C is solvable. If $n = 5$, the arguments of the preceding paragraph show that K/C is solvable or that a composition series for K/C has a unique nonsolvable factor, which is isomorphic to $SL_2(32)$.

Thus, we may assume that $n = 5$, $p = 5$, and K/C has a unique nonsolvable composition factor, isomorphic to $SL_2(32)$. If $F(G/C) = 1$, then $F^*(G/C) \cong SL_2(32)$. Since $C_{G/C}(F^*(G/C)) \leqslant F^*(G/C)$, by [**3**, Theorem 13.12], it follows that $G/C \cong \mathrm{Aut}(SL_2(32))$ and $K/C \cong SL_2(32)$.

We may assume that $F(G/C) \neq 1$. Under this assumption we will show that K/C acts faithfully on an extraspecial group of order 2^{11}.

Since E/Z is elementary abelian and $Z \leqslant Z(E)$, each commutator of E has order 2 and $|E'| = 2$. An application of Fitting's lemma to the coprime action of $F(G/C)$ on $O_2(E)/E'$ yields that $E/E' = (E_0/E') \times (Z/E')$ for some $E_0 \lhd G$. Since E/Z is chief and E is nonabelian, $E' = Z(E_0) = \Phi(E_0)$. Since $|E'| = 2$, E_0 is extraspecial of order 2^{11} and K/C acts faithfully on E_0.

By [**15**, p. 357], K/C is isomorphic to a subgroup of one of the two orthogonal groups $O^+(10,2)$ or $O^-(10,2)$. By [**15**, p. 248], neither $|O^+(10,2)|$ nor $|O^-(10,2)|$ is divisible by $|SL_2(32)|$. Thus K/C has no nonsolvable composition factor, completing the proof of this step.

Step 11. If q^n is 5, 7, 11, 3^2 or 3^3, then K/C is solvable. Also $q^n \neq 3$.

PROOF. Suppose that q^n is 5, 7, 11, 3^2 or 3^3 and K/C is nonsolvable. Our assumption that $O^{p'}(G) = G$ implies that K/C involves a simple group which admits a coprime automorphism of order $p \neq q$, or that $|K/C|$ is divisible by the pth power of the order of a nonabelian simple group. Since K/C is subgroup of $\mathrm{Sp}(2n, q)$, the order formulas [**9**, p. 491] yield a contradiction.

If $q^n = 3$, then $|\mathrm{Aut}(E/Z) = 48$. Since p divides $|\mathrm{Aut}(E/Z)|$, this contradicts the hypothesis that $p \neq 2$ and $p \nmid |K|$.

Step 12. Conclusion.

We may choose an integer $k \geqslant 0$ such that $|E_i/Z| = 4$ if and only if $i \leqslant k$. We let $C_0 = K$ and define C_i to be the centralizer in C_{i-1} of E_i/Z, for $1 \leqslant i \leqslant m$. By Step 2(iv) applied to E_i/Z, C_{i-1}/C_i is isomorphic to a subgroup of $\mathrm{Sp}(2n_i, q_i)$ for each i. By Steps 6 and 3, $C_k = K$ and $C_m = M$. Since $|\mathrm{Sp}(2n, q)| < q^{2n^2+n}$, we have $|\mathrm{Syl}_p(G)| \leqslant |K|$ and

$$\log\bigl(|\mathrm{Syl}_p(G)|\bigr) \leqslant \log|Z| + 2k\log 2 + \sum_{i=k+1}^{m} \bigl(2n_i^2 + 3n_i\bigr)\log q_i. \tag{1}$$

By Steps 4 and 8, we have

$$\log\bigl(|\mathrm{Syl}_p(G)|\bigr) > t2^{k-1}\left(\prod_{i=k+1}^{m} q_i^{n_i}\right)\log|W|. \tag{2}$$

By Step 5, $q_i \leqslant |Z| < |W|$ for all i and thus

$$2k\log 2 + \sum_{i=k+1}^{m} \bigl(2n_i^2 + 3n_i\bigr)\log q_i > \left(-1 + 2^{k-1}\prod_{i=k+1}^{m} q_i^{n_i}\right)\log|W| \tag{3}$$

and

$$1 + 2k + \sum_{i=k+1}^{m} \bigl(2n_i^2 + 3n_i\bigr) > 2^{k-1}\prod_{i=k+1}^{m} q_i^{n_i}. \tag{4}$$

We let $l = \Sigma_{k+1}^{m} n_i$, so that (4) yields $1 + 2k + 2l^2 + 3l > 2^{k+l-1}$ and hence $k + l \leqslant 8$. If $l = 0$, then $K = C_m = M$ and G is solvable. We may assume that $l \geqslant 1$.

Suppose first that $n_{k+1} = 1$. By Step 11, $q_{k+1} \geqslant 5$. Then (4) yields

$$6 + 2k + 2(l-1)^2 + 3(l-1) > 2^{k-1} \cdot 5 \cdot 3^{l-1}.$$

Hence $l \leqslant 2$. If $l = 2$, then $q_{k+2} \geqslant 5$ by Step 11, and (4) gives the contradiction $11 + 2k > 2^{k-1}5^2$. Thus $l = 1$ and $q_{k+1} = 5$, 7 or 11 by (4). Since $C_K = K$ and

$C_{k+1} = M$, it follows from Step 11 that G is solvable. We may assume that $n_i \geqslant 2$ for all $i > k$.

Suppose $n_{k+1} = 2$, so that $q_{k+1} \geqslant 3$ by Step 10. Now (4) becomes

$$15 + 2k + 2(l-2)^2 + 3(l-2) > 2^{k-1} \cdot 3^2 \cdot 2^{l-2}$$

and $l \leqslant 5$. But then Step 10 yields that $q_i \geqslant 3$ for $i > k+1$ and (4) implies that

$$15 + 2k + 2(l-2)^2 + 3(l-2) > 2^{k-1} \cdot 3^l$$

and $l \leqslant 3$. By the last paragraph $l = 2$. Then q_{k+1} is 3 or 5 by inequality (4). If $q_{k+1} = 5$, then (3) and (4) yield that $k = 0$ and $5^{14} > |W|^{23/2}$, whence $|W| < 11$, contradicting Step 5. Thus $q_{k+1} = 3$. Since $C_k = K$ and $C_{k+1} = M$, Step 11 implies that K/C and G are solvable. We may assume that $n_i \geqslant 3$ for all $i > k$.

Suppose that $n_{k+1} = 3$, so that $q_{k+1} \geqslant 3$ by Step 10. Inequality (4) yields that

$$28 + 2k + 2(l-3)^2 + 3(l-3) > 2^{k-1} \cdot 3^3 \cdot 2^{l-3}$$

and that $l < 6$. By the last paragraph $l = 3$. Then $28 + 2k > 2^{k-1} q_{k+1}^3$ by (4). Hence $q_{k+1} = 3$ and $k \leqslant 1$. Since $C_k = K$ and $C_{k+1} = M$, Step 11 implies that K/C and G are solvable. Hence $n_i \geqslant 4$ for all $i > k$.

Suppose $n_{k+1} = 4$. Then

$$45 + 2k + 2(l-4)^2 + 3(l-4) > 2^{k-1} q_{k+1}^4 2^{l-4}$$

by (4) and $l < 8$. By the last paragraph $l = 4$. Then $q = 2$ or 3 and $k = 0$ if $q = 3$. If $q = 3$, then inequality (3) becomes $3^{44} > |W|^{79/2}$, contradicting Step 5. Hence $q = 2$, and K/M and G are solvable. Hence $n_i \geqslant 5$ for all $i > k$.

Now $m = k+1$, since $k < k + l \leqslant 8$. If $n_{k+1} = 8$, then $k = 0$ and $q_1 = 2$ by (4). Inequality (3) becomes $2^{152} > |W|^{127}$, contradicting Step 5. Thus $5 \leqslant n_{k+1} \leqslant 7$.

Suppose $n_{k+1} = 6$. By (4), $k \leqslant 1$. If $k = 1$, then $q_{k+1} = 2$ and (3) implies that $2^{92} > |W|^{63}$, a contradiction. Thus $k = 0$ and (3) becomes $2^{90} > |W|^{31}$. Since $|W|$ is a power of p, it follows that $|W| = p$ and p is 3, 5 or 7. Since $|Z| < |W| = p$, we have $P \leqslant C_G(Z)$. By Step 2, $|K/M|$ divides $|\mathrm{Sp}(12,2)|$ and thus $|K/Z| \,|\, 2^{48} \cdot 3^8 \cdot 5^3 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 31$. If p is 5 or 7, then P must fix and centralize an r-Sylow subgroup of K/Z, whenever r is 5, 7, 13 or 17. Thus

$$|\mathrm{Syl}_p(G)| = |K/Z : C_{K/Z}(P)| \leqslant 2^{48} \cdot 3^8 \cdot 11 \cdot 31 \leqslant 2^{70}.$$

Inequality (2) now has $2^{70} > |W|^{32}$ and so $|W| < 5$, a contradiction. Thus $p = 3 = |W|$. By Step 9, $|\mathrm{Syl}_3(G)| \leqslant |K/Z| \leqslant 2^{40}$ and inequality (2) yields $2^{40} > 3^{32}$, a contradiction. Hence $n_{k+1} \neq 6$. Similarly $n_{k+1} \neq 7$.

Thus $n_{k+1} = 5$ and $q_{k+1} = 2$. By Steps 9 and 10, we may assume that $p = 5$ and $K/M \cong SL_2(32)$. Since $|K/M| < 2^{15}$, a modification of the argument used to derive inequality (3) shows that

$$2k(\log 2) + 25 \log 2 > (-1 + 16 \cdot 2^k) \log |W|.$$

This contradicts the fact that $|W| \geqslant p = 5$ and completes the proof of the theorem.

4. In this section we consider the case that V is a primitive $GF(p)[G/N]$-module and $F^*(G/N) \neq F(G/N)$. The group G in the statements of Propositions 4.1 and 4.2 corresponds to $G/O_p(N)$ in the setting of Proposition 0.

PROPOSITION 4.1. *Let $G = O^{p'}(G)$ and $|G : O_{p'}(G)| = p$ for an odd prime p. Suppose that L/W is a nonabelian simple chief factor of G. Suppose that $\mu \in \mathrm{Irr}(W)$ is invariant in G. Then some character in $\mathrm{Irr}(G|\mu)$ has degree divisible by p.*

PROOF. By applying a character triple isomorphism [**16**, Theorem 11.28] we may suppose that μ is linear and faithful, so that $W \leqslant Z(G)$. We must produce $\chi \in \mathrm{Irr}(L|\mu)$ such that $p \nmid |I_G(\chi)|$. We will do this in a series of steps.

Step 1. We may assume that $L = L'$.

PROOF. Since $(L/W)' = L/W$, we have $L = L'W$ and $L'/L' \cap W \cong L/W$. Suppose there were a character $\chi' \in \mathrm{Irr}(L'|\mu_{L'\cap W})$ such that $p \nmid |I_G(\chi')|$. Then $L = L'W \leqslant I_G(\chi')$, and since $L/L' \cong W/L' \cap W$ is cyclic, there exists $\chi_1 \in \mathrm{Irr}(L)$ which extends χ'. Since $\chi_1|_W$ extends $\chi'(1)\mu_{L'\cap W}$, we may choose a linear character ν of $L/L' \cong W/L' \cap W$ so that $\chi_1\nu \in \mathrm{Irr}(L|\mu)$. Set $\chi = \chi_1\nu$. Then χ extends χ', $\chi \in \mathrm{Irr}(L|\mu)$, and $I_G(\chi) \leqslant I_G(\chi')$. Thus $p \nmid |I_G(\chi)|$.

Step 2. L/W is an adjoint group of Lie type.

PROOF. This follows from $G = O^{p'}(G)$ and Lemma 1.3.

Step 3. There is an automorphism σ of L/W and a prime number r such that $|\sigma| = p$, $r \nmid |W|$, $r \,||\, |L|$, and $r \nmid |C_{L/W}(\sigma)|$.

PROOF. By Step 2, L/W is an adjoint group over $GF(q^p)$ where q is a prime power; of course, q is not a power of p. Let $\mathbf{G}(q^p)$ be the simply connected group of the same type, so that $\mathbf{G}(q^p)$ is a central extension of L/W. Then there is a simply connected and simple (in the sense of algebraic groups) algebraic group $\mathbf{G}$ and an endomorphism σ of $\mathbf{G}$ such that $\mathbf{G}_\sigma$, the fixed point group, is $\mathbf{G}(q)$ (see [**22**, pp. 82–83]). Let $\tau = \sigma^p$. Then $\mathbf{G}_\tau$ is finite [**21**, 10.6] and $\mathbf{G}_\tau = \mathbf{G}(q^p)$ by [**21**, 11.16, 11.13]. Moreover, $\mathbf{G}_\tau$ admits σ and the restriction of σ to $\mathbf{G}_\tau$ has order p. Let $d_\tau = d(q^p) = |Z(\mathbf{G}_\tau)|$. By Lemma 1.2, $d_\tau \,||\, \mathbf{G}_\tau/Z(\mathbf{G}_\tau)|$, so $p \nmid |\mathbf{G}_\tau|$. Consequently, $C_{\mathbf{G}_\tau/Z(\mathbf{G}_\tau)}(\sigma) \cong \mathbf{G}_\sigma/\mathbf{G}_\sigma \cap Z(\mathbf{G}_\tau)$ and σ induces an automorphism of order p on $\mathbf{G}_\tau/Z(\mathbf{G}_\tau) \cong L/W$.

By the order formulas [**2**, 11.16], $|\mathbf{G}(q^p)|$ has the form $(q^p)^N \prod_{j \geqslant 1}(q^{pm_j} - \varepsilon_j)$ where each ε_j is a root of 1 of order 1, 2 or 3. Choose notation so that $m_1 \geqslant m_2 \geqslant \cdots$. If $\mathbf{G}$ is untwisted let r be a primitive divisor of $q^{pm_1} - 1$. If $\mathbf{G}$ is of type ${}^2B_2$, ${}^2D_n$, ${}^3D_4$, ${}^2G_2$, ${}^2F_4$, ${}^2E_6$, let r be a primitive divisor of $q^{4p} - 1$, $q^{2np} - 1$, $q^{12p} - 1$, $q^{6p} - 1$, $q^{12p} - 1$, $q^{18p} - 1$, respectively. If $\mathbf{G}$ is of type ${}^2A_n$, let r be a primitive divisor of $q^{2p(n+1)} - 1$ if n is even and $q^{2np} - 1$ if n is odd. Since $p \geqslant 3$, the exceptional cases $2^6 - 1$ and $p^2 - 1$ in Lemma 1.1 do not arise. Also $r > 3$.

By the order formulas, $r \,||\, \mathbf{G}(q^p)|$ and $r \nmid d(q^p)$. Hence $r \,||\, L/W|$. Let M be the Schur multiplier of $\mathbf{G}(q^p)$. By [**11**, p. 280], any prime greater than 3 which divides $|M|$ must divide $d(q^p)$. Since $r \nmid d(q^p)$ and $L = L'$ it follows that $r \nmid |W|$.

Finally, we show that $r \nmid |C_{L/W}(\sigma)|$. Note that $|C_{L/W}(\sigma)| \,||\, \mathbf{G}(q)|$ and $|\mathbf{G}(q)|$ has the form $q^N \prod_{j \geqslant 1}(q^{m_j} - \varepsilon_j)$. If $\mathbf{G}$ is untwisted, the definition of r makes it clear that $r \nmid |\mathbf{G}(q)|$. If $\mathbf{G}$ has type ${}^3D_4$, then any prime divisor of $|\mathbf{G}(q)|$ divides $q^{12} - 1$, so

$r \nmid |\mathbf{G}(q)|$. The verification for the other twisted types is equally trivial and is omitted.

Step 4. Let r be as in Step 3 and let $\alpha \in \mathrm{Aut}(L/W)$ we have order p. Then $r \nmid |C_{L/W}(\alpha)|$.

Proof. Let σ be as in Step 3. By Lemma 1.3 and Sylow's theorem, $\langle \sigma \rangle$ and $\langle \alpha \rangle$ are conjugate in $\mathrm{Aut}(L/W)$. Thus $r \nmid |C_{L/W}(\alpha)|$.

Step 5. Any two elements of order p in G fix the same irreducible characters of L.

PROOF. Let $g_1, g_2 \in G$ have order p. We may assume that $g_1 g_2^{-1} \in O^p(G)$. By Lemma 1.3, $g_1 g_2^{-1}$ induces an inner automorphism of L/W. Hence we may choose $x \in L$ so that $g_1 g_2^{-1} x$ centralizes L/W. Since $W \leqslant Z(G)$, $g_1 g_2^{-1} x$ also centralizes W. Therefore $[g_1 g_2^{-1} x, L, L] = [L, g_1 g_2^{-1} x, L] = 1$. The three subgroup lemma yields $1 = [L, L, g_1 g_2^{-1} x] = [L, g_1 g_2^{-1} x]$ so $g_1 g_2^{-1} x$ centralizes L. Hence $g_1 g_2^{-1}$ induces an inner automorphism of L, and the result follows.

Step 6. Let $g \in G$ be a fixed element of order p. Let $x \in L$ be a fixed element of order r. Suppose that $\langle x^g \rangle$ and $\langle x \rangle$ are conjugate in L. Then the conclusion of Proposition 4.1 holds.

PROOF. Since $p \nmid |L|$, g must normalize an L-congugate $\langle y \rangle$ of $\langle x \rangle$. By Step 4, g does not centralize $\langle y \rangle$. By Step 3, $\langle y, W \rangle = \langle y \rangle \times W$. Let ν be a faithful linear character of $\langle y \rangle$. Let $\theta = (\mu \times \nu)^L$, let $c = |C_L(y)|/|\langle y \rangle \times W|$, and let $\varepsilon = \nu(y)$. By the definition of induced characters, $\theta(y) = c\Sigma_{\gamma \in S} \varepsilon^\gamma$, where S is a p'-subgroup of $\mathrm{Gal}(\mathbf{Q}(\varepsilon)/\mathbf{Q})$. Also

$$\theta^g(y) = \sum_{\gamma \in S} \varepsilon^{\beta\gamma},$$

where $\beta \in \mathrm{Gal}(\mathbf{Q}(\varepsilon)/\mathbf{Q})$ has order p. Since the primitive rth roots of 1 are linearly independent over $\mathbf{Q}$, it follows that $\theta^g(y) \neq \theta(y)$, so $\theta^g \neq \theta$.

Let χ be an irreducible constituent of θ such that $\chi^g \neq \chi$. Then $\chi \in \mathrm{Irr}(L \mid \mu)$. By Step 5, χ is fixed by no element of order p in G, so $p \nmid |I_G(\chi)|$.

Step 7. Let g and x be as in Step 6. Suppose that $\langle x^g \rangle$ and $\langle x \rangle$ are not conjugate in L. Then the conclusion of Proposition 4.1 holds.

PROOF. As in Step 6, $\langle x, W \rangle = \langle x \rangle \times W$. Let $\theta = (1_{\langle x \rangle} \times \mu)^L$. Then $\theta(x) = |N_L\langle x \rangle : \langle x, W \rangle| \neq 0$, while $\theta(x^g) = 0$. Hence $\theta \neq \theta^g$. The conclusion of Proposition 4.1 follows as in Step 6.

PROPOSITION 4.2. *Let $G = O^{p'}(G)$ and $|G: O_{p'}(G)| = p$ for an odd prime p. Suppose that L/W is a nonabelian nonsimple chief factor of G. Suppose that $\mu \in \mathrm{Irr}(W)$ is invariant in G. Then some character in $\mathrm{Irr}(G \mid \mu)$ has degree divisible by p.*

PROOF. As in the proof of Proposition 4.1, we may assume that μ is linear and faithful and that $L = L'$. We have $L/W = \prod_{i=1}^n S_i/W$, where the S_i/W are isomorphic simple groups. The S_i are transitively permuted by the action of G.

Step 1. L is the central product of the S_i.

PROOF. For $i \neq j$, $x \in S_i$, $y \in S_j$, the map $y \to [x, y]$ defines a homomorphism from S_j to W whose kernel contains W. Since S_j/W is simple, this homomorphism must be trivial. Thus $[S_i, S_j] = 1$. Since $\bigcap S_i = W$, the result follows.

Step 2. Each S_i is perfect.

PROOF Since L is perfect, L is the product of the S_i'. Since G permutes the S_i' transitively, $S_i' \cap W$ is the same group W_0 for all i. Then L/W_0 is the direct product of the S_i'/W_0. Thus $|L| = |W_0| \prod |S_i/W|$, so $W_0 = W$ and so $S_i' = S_i$ for all i.

To make the remaining steps of the proof clearer we introduce an "abstract" group S, isomorphic to each S_i. Thus S is perfect and $Z(S) \cong W$.

Step 3. Let μ_0 be a faithful linear character of $Z(S)$. Let A be the centralizer in $\mathrm{Aut}(S)$ of $Z(S)$. Then A has more than one orbit on $\mathrm{Irr}(S \mid \mu_0)$.

PROOF. Suppose not. Then every character in $\mathrm{Irr}(S \mid \mu_0)$ has the same degree d. Let $m = |\mathrm{Irr}(S \mid \mu_0)|$. By [**16**, p. 84], $|S : Z(S)| = md^2$.

By the argument in Step 5 of Proposition 4.1, any element of A which induces an inner automorphism of $S/Z(S)$ lies in $\mathrm{Inn}(S)$, so that $A/\mathrm{Inn}(S)$ is isomorphic to a subgroup of $\mathrm{Out}(S/Z(S))$. Therefore, m divides $|\mathrm{Out}(S/Z(S))|$.

Let r be as in Corollary 1.4, applied to $S/Z(S)$. Since $r \,\|\, |S/Z(S)|$ and $r \nmid |\mathrm{Out}(S/Z(S))|$, it follows that $r \nmid m$ and $r \mid d$. Let $R \in \mathrm{Syl}_r(S)$. Since $r \nmid |Z(S)|$, $R \times Z(S)$ is a subgroup of S. Let $\theta = (1_R \times \mu_0)^S$. Then $r \nmid \theta(1)$, which contradicts the fact that every irreducible constituent of θ lies in $\mathrm{Irr}(S \mid \mu_0)$.

Step 4. Let U be the permutation group on $\{S_1, \dots, S_n\}$ induced by the action of G. Then the conclusion of Proposition 4.2 holds if $p > 3$ or if $U \not\cong J$.

PROOF. Since $O^{p'}(G) = G$ we have $p \,\|\, |U|$. By Theorem 2.5 we can choose $\Delta \leqslant \{S_1, \dots, S_n\}$ so that no element of order p in G fixes Δ. Fix isomorphisms f_i: $S \to S_i$ so that the restrictions f_i: $Z(S) \to W$ are the same function for all i. Then $\mu_0 = f_i^{-1}(\mu)$ is a well-defined linear character of $Z(S)$. By Step 3, we may choose χ, $\psi \in \mathrm{Irr}(S \mid \mu_0)$ to lie in different A-orbits. Define $\eta \in \mathrm{Irr}(L \mid \mu)$ by requiring that $\eta|_{S_i} = (\eta(1)/\chi(1)) f_i(\chi)$ for $S_i \in \Delta$ and $\eta|_{S_i} = (\eta(1)/\psi(1)) f_i(\psi)$ for $S_i \notin \Delta$.

Suppose $g \in G$ fixes η. Then there exist indices i, j such that $S_i \in \Delta$, $S_j \notin \Delta$ and $S_i^g = S_j$. Let $c(g)$: $S_i \to S_j$ be the isomorphism given by conjugating by g. Then $f_i c(g) f_j^{-1}$: $S \to S$, $f_i c(g) f_j^{-1} \in A$, and $f_i c(g) f_j^{-1}$ takes χ to ψ, a contradiction.

Step 5. Conclusion.

Let S, A and U be as above. We may assume by Step 4 that $U \cong J$, $p = 3$, $n = 8$ and $S/Z(S) \cong \mathrm{Sz}(q)$ for some odd power q of 2. If $q > 8$ then $\mathrm{Sz}(q)$ has a trivial Schur multiplier, so L is the direct product of 8 copies of $\mathrm{Sz}(q)$ and $\mu = 1$. We can write $\{S_1, \dots, S_8\}$ as the disjoint union of 3 sets Δ_1, Δ_2, Δ_3 so that no element of order 3 in G stabilizes all 3 sets. Now choose irreducible characters χ_1, χ_2, χ_3 of $S \cong \mathrm{Sz}(q)$ whose degrees are all different. Define $\chi \in \mathrm{Irr}(L \mid \mu)$ to be the direct product whose jth component is χ_i if $S_j \in \Delta_i$. Then χ is not fixed by an element of order 3 in G.

Thus we may assume that $S/Z(S) \cong \mathrm{Sz}(8)$. By the argument in the preceding paragraph, we may assume that $Z(S) \neq 1$. Since S is perfect, $Z(S)$ is cyclic, and the multiplier of $\mathrm{Sz}(8)$ is $\mathbf{Z}_2 \times \mathbf{Z}_2$ by [**1**, Theorem 2], we have $|Z(S)| = 2$. Since $|\mathrm{Out}(\mathrm{Sz}(8))| = 3$ and $\mathrm{Aut}(\mathrm{Sz}(8))$ has a trivial multiplier [**1**, Theorem 2], it follows that every automorphism of S is inner. Let Δ_1, Δ_2, Δ_3 be as in the preceding paragraph. Since $|S/Z(S)| = 29{,}120$ is not the sum of two squares, we can choose distinct characters χ_1, χ_2, $\chi_3 \in \mathrm{Irr}(S \mid \mu)$. Fix isomorphisms f_i: $S \to S_i$ for $1 \leqslant i \leqslant 8$ and define $\chi \in \mathrm{Irr}(L \mid \mu)$ by the condition that $\chi|_{S_j} = (\chi(1)/\chi_i(1)) f_j(\chi_i)$ for $S_j \in \Delta_i$.

Since $A = \mathrm{Inn}(S)$, it follows that χ is fixed by no element of order 3 in G. This completes the proof of Proposition 4.2.

PROOF OF THEOREM A. Let G be a minimal counterexample to Theorem A. Then G is nonsolvable by [**8**, Theorem A] and satisfies conditions (1)–(6) of Proposition 0. Let V be as in Proposition 0.

We may apply Corollary 2.6 and Theorem 3.1 to the action of G/N on V to deduce that V is a primitive $GF(p)[G/N]$-module and $F^*(G/N) \neq F(G/N)$. By Lemma 1.5, there is a perfect subgroup $\bar{L}$ of G/N such that $\bar{L}/Z(\bar{L})$ is a nonsolvable chief factor of G/N. Any prime divisor of $|Z(\bar{L})|$ divides $|M(S)|$, the order of the Schur multiplier of a nonabelian simple composition factor of $\bar{L}$. By Lemma 1.2 and the table in [**11**, p. 280], we conclude that p exceeds every prime divisor of $|Z(\bar{L})|$. Since V is a primitive $GF(p)[G/N]$-module, $Z(\bar{L})$ is cyclic, and thus every element of order p in G centralizes $Z(\bar{L})$.

Let L and W be the inverse images in $G/O_p(N)$ of $\bar{L}$ and $Z(\bar{L})$. We identify the central cyclic subgroup Z of G with its image in $G/O_p(N)$. Thus W is a normal abelian subgroup of $G/O_p(N)$, and $W/Z \cong Z(\bar{L})$.

Any element of order p in $G/O_p(N)$ centralizes both Z and $W/Z \cong Z(\bar{L})$. As $p \nmid |W|$ and $G = O^{p'}(G)$, it follows that $W \leqslant Z(G/O_p(N))$. Thus, any linear character μ of W which extends λ is invariant in $G/O_p(N)$. We may apply Proposition 4.1 or 4.2 to $G/O_p(N)$, L, W and μ to obtain $\chi \in \mathrm{Irr}(G/O_p(N) \mid \mu)$ such that $p \mid \chi(1)$. Since χ may be viewed as a character in $\mathrm{Irr}(G \mid \lambda)$, this contradicts (6) in Proposition 0 and completes the proof of Theorem A.

REFERENCES

1. J. L. Alperin and D. Gorenstein, *The multiplicators of certain simple groups*, Proc. Amer. Math. Soc. **17** (1966), 515–519.
2. L. Babai, *On the order of uniprimitive permutation groups*, Ann. of Math. (2) **113** (1981), 553–568.
3. N. Blackburn and B. Huppert, *Finite groups*. III, Springer-Verlag, Berlin, 1982.
4. P. Cameron, *Finite permutation groups and finite simple groups*, Bull. London Math. Soc. **13** (1981), 1–22.
5. P. Fong, *On the characters of p-solvable groups*, Trans. Amer. Math. Soc. **98** (1961), 263–284.
6. ______, *A note on a conjecture of Brauer*, Nagoya Math. J. **22** (1963), 1–13.
7. D. Gluck, *Trivial set-stabilizers in finite permutation groups*, Canad. J. Math. **35** (1983), 59–67.
8. D. Gluck and T. R. Wolf, *Defect groups and character heights in blocks of solvable groups*. II, J. Algebra (to appear).
9. D. Gorenstein, *Finite groups*, Harper & Row, New York, 1968.
10. ______, *The classification of finite simple groups*, Bull. Amer. Math. Soc. (N.S.) **1** (1979), 43–200.
11. R. L. Griess, Jr., *Schur multipliers of the known finite simple groups*. II, Proc. Sympos. Pure Math., vol. 37, Amer. Math. Soc., Providence, R. I., 1980, pp. 279–282.
12. R. L. Griess, Jr. and R. Lyons, *The automorphism group of the Tits simple group* ${}^2F_4(2)'$, Proc. Amer. Math. Soc. **52** (1975), 75–78.
13. C. Hering. *Transitive linear groups and linear groups which contain irreducible subgroups of prime order*. II, preprint.
14. M. Herzog and C. Praeger, *On the fixed points of Sylow subgroups of transitive permutation groups*, J. Austral. Math. Soc. Ser. A **21** (1976), 428–437.
15. B. Huppert, *Endliche Gruppen*. I, Springer-Verlag, Berlin, 1967.
16. I. M. Isaacs, *Character theory of finite groups*, Academic Press, New York, 1976.
17. V. Landazuri and G. Seitz, *On the minimal degrees of projective representations of finite Chevalley groups*, J. Algebra **32** (1974), 418–443.

18. R. Ree, *A family of simple groups associated with the simple Lie algebra of type F_4*, Amer. J. Math. **83** (1961), 401–420.

19. ______, *A family of simple groups associated with the simple Lie algebra of type G_2*, Amer. J. Math. **83** (1961), 432–462.

20. R. Steinberg, *Automorphisms of finite linear groups*, Canad. J. Math. **12** (1960), 606–615.

21. ______, *Endomorphisms of linear algebraic groups*, Mem. Amer. Math. Soc. No. 80 (1968).

22. ______, *Algebraic groups and finite groups*, Illinois J. Math. **13** (1969), 81–86.

23. M. Suzuki, *On a class of doubly transitive groups*, Ann. of Math. (2) **75** (1962), 105–145.

24. T. R. Wolf, *Defect groups and character heights in blocks of solvable groups*, J. Algebra **72** (1981), 183–209.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF WISCONSIN, MADISON, WISCONSIN 53706

DEPARTMENT OF MATHEMATICS, OHIO UNIVERSITY, ATHENS, OHIO 45701 (Current address of T. R. Wolf)

Current address (David Gluck): Department of Mathematics, Wayne State University, Detroit, Michigan 48202