TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 361, Number 12, December 2009, Pages 6521–6547
S 0002-9947(09)04718-7
Article electronically published on July 24, 2009

GROUPS WITH JUST ONE CHARACTER DEGREE DIVISIBLE BY A GIVEN PRIME

I. M. ISAACS, ALEXANDER MORETÓ, GABRIEL NAVARRO, AND PHAM HUU TIEP

Abstract. The Ito-Michler theorem asserts that if no irreducible character of a finite group G has degree divisible by some given prime p, then a Sylow p-subgroup of G is both normal and abelian. In this paper we relax the hypothesis, and we assume that there is at exactly one multiple of p that occurs as the degree of an irreducible character of G. We show that in this situation, a Sylow p-subgroup of G is almost normal in G, and it is almost abelian.

1. Introduction

Let G be a finite group, and fix a prime p. One of the fundamental results of character theory is the Ito-Michler theorem, which asserts that if no irreducible character of G has degree divisible by p, then a Sylow p-subgroup P of G is abelian and is normal in G. (As is well known, the converse of this is true too, and is much more elementary.)

What if only a few of the irreducible character degrees of G are divisible by p? Does this imply that in some sense, P is almost abelian and is almost normal in G? In this paper, we test these ideas by going one step beyond the Ito-Michler theorem: we assume that just one irreducible character degree of G is divisible by p, and we show that P has derived length at most 2 and that $P/\mathbf{O}_p(G)$ is under control. In particular, if P is not normal, we have the following.

Theorem A. *Let G be a finite group with exactly one irreducible character degree n divisible by p, and let $P \in \mathrm{Syl}_p(G)$. Write $U = \mathbf{O}_p(G)$, and assume that $U < P$. Then*

(a) *U is abelian.*
(b) *P/U is abelian, and if G is p-solvable, P/U is cyclic.*
(c) *$|P/U| = n_p$, the p-part of n.*
(d) *P/U is a TI-set in G/U.*

We mention that if G is not p-solvable, then the group P/U of Theorem A need not be cyclic. A counterexample is $G = M_{11}$ with $p = 3$.

Recall that for groups that are not p-solvable, the proof of the Ito-Michler theorem requires an appeal to the classification and representation theory of simple

Received by the editors October 2, 2007 and, in revised form, December 14, 2007.
2000 *Mathematics Subject Classification.* Primary 20C15; Secondary 20C33.
This research was partially supported by the Spanish Ministerio de Educación y Ciencia, MTM2004-06067-C02-01 and MTM2004-04665, and the FEDER. The second author was also supported by the Programa Ramón y Cajal and the Generalitat Valenciana. The fourth author gratefully acknowledges the support of the NSF (grant DMS-0600967).

groups. As might be expected, the proof of our Theorem A is considerably more involved, and even in the p-solvable case it requires information about representations of simple and almost simple groups. (Sections 6 and 7 of this paper contain the representation theory that we need.)

In the situation of Theorem A, where the Sylow p-subgroup P is not normal, it is clear that P has derived length at most 2. In fact, we can obtain more precise information about P, whether or not it is normal.

Corollary B. *Let G be a finite group with exactly one irreducible character degree n divisible by p, and let $P \in \mathrm{Syl}_p(G)$. If $\theta \in \mathrm{Irr}(P)$, then $\theta(1)$ lies in the set $\{1, n_p\}$, and in particular, P is metabelian.*

Corollary B suggests that perhaps in general the number of distinct irreducible character degrees of a Sylow p-subgroup P of an arbitrary finite group G is at most one more than the number of irreducible character degrees of G that are multiples of p. (As is well known, that would imply that the derived length of P is also bounded by this number.) This, in fact, was the idea that originally motivated this project.

We should remark that another invariant relating the character degrees of G and the structure of a Sylow p-subgroup P of G has been studied previously: the number k of different p-parts of the irreducible character degrees of G. (See [I1, M1, M2].) Most of the known results in that direction refer only to solvable groups, and although some inequalities hold, it is not true even for solvable groups that the derived length of P is at most k. (This fails even if $k = 2$.)

We also obtain some additional structural information about non-p-solvable groups that have just one irreducible character degree divisible by p.

Theorem C. *Let G be a finite group with exactly one irreducible character degree divisible by p. Assume that G is not p-solvable, and let $U = \mathbf{O}_p(G)$ and $K/U = \mathbf{O}_{p'}(G/U)$. Then K is the unique largest normal p-solvable subgroup of G. Also, G/K has a simple socle S/K, and $|G : S|$ is not divisible by p.*

In fact, the simple group S/K in Theorem C must be one of M_{11}, J_1, or $PSL_2(q)$. (See Corollary 7.5.)

2. Preliminaries

Although our notation is more or less standard and follows [I2], it is worth mentioning a few specific items here. If G is a finite group, then $\mathrm{cd}(G)$ is the set of irreducible character degrees of G. If $N \triangleleft G$ and $\theta \in \mathrm{Irr}(N)$, then G_θ is the stabilizer of θ in G and $\mathrm{Irr}(G|\theta)$ is the set of characters $\chi \in \mathrm{Irr}(G)$ that lie over θ. In this situation, we will use the notation $\mathrm{cd}(G|\theta) = \{\chi(1) \mid \chi \in \mathrm{Irr}(G|\theta)\}$.

For convenience, we will say that a finite group G is a **one-p-degree** group if $\mathrm{cd}(G)$ contains at most one multiple of the prime p. It is useful to observe that homomorphic images of one-p-degree groups are again one-p-degree groups (and this is the reason that we include as one-p-degree groups the groups having no irreducible character of degree divisible by p). Since the Ito-Michler theorem guarantees that $\mathrm{cd}(G)$ contains a multiple of p unless a Sylow p-subgroup of G is both normal and abelian, it follows that if G is a one-p-degree group and a Sylow subgroup of G either fails to be normal or fails to be abelian, then $\mathrm{cd}(G)$ does contain a (necessarily unique) multiple of p.

We start by deducing Corollary B from Theorem A.

Proof of Corollary B. First, suppose that $P \lhd G$. If $\alpha \in \mathrm{Irr}(P)$, let $\chi \in \mathrm{Irr}(G)$ lie over α. Then $\alpha(1) = \chi(1)_p$ by Corollary 11.29 of [I2], and the result is immediate in this case. We can thus assume that P is not normal, and so Theorem A applies.

Let $U = \mathbf{O}_p(G)$, and let $\lambda \in \mathrm{Irr}(U)$. Then λ is linear because U is abelian by Theorem A, and we claim that either λ extends to P or that λ^P is irreducible. To see that this will complete the proof, let $\alpha \in \mathrm{Irr}(P)$ and let $\lambda \in \mathrm{Irr}(U)$ lie under α. If $\lambda^P \in \mathrm{Irr}(P)$, then $\alpha = \lambda^P$, and so $\alpha(1) = |P : U| = n_p$, by Theorem A. If, on the other hand, λ extends to P, let $\psi \in \mathrm{Irr}(P)$ be an extension. Then by Gallagher's theorem (Corollary 6.17 of [I2]) we have $\alpha = \psi\tau$ for some character $\tau \in \mathrm{Irr}(P/U)$. Since P/U is abelian (again by Theorem A) we have $\tau(1) = 1$, and so $\alpha(1) = \psi(1) = 1$.

To prove that λ either extends or induces irreducibly to P, let $T = G_\lambda$, the stabilizer of λ. If $T \cap P = U$, then λ^P is irreducible by the Clifford correspondence (Theorem 6.11 of [I2]), and so we can assume that $T \cap P > U$. Now $T \cap P$ is a full Sylow p-subgroup of T, since otherwise there would exist two distinct Sylow p-subgroups of G with intersection containing $T \cap P$, and hence properly containing U. This contradicts the assertion in Theorem A that the Sylow p-subgroups of G/U are TI-sets.

If all members of $\mathrm{Irr}(G|\lambda)$ have degree n, then all members of $\mathrm{Irr}(T|\lambda)$ have degree $n/|G : T|$, and writing $e = n/|G : T|$, we have

$$e_p = \frac{n_p}{|G : T|_p} = \frac{|G : U|_p}{|G : T|_p} = |T : U|_p \,.$$

Since

$$|T : U| = \sum_{\psi \in \mathrm{Irr}(T|\lambda)} \left(\frac{\psi(1)}{\lambda(1)}\right)^2 = |\mathrm{Irr}(T|\lambda)| e^2 \,,$$

it follows that e^2 divides $|T : U|$. Then $(e_p)^2 = (|T : U|_p)^2$ divides $|T : U|$, and thus $|T : U|_p = 1$. This yields $T \cap P = U$, which is a contradiction.

We conclude that there exists $\chi \in \mathrm{Irr}(G|\lambda)$ with p'-degree, and we write $\chi = \psi^G$, where $\psi \in \mathrm{Irr}(T|\lambda)$. Since $|G : T|$ and $\psi(1)$ divide $\chi(1)$, both are p'-numbers. In particular, the Sylow p-subgroup $T \cap P$ of T is a full Sylow p-subgroup of G, and hence $P \subseteq T$. Also, ψ_P has some irreducible constituent μ of degree not divisible by p, and thus μ is linear. Since μ lies over λ, it follows that λ extends to P, and this completes the proof. □

For Theorems A and C, we need some facts about characters of groups having a nonabelian simple socle. We state what we need here, but we defer the proof to Section 7.

Theorem 2.1. *Let S be the socle of G, and assume that S is a nonabelian simple group. The following then hold.*

(a) *G has faithful irreducible characters α and β with distinct degrees.*
(b) *If p is a prime divisor of $|G : S|$, then α and β can be chosen to have degrees divisible by p.*

Theorem 2.1 will enable us to prove Theorem A (but only for p-solvable groups) and Theorem C in full generality. To prove Theorem A in general, we will need an additional result on simple groups, which appears as Theorem 5.1. The proof of that result too will be deferred to Section 7.

We start by using Theorem 2.1 to establish several facts about one-p-degree groups.

Lemma 2.2. *Let G be a one-p-degree group. Suppose that $N \triangleleft G$ is a direct product of nonabelian simple groups, and let L be the product of all but one of the simple factors of N. Let $M = \mathbf{N}_G(L)$ and $C/L = \mathbf{C}_{M/L}(N/L)$. Then $|G : NC|$ is not divisible by p and α^G is irreducible for all faithful characters $\alpha \in \mathrm{Irr}(M/C)$.*

Proof. Observe that $M \supseteq N$ and that $C \cap N = L$. Then $NC/C \cong N/L$, and so NC/C is a nonabelian simple group, and it is the socle of M/C. Let $\alpha \in \mathrm{Irr}(M/C)$ be faithful, and observe that if φ is an irreducible constituent of α_N, then $L = \ker(\varphi)$, and thus $M = \mathbf{N}_G(L) \supseteq G_\varphi$, the stabilizer of φ in G. Since $\alpha \in \mathrm{Irr}(M|\varphi)$, it follows that α^G is irreducible, by the Clifford Correspondence.

Now, by Theorem 2.1(a), there exists a faithful character $\beta \in \mathrm{Irr}(M/C)$ with $\alpha(1) \neq \beta(1)$, and again β^G is irreducible. If $|G : M|$ is divisible by p, then α^G and β^G have different degrees divisible by p, and since this contradicts the one-p-degree hypothesis, we deduce that p does not divide $|G : M|$. Also, if p divides $|M : NC|$, then by Theorem 2.1(b), it is possible to choose α and β having degrees divisible by p, and in this case too, α^G and β^G have different degrees divisible by p, and again, we have a contradiction. Thus p does not divide $|M : NC|$, and thus p does not divide $|G : NC|$, as required. □

Lemma 2.3. *Let G be a one-p-degree group, and let N be minimal normal in G with order not divisible by p. Suppose that $N \subseteq K \triangleleft G$, where K/N is a p-group, and assume that $\mathbf{O}^{p'}(K) = K$. Then N is abelian.*

Proof. Assume that N is nonabelian, so that it is a direct product of nonabelian simple groups, and Lemma 2.2 applies. Let L, M and C be as in that lemma, so that $|G : NC|$ is a p'-number. Since K/N is a normal p-subgroup of G/N and NC/N is a subgroup having p'-index, it follows that $K \subseteq NC$, and thus $K \cap C \triangleleft K$. Also $K/(K \cap C) \cong N/L$ is a p'-group, and this contradicts the assumption that $K = \mathbf{O}^{p'}(K)$. □

In the next lemma, we use the following nearly trivial fact: if $f \in \mathrm{cd}(G)$ and $A \subseteq G$ is abelian, then $f \leq |G : A|$. This is an immediate consequence of Frobenius reciprocity.

Lemma 2.4. *Let $M \triangleleft G$, where G is a one-p-degree group, and suppose that $\theta \in \mathrm{Irr}(M)$ has degree divisible by p. If θ extends to G_θ, then G/M has a normal abelian Sylow p-subgroup. In particular, this happens if θ has p-power degree and determinantal order and G/M has a cyclic Sylow p-subgroup.*

Proof. Since p divides $\theta(1)$, we have $\mathrm{cd}(G|\theta) = \{n\}$, where n is the unique member of $\mathrm{cd}(G)$ that is divisible by p. Then all members of $\mathrm{Irr}(T|\theta)$ have degree $n/|G : T|$, where $T = G_\theta$. By hypothesis, one of these characters is an extension of θ, and thus all of them are extensions of θ. Hence, T/M is abelian by Gallagher's theorem (Corollary 6.17 of [I2]). If $f \in \mathrm{cd}(G/M)$, therefore, then $f \leq |G : T| = n/\theta(1) < n$, and so $n \notin \mathrm{cd}(G/M)$. Then no member of $\mathrm{cd}(G/M)$ has degree divisible by p, and the result follows by Ito-Michler.

Finally, suppose that θ has p-power degree and determinantal order, and that G/M has a cyclic Sylow p-subgroup. We wish to show that θ extends to G_θ. By Corollary 11.31 of [I2], it is enough to show for every prime q that θ extends to

Q, where Q/M is a Sylow q-subgroup of G_θ/M. If $q = p$, then Q/M is cyclic and θ extends by Corollary 11.22 of [I2]. Also, if $q \neq p$, then θ extends to Q by Corollary 8.16 of [I2]. □

The following is an easy special case of a known and more general fact about half-transitive group actions. (See [IP].)

Lemma 2.5. *Let P be an abelian p-group that acts faithfully on an abelian p'-group A, and suppose that all P-orbits of nonidentity elements of A have equal size q. Then P is cyclic, and $|P| = q$.*

Proof. Let $1 \neq x \in A$, and let $K = \mathbf{C}_P(x)$, so that $|P : K| = q$. By Fitting's lemma, $A = \mathbf{C}_A(K) \times [A, K]$, and each factor is P-invariant since $K \lhd P$. Of course, x lies in $\mathbf{C}_A(K)$, and if $[A, K]$ is nontrivial, choose a nonidentity element $y \in [A, K]$ and observe that $\mathbf{C}_P(xy) = \mathbf{C}_P(x) \cap \mathbf{C}_P(y)$. Since each of these three centralizers has index q in P, we have $K = \mathbf{C}_P(x) = \mathbf{C}_P(y)$, and thus $y \in \mathbf{C}_A(K) \cap [A, K] = 1$. This contradiction shows that $[A, K] = 1$, and since the action of P is faithful, we have $K = 1$. Thus $|P| = |P : K| = q$. Also, $\mathbf{C}_P(x) = 1$ for every nonidentity element $x \in A$, and so the action of P is Frobenius. Since P is abelian, it is cyclic. □

Finally, we shall need the following well known elementary lemma.

Lemma 2.6. *Suppose that $A \subseteq G$ is abelian. If $\chi \in \mathrm{Irr}(G)$ and $\chi(1) = |G : A|$, then $\chi(g) = 0$ for every element $x \in G - A$. Also, there exists $N \lhd G$ with $N \subseteq A$ and such that $\chi(g) = 0$ for all $g \in G - N$.*

Proof. Since A is abelian, all irreducible constituents of χ_A are linear, and thus $[\chi_A, \chi_A] \geq \chi(1) = |G : A|$. The sum of $|\chi(a)|^2$ for $a \in A$ is therefore at least $|G|$, and since $[\chi, \chi] = 1$, it follows that $\chi(g) = 0$ for all $g \in G - A$. Now let $N = \langle g \mid \chi(g) \neq 0 \rangle$. Then $N \lhd G$ and $N \subseteq A$, and so the proof is complete. □

3. Theorem A for p-solvable groups

Theorem 3.1. *Let G be a p-solvable one-p-degree group, and let $U = \mathbf{O}_p(G)$. Then either U is a full Sylow p-subgroup of G, or else U is abelian and G/U has a cyclic Sylow p-subgroup of order n_p, where $n \in \mathrm{cd}(G)$ is divisible by p.*

Proof. Assume that U is not a full Sylow p-subgroup of G, so that there exists $n \in \mathrm{cd}(G)$ divisible by p. We proceed by induction on $|G|$. Now $\mathbf{O}_p(G/U)$ is trivial, and thus G/U fails to have a normal Sylow p-subgroup. If $U > 1$, the inductive hypothesis applies to G/U, and we conclude that G/U has a cyclic Sylow p-subgroup of order n_p, as required. Also, if U is nonabelian, we can apply Lemma 2.4 to a nonlinear irreducible character of U, and we conclude that G/U has a normal Sylow p-subgroup, which is not the case. It follows that U is abelian, as required.

We can now assume that $U = 1$. Let N be a minimal normal subgroup of G. Since G is p-solvable and $\mathbf{O}_p(G) = 1$, we see that N is a p'-group. Let $K/N = \mathbf{O}_p(G/N)$. If $K = N$, then by the inductive hypothesis applied to G/N, we conclude that G/N has cyclic Sylow p-subgroups of order n_p, and thus the same is true about G. We can assume, therefore, that $K > N$.

By elementary group theory, $\mathbf{C}_K(N) \subseteq N$, since K/N is a p-group and $\mathbf{O}_p(K) = 1$. If $N \cap \mathbf{O}^{p'}(K) = 1$, then $\mathbf{O}^{p'}(K)$ is a normal p-subgroup of K, and thus $\mathbf{O}^{p'}(K) = 1$ and K is a p'-group, which is not the case because $K > N$. Since N is minimal

normal in G, it follows that $N \subseteq \mathbf{O}^{p'}(K)$, and thus $\mathbf{O}^{p'}(K) = K$ since K/N is a p-group. By Lemma 2.3, therefore, N is abelian. In particular, $\mathbf{C}_K(N) = N$.

We claim now that G/K is a p'-group. Otherwise, K/N is not a full Sylow p-subgroup of G/N. By the inductive hypothesis applied to G/N, it follows that G/K has a cyclic Sylow p-subgroup. Now, all irreducible characters of K have p-power degree, and they also have p-power determinantal order since $K = \mathbf{O}^{p'}(K)$. Furthermore, K is not abelian since $\mathbf{O}^{p'}(K) = K$ and K is not a p-group. It follows that there exists a nonlinear character $\theta \in \mathrm{Irr}(K)$. Lemma 2.4 now applies, and we conclude that G/K has a normal Sylow p-subgroup, proving the claim.

Since $|G : K|$ is a p'-number, it follows that if $\psi \in \mathrm{Irr}(K)$, then $\psi(1)_p = \chi(1)_p$, where $\chi \in \mathrm{Irr}(G|\psi)$, and thus since $\psi(1)$ is a p-power, either $\psi(1) = 1$ or $\psi(1) = n_p$, and this shows that $\mathrm{cd}(K) = \{1, n_p\}$.

Now let $\lambda \in \mathrm{Irr}(N)$ be nonprincipal. If λ is invariant in K, then $[N, K] \subseteq \ker(\lambda) < N$, and thus $[N, K] = 1$, which is not possible since $\mathbf{C}_K(N) = N$. Thus λ lies in a nontrivial K-orbit. Since λ extends to K_λ, it follows that $|K : K_\lambda| \in \mathrm{cd}(K) = \{1, n_p\}$, and thus λ lies in a K-orbit of size n_p. Also, since $\mathrm{cd}(K|\lambda) = \{n_p\}$ and λ extends to K_λ, we see that $\mathrm{cd}(K_\lambda|\lambda) = \{1\}$ by Gallagher's theorem, and thus K_λ/N is abelian.

We argue next that K/N is abelian. Otherwise, there exists a nonlinear character $\eta \in \mathrm{Irr}(K/N)$, and thus $\eta(1) = n_p$. Since K_λ/N is an abelian subgroup of K/N of index $n_p = \eta(1)$, it follows by Lemma 2.6 that η vanishes on $K - K_\lambda$. In other words, if $x \in K$ and $\eta(x) \neq 0$, then x lies in K_λ for every linear character λ of N, and thus $x \in \mathbf{C}_K(N) = N \subseteq \ker(\eta)$. It is not possible, however, for a nonprincipal character to vanish on every element outside of its kernel, and thus K/N is abelian, as claimed.

Now let $P \in \mathrm{Syl}_p(K)$, so that P is a Sylow p-subgroup of G. Then P is abelian, and it acts faithfully on N, and hence it also acts faithfully on the group A of linear characters of N. Furthermore, all P-orbits of nonidentity elements of A have size n_p, and it follows by Lemma 2.5 that P is cyclic of order n_p, as required. □

At this point, we have almost completed the proof of Theorem A in the case where G is p-solvable. All that remains is to show that P/U is a TI-set in G/U, where $U = \mathbf{O}_p(G)$ and $P \in \mathrm{Syl}_p(G)$. To accomplish that, we prove a more general result than we need here; it will be used again to handle groups that are not p-solvable.

Theorem 3.2. *Suppose that n is the unique member of $\mathrm{cd}(G)$ that is divisible by the prime p. Let $K \triangleleft G$ be a p'-group and assume that a Sylow p-subgroup of G is abelian of order n_p. If distinct Sylow p-subgroups of G/K intersect trivially, then distinct Sylow p-subgroups of G also intersect trivially.*

To prove this, we recall the following well known fact from the theory of coprime actions: if A acts coprimely on G and A fixes all conjugacy classes of G, then the action of A on G is trivial. (This follows, for instance, from Corollary 13.10 of [I2].)

Lemma 3.3. *Let P be a p-group that acts on a p'-group N, and assume that each P-orbit on $\mathrm{Irr}(N)$ has size 1 or $|P|$. Then the same is true for the P-orbits on the elements of N.*

Proof. It is a consequence of the Glauberman character correspondence that the actions of P on $\mathrm{Irr}(N)$ and on the set of classes of N are permutation isomorphic.

(See Theorem 13.24(b) of [I2].) It follows that every class of N that is not fixed by P lies in a regular P-orbit. Now let $x \in N$, and write $D = \mathbf{C}_P(x)$. Assuming that $1 < D < P$, we work to derive a contradiction.

Let $B = \mathbf{C}_N(D)$ and $E = \mathbf{N}_P(D)$. Then E acts on B, and this action is nontrivial since $x \in B$ and $\mathbf{C}_E(x) = D < E$. It follows that some conjugacy class L of B is not E-invariant. By Corollary 13.10 of [I2], intersection defines a bijection from the set of D-invariant classes of N to the set of all classes of B, and so it follows that $L = K \cap B$, where K is some D-invariant class of N. Since K is D-invariant and $D > 1$, the P-orbit of K is not regular, and thus K is P-fixed. This is a contradiction, however, since K cannot be E-fixed because L is not E-fixed. □

Proof of Theorem 3.2. Let $P \in \mathrm{Syl}_p(G)$. If $Q \in \mathrm{Syl}_p(G)$ and $P \cap Q > 1$, we argue first that $KP = KQ$. We have $KP \cap KQ \supseteq P \cap Q > 1$, and since K is a p'-group, it follows that $P \cap Q \not\subseteq K$, and hence $KP \cap KQ > K$. By assumption, however, distinct Sylow p-subgroups of G/K intersect trivially, and thus $KP = KQ$, as claimed.

We show next that if $\theta \in \mathrm{Irr}(K)$, then the P-orbit of θ has size 1 or $|P|$. In other words, we claim that if $T \cap P > 1$, then $P \subseteq T$, where $T = G_\theta$. To see this, suppose first that some member of $\mathrm{Irr}(G|\theta)$ has degree not divisible by p. Then p does not divide $|G : T|$, and so T contains a full Sylow p-subgroup Q of G, and we can assume that $Q \supseteq T \cap P$. Then $1 < T \cap P \subseteq Q \cap P$, and thus $P \subseteq KP = KQ \subseteq T$, as wanted. In the remaining case, $\mathrm{cd}(G|\theta) = \{n\}$. Since K is a p'-group, θ extends to some character $\eta \in \mathrm{Irr}(S)$, where $S/K \in \mathrm{Syl}_p(T/K)$. Now $\eta^T(1) = |T : S|\theta(1)$ is not divisible by p, and hence some irreducible constituent γ of η^T has degree not divisible by p. Since $\gamma \in \mathrm{Irr}(T|\theta)$, it follows that γ^G is irreducible, and thus $|G : T|\gamma(1) = \gamma^G(1) = n$. Then $|P| = n_p$ divides $|G : T|$, and it follows in this case that T is a p'-group, and thus $T \cap P = 1$, which is a contradiction.

We can now apply Lemma 3.3 to deduce that every element of K that is not fixed by P lies in a regular P-orbit. Now let $Q \in \mathrm{Syl}_p(G)$, and suppose that $D = P \cap Q > 1$. Since $D > 1$, the first paragraph of the proof shows that $KP = KQ$. Then $P, Q \in \mathrm{Syl}_p(PK)$, and hence $Q = P^k$ for some element $k \in K$. Now let $d \in D = P \cap P^k$, and write $d = u^k$, where $u \in P$. Then $[u, k] = u^{-1}u^k \in P$, and also $[u, k] \in K$, so $[u, k] = 1$ and $d = u^k = u$ is centralized by k. Thus $D > 1$ centralizes k, which, therefore, does not lie in a regular P-orbit. Thus P centralizes k and $Q = P^k = P$, as wanted. □

To complete the proof of Theorem A in the case where G is p-solvable, it suffices to establish the following.

Corollary 3.4. *Let G be a p-solvable one-p-degree group, and let $U = \mathbf{O}_p(G)$. Then a Sylow p-subgroup of G/U is a TI-set in G/U.*

Proof. We can assume that U is not a full Sylow p-subgroup of G. By Theorem 3.1, we have that a Sylow p-subgroup of G/U is cyclic of order n_p, where n is the unique member of $\mathrm{cd}(G)$ divisible by p. Since G/U is p-solvable and has an abelian Sylow p-subgroup, it follows that a Sylow p-subgroup of G/K is normal, where $K/U = \mathbf{O}_{p'}(G/U)$. In particular, a Sylow subgroup of G/K is a TI-set. By Theorem 3.2 applied in the group G/U, we deduce that a Sylow p-subgroup of G/U is a TI-set, as required. □

4. Theorem C

We are now ready to proceed to the case where G is not p-solvable, although our first two results hold in general.

Lemma 4.1. *Let $K \triangleleft G$, where $\mathbf{O}^{p'}(K) = K$, and let $N = \mathbf{O}^p(K)$. If $N' < N$, then K has a nonlinear irreducible character of p-power degree that extends to its stabilizer in G.*

Proof. Let λ be a nonprincipal linear character of N, and note that $o(\lambda)$ is a p'-number since $\mathbf{O}^p(N) = N$. By Corollary 8.16 of [I2], we know that there exists a unique extension $\hat{\lambda}$ of λ to its stabilizer K_λ in K such that $\hat{\lambda}$ has p'-order. Note that $K_\lambda < K$ since K has no nonprincipal p'-order linear character. Let $\theta = (\hat{\lambda})^K$, so that $\theta \in \mathrm{Irr}(K)$, and note that $\theta(1) = |K : K_\lambda|$ exceeds 1 and is a power of p.

We argue next that θ extends to $T = G_\theta$. Now $o(\theta)$ is a power of p because $\mathbf{O}^{p'}(K) = K$. Also, $\theta(1)$ is a power of p, and hence, by Corollaries 8.16 and 11.31 of [I2], it suffices to show that θ extends to S, where $S/K \in \mathrm{Syl}_p(T/K)$. Let $Q = S_\lambda$ be the stabilizer of λ in S. Then $K \cap Q = K_\lambda$. Also, since θ is invariant in S, the action of K on the S-orbit of λ is transitive, and thus $KQ = S$.

Now λ uniquely determines $\hat{\lambda}$, and so $\hat{\lambda}$ is Q-invariant. Also, Q/K_λ is a p-group while the degree and order of $\hat{\lambda}$ are p'-numbers, and it follows that $\hat{\lambda}$ extends to a linear character μ of Q, again by Corollary 8.16 of [I2]. Then $(\mu^S)_K = (\hat{\lambda})^K = \theta$, and this completes the proof. □

Theorem 4.2. *Let G be a one-p-degree group, and suppose $R \triangleleft G$ is p-solvable. Then either R has a normal Sylow p-subgroup or else G/R has a normal abelian Sylow p-subgroup.*

Proof. Assume that R does not have a normal Sylow p-subgroup, and let $K = \mathbf{O}^{p'}(R)$. Then K is not a p-group, and so $N > 1$, where $N = \mathbf{O}^p(K)$. If $N' < N$, then Lemma 4.1 guarantees that K has a nonlinear irreducible character of p-power degree that extends to its stabilizer in G. By Lemma 2.4, therefore, G/K has a normal abelian Sylow p-subgroup, and thus the same is true for G/R.

We can now assume that $N' = N$, and we let N/M be a chief factor of G, so that N/M is minimal normal in G/M. Also, N/M is p-solvable since R is p-solvable, and since N/M is not a p-group, it must be a p'-group. By Lemma 2.3 applied in the group G/M, it follows that N/M is abelian, and this is a contradiction. □

We can now prove Theorem C, which we restate here.

Theorem 4.3. *Let G be a one-p-degree group that is not p-solvable, and let $U = \mathbf{O}_p(G)$ and $K/U = \mathbf{O}_{p'}(G/U)$. Then K is the unique largest normal p-solvable subgroup of G. Also, G/K has a simple socle S/K, and $|G : S|$ is not divisible by p.*

Proof. Let R be the unique largest normal p-solvable subgroup of G. Since G/R is not p-solvable, it certainly does not have a normal Sylow p-subgroup, and hence R has a normal Sylow p-subgroup by Theorem 4.2. It follows that $R = K$, as required.

We can now replace G by G/K, and so we assume that G has no nontrivial normal p-solvable subgroup. Let N be the socle of G, so that N is a direct product of nonabelian simple groups of order divisible by p. Our goal is to show that N is simple and that p does not divide $|G : N|$.

Let L, M and C be as in Lemma 2.2, so that L is the product of all but one of the simple factors of N. Also, $M = \mathbf{N}_G(L)$ and $C/L = \mathbf{C}_{M/L}(N/L)$, and N/L is a nonabelian simple group of order divisible by p. By Ito-Michler, there exists $\varphi \in \mathrm{Irr}(N/L)$ with degree divisible by p. Let $\theta \in \mathrm{Irr}(NC/C)$ with $\theta_N = \varphi$, and let $\alpha \in \mathrm{Irr}(M|\theta)$. Since NC/C is the socle of M/C, we see that α is a faithful character in $\mathrm{Irr}(M/C)$ and its degree is divisible by p.

Now α^G is irreducible by Lemma 2.2, and also $|G : NC|$ is not divisible by p. Since α^G has degree divisible by p, we have that $n = \alpha^G(1) = \alpha(1)|G : M|$ is the unique character degree of G divisible by p. Notice that $n_p = \alpha(1)_p$ because p does not divide $|G : M|$. Also, α lies above θ, and $\theta_N = \varphi$. Since p does not divide $|M : NC|$ it follows that $\varphi(1)_p = \theta(1)_p = \alpha(1)_p = n_p$. Since n is the only character degree of G divisible by p, it follows that no irreducible character of N can have degree with the p-part exceeding $n_p = \varphi(1)_p$. But $L = \ker(\varphi)$ is a direct factor of N, and thus no irreducible character of L has degree divisible by p. Since L is a direct product of simple groups of order divisible by p, we conclude that $L = 1$, and so N is simple.

Now $C \triangleleft G$ and $C \cap N = 1$, and since N is the socle of G, it follows that $C = 1$. Then $NC = N$, and since we know that $|G : NC|$ is not divisible by p, the proof is complete. □

5. Theorem A

In order to prove Theorem A in full generality, we need an additional fact about simple groups. (So far, the only facts on simple groups that we have used are contained in Theorem 2.1.) We defer the proof of the following to Section 7.

Theorem 5.1. *Let S be the socle of G, and assume that S is a nonabelian simple group of order divisible by the prime p. Assume that n is the only multiple of p that occurs as the degree of a faithful irreducible character of G. Then the Sylow p-subgroups of G are abelian TI-sets of order n_p.*

Basically, what remains is to show the following.

Theorem 5.2. *Let G be a one-p-degree group that is not p-solvable, and let $U = \mathbf{O}_p(G)$. Then U is abelian.*

We need the following two lemmas.

Lemma 5.3. *Let $P \in \mathrm{Syl}_p(G)$, and suppose that $\theta \in \mathrm{Irr}(P)$ has the property that every character $\chi \in \mathrm{Irr}(G|\theta)$ satisfies $\chi_P \in \mathrm{Irr}(P)$. Assume also that $P/\mathbf{O}_p(G)$ is abelian. Then G has an abelian subgroup of order $|G : P|$.*

Proof. Write $U = \mathbf{O}_p(G)$, let $N = \mathbf{N}_G(P)$, and let $\psi \in \mathrm{Irr}(N|\theta)$. Then every member $\chi \in \mathrm{Irr}(G|\psi)$ restricts irreducibly to P and hence to N, and thus $\chi_N = \psi$. It follows by Lemma 12.17 of [I2], that $W \triangleleft G$, where $W = \langle g \in N \mid \psi(g) \neq 0\rangle$. (In other words, W is the "vanishing-off" subgroup of ψ.) Let $V = UW$ and $Q = V \cap P$. Then since $V \subseteq N$, we see that V normalizes P, and thus V normalizes Q. But $V \triangleleft G$, and thus $Q = V \cap P$ is a normal Sylow p-subgroup of V, and hence $Q \triangleleft G$.

Now $\psi_P = \theta$, and hence ψ_{PV} is irreducible. But ψ vanishes outside of PV, and so

$$|PV| = |PV|[\psi_{PV}, \psi_{PV}] = |N|[\psi, \psi] = |N|\,.$$

It follows that $N/Q = (V/Q) \times (P/Q)$, and N/Q is the normalizer in G/Q of the Sylow p-subgroup P/Q. Also, since $U \subseteq Q$, it follows that P/Q is abelian. It is thus

central in N/Q, and hence G/Q has a normal p-complement A/Q by Burnside's theorem.

Now let φ be an irreducible constituent of θ_Q. We argue that every member of $\mathrm{Irr}(A|\varphi)$ has p-power degree. Let $\alpha \in \mathrm{Irr}(A|\varphi)$, and observe that θ is a constituent of $(\alpha_Q)^P = (\alpha^G)_P$, and thus some irreducible constituent χ of α^G is a member of $\mathrm{Irr}(G|\theta)$. Then $\chi(1) = \theta(1)$ is a p-power, and since $A \triangleleft G$ and α lies under χ, it follows that α has p-power degree, as wanted.

Since A/Q is a p'-group, we see that $\varphi(1) = (\varphi^A(1))_p$, and thus some irreducible constituent α of φ^A has degree with p-part not exceeding $\varphi(1)$. Since $\alpha(1)$ is a p-power and $\alpha(1) \geq \varphi(1)$, it follows that $\alpha(1) = \varphi(1)$, and thus α is an extension of φ. Since $Q \triangleleft A$, it follows by Gallagher's theorem that if β is an irreducible character of A/Q, then $\alpha\beta \in \mathrm{Irr}(A|\varphi)$, and hence $\beta(1)$ is a p-power. But A/Q is a p'-group, and thus $\beta(1) = 1$, and A/Q is abelian. A complement for Q in A/Q is thus an abelian subgroup of G of order $|G : P|$, as desired. □

Lemma 5.4. *Let $N \triangleleft G$ and $\beta \in \mathrm{Irr}(N)$ be G-invariant, and assume that $\mathrm{cd}(G|\beta) = \{e\}$. Suppose that the degree and determinantal order of β are powers of p, and let $P/N \in \mathrm{Syl}_p(G/N)$. Then e is a power of p, and every member of $\mathrm{Irr}(G|\beta)$ restricts irreducibly to P.*

Proof. Let q be a prime different from p, and let $S/N \in \mathrm{Syl}_q(G/N)$. Then β extends to $\gamma \in \mathrm{Irr}(S)$ by Corollary 8.16 of [I2], and since q does not divide $\gamma(1)$, some irreducible constituent of γ^G also has q'-degree. Thus q does not divide e, and hence e is a p-power.

Now let $\theta \in \mathrm{Irr}(P|\beta)$. Then θ^G has degree $\theta(1)|G : P|$, which must be a multiple of e, and thus since e is a p-power, it follows that e divides $\theta(1)$. But if $\chi \in \mathrm{Irr}(G|\theta)$, then $e = \chi(1) \geq \theta(1)$, and equality holds. Then $\chi_P = \theta$, and the proof is complete. □

Proof of Theorem 5.2. Let $\beta \in \mathrm{Irr}(U)$, and suppose that $\beta(1) > 1$. We work to derive a contradiction. Since $\beta(1)$ is divisible by p, we have $\mathrm{cd}(G|\beta) = \{n\}$, where n is the unique member of $\mathrm{cd}(G)$ that is divisible by p. If $T = G_\beta$, therefore, then $\mathrm{cd}(T|\beta) = \{e\}$, where $e = n/|G : T|$.

Let $Q \in \mathrm{Syl}_p(T)$ and $Q \subseteq P \in \mathrm{Syl}_p(G)$. By Lemma 5.4, we deduce that e is a power of p and that every member of $\mathrm{Irr}(T|\beta)$ restricts irreducibly to Q.

By Theorem C, we know that G/K has a simple socle, where K is the largest p-solvable normal subgroup of G, and also that K/U is a p'-group. By Theorem 5.1, the Sylow p-subgroups of G/K are abelian of order n_p, and the same is therefore true about G/U. Thus P/U is abelian of order n_p, and hence

$$|Q : U| = \frac{|P : U|}{|P : Q|} = \frac{n_p}{|G : T|_p} = \left(\frac{n}{|G : T|}\right)_p = e_p = e\,.$$

If $\theta \in \mathrm{Irr}(Q|\beta)$, then we know that every member of $\mathrm{Irr}(T|\theta)$ restricts irreducibly to Q, and so by Lemma 5.3, it follows that T has an abelian subgroup of order $|T : Q|$, and thus the same is true for T/U.

Now G/K does not have a normal Sylow p-subgroup, and so by the Ito-Michler theorem, there exists $\xi \in \mathrm{Irr}(G/K)$ with $\xi(1) = n$. Let η be an irreducible constituent of ξ_T, so that ξ is a constituent of η^G, and we have $n = \xi(1) \leq \eta(1)|G : T|$. Then $\eta(1) \geq n/|G : T| = e$. But T/U has an abelian subgroup A/U of order

$|T:Q|$. Then

$$|T:A| = \frac{|T:U|}{|A:U|} = \frac{|T:U|}{|T:Q|} = |Q:U| = e\,,$$

and since $U \subseteq \ker(\eta)$ and A/U is abelian, we have $\eta(1) \leq |T:A| = e$. It follows that $\eta(1) = e$, and thus $\xi(1) = \eta(1)|G:T|$ and therefore $\xi = \eta^G$. Also, since $\eta(1) = |T/U : A/U|$, we deduce that η (and therefore ξ) is induced from a linear character of the abelian subgroup A/U of G/U. In particular, since $K \subseteq \ker(\xi)$, we have $K \subseteq A$, and thus viewing ξ as a character of G/K, we see that it is induced from a linear character of the abelian subgroup A/K. By Lemma 2.6, it follows that A/K contains a normal subgroup N/K of G/K and that ξ vanishes on $G-N$. But then $N > \ker(\xi) \supseteq K$, and this is impossible since K is maximal among p-solvable normal subgroups of G, and yet $N > K$ and N/K is abelian. This completes the proof. □

We are finally ready to prove Theorem A, which we restate here.

Theorem 5.5. *Let G be a finite group with exactly one irreducible character degree n divisible by p. Let $P \in \mathrm{Syl}_p(G)$ and $U = \mathbf{O}_p(G)$, and assume that $U < P$. Then*

(a) *U is abelian.*
(b) *P/U is abelian, and if G is p-solvable, P/U is cyclic.*
(c) *$|P/U| = n_p$.*
(d) *P/U is a TI-set in G/U.*

Proof. By Theorem 3.1 and Corollary 3.4 we may assume that G is not p-solvable. In particular, a Sylow p-subgroup of G is not normal. Let $U = \mathbf{O}_p(G)$, and let $K/U = \mathbf{O}_{p'}(G/U)$, as in Theorem C. By Theorem C, we know that Theorem 5.1 applies to G/K, and hence the Sylow p-subgroups of G/K are abelian TI-sets of order n_p, where n is the unique multiple of p in $\mathrm{cd}(G/K)$ and hence in $\mathrm{cd}(G)$. It follows by Theorem 3.2 that the Sylow p-subgroups of G/U are abelian TI-sets of order n_p. The result now follows from Theorem 5.2. □

6. Almost simple groups I

Here and in the next section, we prove Theorems 2.1 and 5.1. Our proofs would be substantially easier if we wanted these results only for simple groups, but we do, in fact, need them more generally for almost simple groups. Recall that a finite group G is **almost simple** if its socle is a nonabelian simple group S. In this case, $\mathbf{C}_G(S) = 1$, and we can assume that $S \triangleleft G \subseteq \mathrm{Aut}(S)$.

We will rely heavily on the Deligne-Lusztig theory of complex representations of finite groups of Lie type (see [C] and [DM]).

Recall that if ℓ and p are primes and n is a positive integer, then ℓ is a **Zsigmondy prime** divisor of $p^n - 1$ if ℓ divides $p^n - 1$, but ℓ does not divide $p^m - 1$ for $0 < m < n$. In fact, Zsigmondy prime divisors almost always exist.

Lemma 6.1. *Let p be a prime and $n \geq 2$ an integer. Assume that $(p,n) \neq (2,6)$ and, if $n = 2$, assume in addition that p is not a Mersenne prime. Then $p^n - 1$ has a Zsigmondy prime divisor and every such Zsigmondy prime divisor is at least $n+1$.*

Proof. See [Zs]. □

In the following, with q fixed by the context, we write Φ_m to denote $\Phi_m(q)$, where $\Phi_m(x)$ is the mth cyclotomic polynomial. Also, we will consider a number of variants of finite groups of Lie type as defined in [KL], and we will utilize certain semisimple elements in finite groups of Lie type whose existence was established in [MT].

Lemma 6.2. *Let $\mathcal{G}$ be a simple algebraic group defined over a field of characteristic $r > 0$, and let F be a Frobenius map on $\mathcal{G}$, with $q = r^f$ the common absolute value of eigenvalues of F. Suppose that, for $i = 1$ or $i = 2$, the Zsigmondy prime divisor p_i of $r^{m_i f} - 1$ exists, where m_i is as defined in Table I. Then $G = \mathcal{G}^F$ contains a semisimple element s_i of order p_i, with $|\mathbf{C}_G(s_i)|_{r'}$ as indicated in the table.*

TABLE I. Certain semisimple elements in finite groups of Lie type

L	$m = m_i$	$\lvert\mathbf{C}_G(s_i)\rvert_{r'}$
$SL_n(q)$, $n \geq 2$	n $n-1$	$(q^n-1)/(q-1)$ $q^{n-1}-1$
$SU_n(q)$, $2 \nmid n,\ n \geq 3$	$2n$ $2(n-2)$ 2	$(q^n+1)/(q+1)$ $(q^{n-2}+1)(q^2-1)$, $n \geq 5$ $(q+1)^2$, $n = 3$
$SU_n(q)$, $2 \mid n,\ n \geq 4$	$2(n-1)$ $2(n-3)$ 2	$q^{n-1}+1$ $(q^{n-3}+1)(q^3+1)(q^2-1)$, $n \geq 6$ $(q+1)^3$, $n = 4$
$Sp_{2n}(q)$, $Spin_{2n+1}(q)$	$2n$ $2(n-1)$	q^n+1 $(q^{n-1}+1)(q^2-1)$
$Spin^+_{2n}(q)$, $n \geq 4$	$2(n-1)$ n $n-1$	$(q^{n-1}+1)(q+1)$ q^n-1, $2 \nmid n$ $(q^{n-1}-1)(q-1)$, $2 \mid n$
$Spin^-_{2n}(q)$, $n \geq 4$	$2n$ $2(n-1)$	q^n+1 $(q^{n-1}+1)(q-1)$
${}^2B_2(q)$	4 1	$q \pm \sqrt{2q}+1$ $q-1$
${}^2G_2(q)$	6 1	$q \pm \sqrt{3q}+1$ $q-1$
${}^2F_4(q)$	12 6	$q^2+q+1 \pm (q+1)\sqrt{2q}$ q^2-q+1
${}^3D_4(q)$	12 6	q^4-q^2+1
$G_2(q)$	$6,\ 3$	Φ_m
$F_4(q)$	$12,\ 8$	Φ_m
$E_6(q)$	9 12	Φ_9 $\Phi_{12}\Phi_3$
${}^2E_6(q)$	18 12	Φ_{18} $\Phi_{12}\Phi_6$
$E_7(q)$	$18,\ 14$	$\Phi_m\Phi_2$
$E_8(q)$	$30,\ 24$	Φ_m

In this table, L is the Lie-type group of simply connected type corresponding to G.

Proof. This is a combination of Lemmas 2.3 and 2.4 of [MT]. □

The semisimple elements mentioned in Lemma 6.2 will be exploited in the following.

Lemma 6.3. *Let $\mathcal{G}$ be a simple algebraic group in characteristic r, let F be a Frobenius map on $\mathcal{G}$, and let $G = \mathcal{G}^F$. Let the pair $(\mathcal{G}^*, F^*)$ be dual to $(\mathcal{G}, F)$ and $G^* = (\mathcal{G}^*)^{F^*}$. Assume $s \in G^*$ is a semisimple element of order coprime to the order of both $\pi_1(\mathcal{G}^*)$ (the fundamental group of $\mathcal{G}^*$) and $\mathbf{Z}(G)$.*

(a) *Then there exists a character $\chi_s \in \mathrm{Irr}(G/Z(G))$ of degree $|G^* : \mathbf{C}_{G^*}(s)|_{r'}$.*
(b) *Let σ and σ^* be automorphisms of the (abstract) groups $\mathcal{G}$ and $\mathcal{G}^*$, respectively, induced by the field automorphism $x \mapsto x^q$ for some power q of r and such that $\sigma \circ F = F \circ \sigma$. Assume in addition that r does not divide $|(\mathcal{G}^*)^{\sigma^*}|$. Then χ_s is not σ-invariant.*

Proof. This is Lemma 2.5 of [DNT]. □

The following observation is well known.

Lemma 6.4. *Let $\mathcal{G}$ be a connected reductive algebraic group in characteristic p, let F be a Frobenius map on $\mathcal{G}$, and let $G = \mathcal{G}^F$. Then the kernel of every unipotent character of G contains $\mathbf{Z}(G)$.*

Proof. Observe that every unipotent character χ of G is the sum of a linear combination of the Deligne-Lusztig characters $R_{\mathcal{T},1}^{\mathcal{G}}$ and an orthogonal function f. Furthermore, f vanishes at any semisimple element of G (see for instance Lemma 10.2 of [GT]). In particular, $f(z) = 0 = f(1)$ if $z \in \mathbf{Z}(G)$. On the other hand, the explicit character formula for $R_{\mathcal{T},1}^{\mathcal{G}}$ (see [C]) implies that $R_{\mathcal{T},1}^{\mathcal{G}}(z) = R_{\mathcal{T},1}^{\mathcal{G}}(1)$. It follows that $\chi(z) = \chi(1)$, as desired. □

Lemma 6.5. *Let S be either a sporadic finite simple group or an alternating group A_n with $n \geq 6$. Then there is an odd prime p and characters $\alpha, \beta \in \mathrm{Irr}(S)$ of even degree such that p divides exactly one of $\alpha(1)$, $\beta(1)$.*

Proof. The sporadic groups and A_6 can be checked by using [Atlas] or the GAP software. Consider the case $S = \mathsf{A}_n$ with $n \geq 7$. For a partition λ of n, let $[\lambda]$ be the irreducible character of $G = \mathsf{S}_n$ labeled by λ. Note that the characters $[(n-2, 1^2)]$ and $[(n-2, 2)]$ have degrees $(n(n-3)/2)+1$ and $n(n-3)/2$, respectively, so exactly one of them has even degree, and both restrict irreducibly to S. Let α be the restriction to S of the one of even degree.

Assume first that n is odd. In this case $[(n-1, 1)]$ has even degree $n-1$ and it restricts irreducibly to S. We let $\beta = [(n-1, 1)]_S$. If $\alpha = [(n-2, 1^2)]_S$, then $\alpha(1) = (n-1)(n-2)/2$. Choosing an odd prime divisor p of $n-2$, we see that p divides $\alpha(1)$ but not $\beta(1)$. If $\alpha = [(n-2, 2)]_S$, then the greatest common divisor $(\alpha(1), \beta(1))$ divides 2. Also, $\alpha(1), \beta(1) \geq 6$, and so there exists some odd prime p which divides exactly one of $\alpha(1)$ or $\beta(1)$.

Assume finally that n is even. Then $[(n-3, 2, 1)]$ has even degree $n(n-2)(n-4)/3$ and it also restricts irreducibly to S. We denote its restriction to S by β. Suppose that $\alpha(1) = n(n-3)/2$. Now if $n-3 \neq 3^a$, then there is some prime divisor $p \geq 5$ of $n-3$, and p divides $\alpha(1)$ but not $\beta(1)$. If $n-3 = 3^a$, then 3^2 does not divide n. It follows that $p = 3$ divides $\alpha(1)$ but not $\beta(1)$. Finally, suppose $\alpha(1) = (n-1)(n-2)/2$. Now if $n-1 \neq 3^a$, then there is some prime divisor $p \geq 5$

of $n-1$, and p divides $\alpha(1)$ but not $\beta(1)$. If $n-1=3^a$, then since $n \geq 7$, we see that 3^2 does not divide $n-4$. It follows that $p=3$ divides $\alpha(1)$ but not $\beta(1)$. $\square$

Proposition 6.6. *Let p be any prime and S be a finite simple Lie-type group in characteristic p. Then one of the following holds.*

(i) *There are a prime ℓ and characters $\alpha, \beta \in \mathrm{Irr}(S)$ such that ℓ does not divide $\alpha(1)|\mathrm{Out}(S)|$, but p divides $\alpha(1)$ and $p\ell$ divides $\beta(1)$.*

(ii) *$S = PSL_2(q)$ for some $q = p^f$, and S has a unique irreducible character of degree divisible by p.*

Proof. We will view S as $G/\mathbf{Z}(G)$, where $G = \mathcal{G}^F$ is a Lie-type group of simply connected type defined over $\mathbb{F}_q$, and $q = p^f$. Let the pair $(\mathcal{G}^*, F^*)$ be dual to $(\mathcal{G}, F)$, and let $G^* = (\mathcal{G}^*)^{F^*}$. By Lemma 6.4, every unipotent character of G can be viewed as a character of S as well. In particular, we can always choose α to be the Steinberg character of G.

(1) First consider the case where $G = SL_n(q)$ for some integer $n \geq 2$. If $n=2$, we get conclusion (ii), so we will assume that $n \geq 3$. Recall that $\alpha(1) = q^{n(n-1)/2}$. Suppose that there exists a Zsigmondy prime divisor r of $p^{(n-1)f}-1$. In particular $r \geq (n-1)f+1 \geq 2f+1$ and $(r, q-1)=1$, whence $(r, |\mathrm{Out}(S)|)=1$. Then we choose $\ell = r$ and we let β be the unipotent character labeled by the partition $(n-1,1)$. This character has degree $q(q^{n-1}-1)/(q-1)$.

It remains to consider what happens when there is no such Zsigmondy prime r. These are the cases $(n,q)=(7,2)$, $(4,4)$, or $n=3$ and $q=p$ is a Mersenne prime. If $(n,q)=(7,2)$ or $(4,4)$, then $|\mathrm{Out}(S)|$ divides 2^2, so we can choose β as above and $\ell = 7$. Assuming that we are in the latter case, it is easy to check that $H = PGL_3(q)$ has an irreducible character χ of degree $q(q^2+q+1)$, that S is a normal subgroup of H of index $(3, q-1)$, and that $|\mathrm{Out}(S)| = 2(3, q-1)$. Now choose ℓ to be a Zsigmondy prime divisor of q^3-1 and let β be an irreducible constituent of χ_S. Then $\ell \geq 5$ and $p\ell \mid \beta(1)$.

(2) Next, we consider the case $G = SU_n(q)$ for some $n \geq 3$, so that $\alpha(1) = q^{n(n-1)/2}$. First suppose that $n \geq 4$ is even. The case $(n,q)=(4,2)$ can be handled directly using [Atlas], so we will assume that $(n,q) \neq (4,2)$. Hence there exists a Zsigmondy prime divisor ℓ of $p^{2(n-1)f}-1$. In particular, $\ell \geq 2(n-1)f+1 \geq 6f+1$ and $(\ell, q+1)=1$, whence $(\ell, |\mathrm{Out}(S)|)=1$. Choose β to be the unipotent character labeled by the partition $(n-1,1)$, so that β has degree $q(q^{n-1}+1)/(q+1)$.

Now we assume that $n \geq 5$ is odd. Suppose that there exists a Zsigmondy prime divisor ℓ of $p^{(n-1)f}-1$. In particular $\ell \geq (n-1)f+1 \geq 4f+1$ and $(\ell, q+1)=1$, whence $(\ell, |\mathrm{Out}(S)|)=1$. In this case, we choose β to be the unipotent character labeled by the partition $(n-1,1)$. Also β has degree $q(q^{n-1}-1)/(q+1)$.

It remains to consider the situation where there is no Zsigmondy prime ℓ, so that $(n,q)=(7,2)$. In this case $|\mathrm{Out}(S)|=2$, so we can choose β as before and take $\ell = 7$.

Finally, assume that $n=3$ (and $q \geq 3$). Then there exists a Zsigmondy prime divisor ℓ of $p^{6f}-1$. Observe that $\ell | (q^2-q+1)$, $\ell \geq 6f+1$, and so $(\ell, |\mathrm{Out}(S)|)=1$. It is easy to check that $H = PGU_3(q)$ has an irreducible character χ of degree $q(q^2-q+1)$ and that S is a normal subgroup of H of index $(3, q+1)$. Choose β to be an irreducible constituent of χ_S so that $p\ell$ divides $\beta(1)$.

(3) Next assume that $\mathcal{G}$ is of type B_n or C_n with $n \geq 2$. In particular, $\alpha(1) = q^{n^2}$ and $|\mathrm{Out}(S)|$ divides $2f$. If $q > 2$, choose β to be a unipotent character of degree

$(q^n+1)(q^n-q)/2(q-1)$. Since $q>2$, there exists a Zsigmondy prime divisor ℓ of $p^{2nf}-1$. Now observe that $p\ell$ divides $\beta(1)$ and $\ell \geq 2nf+1 \geq 4f+1$, and thus $(\ell, |\mathrm{Out}(S)|)=1$.

Assume that $q=2$. Since $Sp_4(2)' \cong \mathsf{A}_6$, we may assume $n \geq 3$. Now $S \cong G = Sp_{2n}(q)$ and G is isomorphic to its dual G^*. Choose $\lambda \in \bar{\mathbb{F}}_q$ of order $q+1$, and let $s \in G^*$ be $\mathcal{G}$-conjugate to $\mathrm{diag}(\lambda, \lambda^{-1}, 1, \ldots, 1)$. Then $\mathbf{C}_{G^*}(s) \cong C_{q+1} \times Sp_{2n-2}(q)$ has a unipotent character ψ of degree $q^{(n-1)^2}$. Choosing β to be the character of G labeled by s and ψ, we get $\beta(1) = q^{(n-1)^2}(q^{2n}-1)/(q+1)$. Finally, we can choose ℓ to be a Zsigmondy prime divisor of $q^{2n}-1$ if $n \geq 4$ and $\ell = 7$ if $n=3$.

(4) Let $\mathcal{G}$ be of type D_n, where $n \geq 4$. In particular $G = Spin^{\epsilon}_{2n}(q)$ with $\epsilon = \pm$ and $\alpha(1) = q^{n(n-1)}$. Now we can choose β to be the (unique) irreducible constituent of degree $(q^{2n}-q^2)/(q^2-1)$ of a rank 3 permutation character of G. (See [ST], for instance.) Also, choose ℓ to be a Zsigmondy prime divisor of $p^{(2n-2)f}-1$ if $(n,q) \neq (4,2)$ and $\ell = 7$ if $(n,q)=(4,2)$. Since $|\mathrm{Out}(S)|$ divides $24f$, we see that $p\ell$ divides $\beta(1)$ and $(\ell, |\mathrm{Out}(S)|)=1$.

(5) Finally, we consider the exceptional groups of Lie type. If $G = G_2(q)$ with $q \geq 3$ (respectively, ${}^3D_4(q)$, $F_4(q)$, $E_6(q)$, ${}^2E_6(q)$, $E_7(q)$, $E_8(q)$), then we can choose β to be a unipotent character of degree $q\Phi_2^2\Phi_6/2$ (respectively, $q\Phi_{12}$, $q^2\Phi_3^2\Phi_6^2\Phi_{12}$, $q\Phi_8\Phi_9$, $q\Phi_8\Phi_{18}$, $q\Phi_7\Phi_{12}\Phi_{14}$, $q\Phi_4^2\Phi_8\Phi_{12}\Phi_{20}\Phi_{24}$). We choose ℓ to be a Zsigmondy prime divisor of $p^{mf}-1$, with $m=6$ (respectively, $m=12$, $m=12$, $m=9$, $m=18$, $m=14$, $m=24$), and observe that ℓ divides Φ_m but it is coprime to $|\mathrm{Out}(S)|$. Finally, if $G = {}^2B_2(q)$ with $q \geq 8$ (respectively, ${}^2G_2(q)$ with $q \geq 27$, ${}^2F_4(q)'$), then we can choose β to be a unipotent character of degree $(q-1)\sqrt{q/2}$ (respectively, $(q^2-1)\sqrt{q/3}$, $q^5\Phi_6\Phi_{12}$ (or half of it if $q=2$)). In these cases, we choose ℓ to be a Zsigmondy prime divisor of $p^{mf}-1$, with $m=1$ (respectively, $m=2$, $m=12$). $\square$

Theorem 6.7. *Let S be a finite simple nonabelian group. Then one of the following holds.*

(i) *There is a prime p not dividing $|\mathrm{Out}(S)|$ and $\alpha, \beta \in \mathrm{Irr}(S)$ of even degree such that p divides exactly one of $\alpha(1)$ or $\beta(1)$.*
(ii) *$S \cong PSL_2(q)$ for some $q = 2^f \geq 4$, and S has a unique irreducible character of even degree.*

Proof. In view of Lemma 6.5 and Proposition 6.6, we need to consider only the case where S is a finite simple Lie-type group over a field $\mathbb{F}_q$ in characteristic $p>2$. We will use the notation of the proof of Proposition 6.6. In particular, observe that Φ_m is even if and only if $m = 2^a$ for some $a \geq 0$.

(1) First we consider the case of the exceptional groups. In all but one case, we will exhibit two unipotent characters α, β of even degree, and a prime ℓ such that ℓ divides $\beta(1)$ but not $\alpha(1) \cdot |\mathrm{Out}(S)|$. The prime ℓ is chosen to be a Zsigmondy prime divisor of $p^{mf}-1$ for a suitable m. The degrees of α, β and the integer m are: $q\Phi_1^2\Phi_3/2$, $q\Phi_2^2\Phi_6/2$, and $m=6$ if $S = G_2(q)$; $q^3\Phi_1^2\Phi_3^2/2$, $q^3\Phi_1^2\Phi_{12}$ and $m=12$ if $S = {}^3D_4(q)$; $q\Phi_2^2\Phi_6^2\Phi_8/2$, $q^3\Phi_4^2\Phi_8\Phi_{12}$, and $m=12$ if $S = F_4(q)$; $q\Phi_8\Phi_9$, $q^2\Phi_4\Phi_5\Phi_8\Phi_{12}$, and $m=12$ if $S = E_6(q)$; $q^2\Phi_4\Phi_8\Phi_{10}\Phi_{12}$, $q\Phi_8\Phi_{18}$, and $m=18$ if $S = {}^2E_6(q)$; $q^6\prod_{m=5,7,8,9,10,14,18}\Phi_m$, $q^{10}\prod_{m=5,7,8,9,10,12,14,18}\Phi_m$, and $m=12$ if $S = E_7(q)$; $q\Phi_4^2\Phi_8\Phi_{12}\Phi_{20}\Phi_{24}$, $q^3\Phi_4^2(\prod_{m=7,8,9,12,14,20,24,30}\Phi_m)/2$, and $m=30$ if

$S = E_8(q)$. If $S = {}^2G_2(q)$, then one can choose α of degree $(q^2-1)\sqrt{q/3}$, ℓ a Zsigmondy prime divisor of $p^{6f}-1$, and β of degree $(q^2-1)(q+\epsilon\sqrt{3q}+1)$, where $\epsilon = \pm$ is chosen such that $\ell|(q+\epsilon\sqrt{3q}+1)$.

From now on we may assume that S is a classical group.

(2) Assume that $S = PSL_2(q)$. Since $PSL_2(4) \cong PSL_2(5)$, we may assume that $q \geq 7$, whence S has irreducible characters of degrees $q-1$ and $q+1$. If $f \geq 2$, then since $p \geq 3$ there exists a Zsigmondy prime divisor ℓ of $p^{2f}-1$, and $\ell \geq 2f+1$. In this case we choose $\alpha(1) = q-1$ and $\beta(1) = q+1$. If $f = 1$, then $|\mathrm{Out}(S)| = 2$, and either $q+1$ or $q-1$ is not a 2-power. In this case choose ℓ to be an odd prime divisor of $q-\epsilon$ for some $\epsilon = \pm 1$, and choose $\alpha(1) = q+\epsilon$ and $\beta(1) = q-\epsilon$.

(3) Here we consider the case $S = PSL_n^\epsilon(q)$, where $\epsilon = +$ stands for $PSL_n(q)$ and $\epsilon = -$ stands for $PSU_n(q)$.

(3a) First assume that $n = 3$. Then we can choose α of degree $q(q-\epsilon)$. It is easy to see that $H = PGL_3^\epsilon(q)$ has an irreducible character χ of degree $q^3-\epsilon$ and that S is a normal subgroup of H of index $(3, q-\epsilon)$. Since $p \geq 3$, there is a Zsigmondy prime divisor ℓ of $p^{3f}-1$ if $\epsilon = +$ and of $p^{6f}-1$ if $\epsilon = -$. Clearly, $\ell \geq 3f+1$. Now we just choose β to be an irreducible constituent of χ_S and observe that $2\ell|\beta(1)$ but ℓ does not divide $\alpha(1)\cdot|\mathrm{Out}(S)|$.

(3b) Next assume that $S = PSL_n^\epsilon(q)$ with $n \geq 4$. Assume in addition that n is odd if $\epsilon = -$. Since $p \geq 3$, there is a Zsigmondy prime divisor p_1 of $p^{nf}-1$ if $\epsilon = +$ and of $p^{2nf}-1$ if $\epsilon = -$. By Lemma 6.2, there is a semisimple element $s_1 \in G^*$ of order p_1, which has connected centralizer in $\mathcal{G}^*$ and $|\mathbf{C}_{G^*}(s_1)| = (q^n-\epsilon^n)/(q-\epsilon)$. Thus it defines a semisimple character χ_{s_1} of G of degree $\prod_{i=1}^{n-1}(q^i-\epsilon^i)$. Since $|s_1| = p_1 > n$, χ_{s_1} contains $\mathbf{Z}(G)$ in its kernel, and so we can take $\alpha = \chi_{s_1}$. Next, we choose $\theta \in \bar{\mathbb{F}}_q$ of order $q^2+\epsilon q+1$ and consider a semisimple element $s_2 \in H^* = SL_n^\epsilon(q)$ which is $\mathcal{G}$-conjugate to $\mathrm{diag}(\theta^{q^2}, \theta^{\epsilon q}, \theta, 1, \ldots, 1)$. Then $|\mathbf{C}_{H^*}(s_2)| = (q^3-\epsilon)\cdot|SL_{n-3}^\epsilon(q)|$. As above, s_2 defines a semisimple character χ_{s_2} of $H = PGL_n^\epsilon(q)$. This character has degree $(q^{n-2}-\epsilon^{n-2})(q^{n-1}-\epsilon^{n-1})(q^n-\epsilon^n)/(q^3-\epsilon)$, and S is a normal subgroup of H of index $(n, q-\epsilon)$. Now take β to be an irreducible constituent of $(\chi_{s_2})_S$ and $\ell = p_1$.

(3c) Now we assume that $S = PSU_n(q)$ with $n \geq 4$ and n even. Since $p \geq 3$, there is a Zsigmondy prime divisor $p_1 > 2(n-1)f$ of $p^{2(n-1)f}-1$. By Lemma 6.2, there is a semisimple element $s_1 \in G^*$ of order p_1, which has connected centralizer in $\mathcal{G}^*$ and $|\mathbf{C}_{G^*}(s_2)| = q^{n-1}+1$. Thus it defines a semisimple character χ_{s_1} of G of degree $(q^n-1)\prod_{i=2}^{n-2}(q^i-(-1)^i)$. Now take $\alpha = \chi_{s_1}$, choose β as in (3b) and set $\ell = p_1$.

(4) For the remaining classical groups, notice that any semisimple element $s \in G^*$ of odd order has a connected centralizer in $\mathcal{G}^*$. Hence it corresponds to a character $\chi_s \in \mathrm{Irr}(G)$ with its kernel containing $\mathbf{Z}(G)$.

Assume that $S = PSp_{2n}(q)$ or $\Omega_{2n+1}(q)$ with $n \geq 2$. Since p is odd, there is a Zsigmondy prime divisor $p_1 > 2nf$ of $p^{2nf}-1$. By Lemma 6.2, there is a semisimple element $s_1 \in G^*$ of order p_1 with $|\mathbf{C}_{G^*}(s_1)|_{p'} = q^n+1$. Now χ_{s_1} has degree equal to $(q^n-1)\prod_{i=1}^{n-1}(q^{2i}-1)$, and we can take $\alpha = \chi_{s_1}$.

Assume that $n \geq 3$. Then there is a Zsigmondy prime divisor $p_2 > 2(n-1)f$ of $p^{2(n-1)f}-1$. By Lemma 6.2, there is a semisimple element $s_2 \in G^*$ of order p_2 with $|\mathbf{C}_{G^*}(s_2)|_{p'} = (q^{n-1}+1)(q^2-1)$. Now $\chi_{s_2}(1) = (q^{2n}-1)(q^{n-1}-1)\prod_{i=2}^{n-2}(q^{2i}-1)$, and we can take $\beta = \chi_{s_2}$. Observe that $p_1 > 2nf$ divides $\beta(1)$ but not $\alpha(1)$, so we can take $\ell = p_1$.

Now suppose that $n = 2$ and so $S \cong PSp_4(q)$. Then choose $\theta \in \bar{\mathbb{F}}_q$ of order $q+1$ and consider a semisimple element $s_3 \in H^* = Sp_4(q)$ which is $\mathcal{G}$-conjugate to $\mathrm{diag}(\theta, \theta^q, 1, 1)$. Then $\mathbf{C}_{H^*}(s_3) = C_{q+1} \times Sp_2(q)$, and so s_3 defines a semisimple character χ_{s_3} of $H = PCSp_4(q)$ of degree $(q-1)(q^2+1)$ and S is a normal subgroup of H of index 2. Now we choose β to be an irreducible constituent of $(\chi_{s_3})_S$ and $\ell = p_1$.

(5) Finally, assume that $S = P\Omega^{\epsilon}_{2n}(q)$ with $n \geq 4$ and $\epsilon = \pm$. Since $p \geq 3$, there is a Zsigmondy prime divisor $p_1 > 2(n-1)f$ of $p^{2(n-1)f} - 1$. By Lemma 6.2, there is a semisimple element $s_1 \in G^*$ of order p_1 with $|\mathbf{C}_{G^*}(s_1)|_{p'} = (q^{n-1}+1)(q+\epsilon)$. Now $\chi_{s_1}(1) = (q-\epsilon)(q^{n-1}-1)(q^n-\epsilon)\prod_{i=2}^{n-2}(q^{2i}-1)$, and we can take $\alpha = \chi_{s_1}$.

First consider the case $\epsilon = -$. Then there is a Zsigmondy prime divisor $p_2 > 2nf$ of $p^{2nf} - 1$. By Lemma 6.2, there is a semisimple element $s_2 \in G^*$ of order p_2 with $|\mathbf{C}_{G^*}(s_2)|_{p'} = q^n + 1$. Now we take $\beta = \chi_{s_2}$, which has degree $\prod_{i=1}^{n-1}(q^{2i}-1)$, and $\ell = p_1$.

Now we assume that $\epsilon = +$. If n is odd, then there is a Zsigmondy prime divisor $p_2 > nf$ of $p^{nf} - 1$. By Lemma 6.2, there is a semisimple element $s_2 \in G^*$ of order p_2, which defines a semisimple character χ_{s_2} of S of degree $\prod_{i=1}^{n-1}(q^{2i}-1)$. If n is even, then there is a Zsigmondy prime divisor $p_2 > (n-1)f$ of $p^{(n-1)f} - 1$. By Lemma 6.2, there is a semisimple element $s_2 \in G^*$ of order p_2, which defines a semisimple character χ_{s_2} of S of degree $(q+1)(q^{n-1}+1)(q^n-1)\prod_{i=2}^{n-2}(q^{2i}-1)$. In both cases, we choose $\beta = \chi_{s_2}$ and observe that $\ell = p_1$ divides $\beta(1)$ but not $\alpha(1)$. □

7. Almost simple groups II

We continue to prove several further results on almost simple groups.

Theorem 7.1. *Suppose that the socle of G is a finite nonabelian simple group S and let p be a prime such that p divides $|G/S|$ but not $|S|$. Then there exist faithful irreducible characters α, β of G of distinct degrees divisible by p.*

Proof. (1) By hypothesis, $S \lhd G \leq \mathrm{Aut}(S)$, whence p divides $|\mathrm{Out}(S)|$ but not $|S|$. Now the well known description of $\mathrm{Out}(S)$ (see for instance [GLS]) implies that S is a finite simple group of Lie type in some characteristic $r \neq p$ and p is the order of some field automorphism of S. We will view S as $L/\mathbf{Z}(L)$, where $L = \mathcal{G}^F$ for some simple simply connected algebraic group $\mathcal{G}$ in characteristic r and some Frobenius map F on $\mathcal{G}$. Let the pair $(\mathcal{G}^*, F^*)$ be dual to $(\mathcal{G}, F)$ and set $H = \mathcal{G}^{*F^*}$. Up to $\mathrm{Aut}(S)$-conjugacy (which does not change the isomorphism type of S), we may assume that G contains the field automorphism σ of order p of S, which is induced by a field automorphism (which without loss we also denote by σ) of standard form of the (abstract) group $\mathcal{G}$ (see [GLS]). Let σ^* denote the corresponding automorphism of $\mathcal{G}^*$. By Lemma 2.5.5 of [GLS], we have that

$$\sigma \circ F = F \circ \sigma. \tag{A1}$$

Let $\pi_1(\mathcal{G}^*)$ denote the fundamental group of $\mathcal{G}^*$ as usual. Assume that $\ell \neq r$ is a prime divisor of $|H| = |L|$ such that

(A2) ℓ is coprime to the orders of $\pi_1(\mathcal{G}^*)$, $\mathbf{Z}(L)$, $\mathcal{G}^{*\sigma^*}$, and $\mathrm{Out}(S)$.

Choose $s \in H$ to be any element of order ℓ. By Lemma 6.3, the facts (A1) and (A2) imply that the corresponding semisimple character χ_s of L is irreducible, of degree $|H : \mathbf{C}_H(s)|_{r'}$, contains $\mathbf{Z}(L)$ in its kernel, and is not σ-invariant. In this case, we can view χ_s as an irreducible character of S. Now, consider any character $\tau_s \in \mathrm{Irr}(G|\chi_s)$. Since χ_s is not σ-invariant, p divides $\tau_s(1)$. On the other hand, $\tau_s(1)/\chi_s(1)$ divides the order of $G/S \leq \mathrm{Out}(S)$ by Corollary (11.29) of [I2], and so it is coprime to ℓ.

(2) We observe that it suffices to find two semisimple elements s_i of H of order ℓ_i, $i = 1, 2$, where ℓ_i satisfies condition (A2) and moreover for some $j \in \{1, 2\}$,

$$\ell_j \text{ divides } \chi_{3-j}(1) \text{ but not } \chi_j(1). \tag{A3}$$

(Here and in what follows, we denote χ_{s_i} by χ_i and τ_{s_i} by τ_i for brevity.) Indeed, the discussion in (1) implies that τ_i is an irreducible character of G of degree divisible by p and not containing S in its kernel. Furthermore, (A3) yields that ℓ_j divides $\tau_{3-j}(1)$ but not $\chi_j(1)$. But ℓ_j is coprime to $\tau_j(1)/\chi_j(1)$; hence it is coprime to $\tau_j(1)$ as well. Setting $\{\alpha, \beta\} = \{\tau_1, \tau_2\}$, we get $\alpha(1) \neq \beta(1)$.

(3) Now we set forth to find the desired elements s_1, s_2 in H. To do this, we will use Lemma 6.2. To illustrate the approach, let us consider the case $L = {}^2B_2(q)$ with $q = 2^f$ (and $r = 2$, $p|f$). Here, $|\mathrm{Out}(S)| = f$, $|\pi_1(\mathcal{G}^*)| = |\mathbf{Z}(L)| = 1$. Then we can take ℓ_1 and ℓ_2 to be Zsigmondy prime divisors of $2^{4f} - 1$ and $2^f - 1$, respectively. Notice that $\ell_i \geq f + 1$. Furthermore, any prime divisor of $|\mathcal{G}^{*\sigma^*}|$ divides $2(2^{4f/p} - 1)$ and $p \geq 3$, so it cannot be equal to any ℓ_i. Thus ℓ_i satisfies (A2). Now Lemma 6.2 yields the desired elements s_1, s_2, and ℓ_2 divides $\chi_1(1) = (q-1)(q \mp \sqrt{2q} + 1)$ but not $\chi_2(1) = q^2 + 1$.

Notice that ${}^2B_2(q)$ are the only nonabelian simple groups of order coprime to 3. Therefore, from now on we may assume $p \geq 5$, and $q = r^f$ is the common absolute value of eigenvalues of F for some f divisible by p. We will use Lemma 6.2 to handle the remaining exceptional groups of Lie type. We give the detailed argument in the cases $L \in \{E_6(q), {}^2E_6(q)\}$ and $L = {}^3D_4(q)$; the other cases are handled similarly. In the former case, set $\epsilon = 1$ for $E_6(q)$ and $\epsilon = -1$ for ${}^2E_6(q)$. In this case, $|\mathrm{Out}(S)|$ divides $6f$, and $|\pi_1(\mathcal{G}^*)|$, $|\mathbf{Z}(L)| \leq 3$. Then take ℓ_1 to be a Zsigmondy prime divisor of $r^{mf} - 1$, with $m = 9$ for $E_6(q)$ and $m = 18$ for ${}^2E_6(q)$, and take ℓ_2 to be a Zsigmondy prime divisor of $r^{12f} - 1$. In particular, $\ell_i \geq 9f + 1$. Here, each prime divisor of $|\mathcal{G}^{*\sigma^*}|$ divides $r(r^{Nf/p} - 1)$ for some $N \leq 18$, so it cannot be equal to any ℓ_i. Also, ℓ_2 divides $\chi_1(1) = D/\Phi_m$ but not $\chi_2(1) = D/\Phi_{12}\Phi_{m/3}$, where $D = \prod_{i=2,5,6,8,9,12}(q^i - \epsilon^i)$.

Consider the latter case: $L = {}^3D_4(q)$. Here, $|\mathrm{Out}(S)| = 3f$, and $|\pi_1(\mathcal{G}^*)|$, $|\mathbf{Z}(L)| \leq 4$. Choose ℓ_1, respectively ℓ_2, to be a Zsigmondy prime divisor of $r^{12f} - 1$, respectively $r^{6f} - 1$; in particular, $\ell_i \geq 6f + 1$. Then ℓ_i satisfies (A2) and ℓ_1 divides $\chi_2(1) = D/|\mathbf{C}_H(s_2)|_{r'}$ but not $\chi_1(1) = D/\Phi_{12}$, where $D = (q^8 + q^4 + 1)(q^6 - 1)(q^2 - 1)$ (the possibilities for $|\mathbf{C}_H(s_2)|$ are listed in the proof of Lemma 2.3 of [MT]).

(4) Next we deal with the classical groups. Again we give the detailed argument for the unitary groups; other cases are treated similarly. Assume that $L = SU_n(q)$ with $q = r^f$ and $n \geq 3$. In this case, $|\mathrm{Out}(S)|$ divides $2nf$, and $|\pi_1(\mathcal{G}^*)|$, $|\mathbf{Z}(L)| \leq n$. If n is even, then take ℓ_1 (respectively ℓ_2) to be a Zsigmondy prime divisor of $r^{2(n-1)f} - 1$ (respectively $r^{2(n-3)f} - 1$). If n is odd, take ℓ_1 (respectively ℓ_2) to be a Zsigmondy prime divisor of $r^{2nf} - 1$ (respectively $r^{2(n-2)f} - 1$). In either case, $\ell_i > \max\{2, n, f\}$. Any prime divisor of $|\mathcal{G}^{*\sigma^*}|$ divides $r(r^{Nf/p} - 1)$ for some

$N \leq 2n$, so it cannot be equal to any ℓ_i. Now Lemma 6.2 provides us with the desired elements s_1, s_2. Furthermore, ℓ_1 divides

$$\chi_2(1) = \begin{cases} D/(q^2-1)(q^3+1)(q^{n-3}+1), & 2|n,\ n \geq 6, \\ D/(q+1)^3, & n = 4, \\ D/(q^2-1)(q^{n-2}+1), & 2 \not| n,\ n \geq 5, \\ D/(q+1)^2, & n = 3, \end{cases}$$

but not

$$\chi_1(1) = \begin{cases} D/(q^{n-1}+1), & 2|n, \\ D(q+1)/(q^n+1), & 2 \not| n, \end{cases}$$

where $D = \prod_{i=2}^{n}(q^i - (-1)^i)$. □

Proposition 7.2. *Let $\mathsf{A}_n \lhd G \leq \mathsf{S}_n$ with $n \geq 7$, and let p be an odd prime divisor of $|G|$. Then G has two irreducible characters of distinct degrees divisible by p.*

Proof. (1) As in Lemma 6.5, for a partition λ of n, let $[\lambda]$ be the irreducible character of $G = \mathsf{S}_n$ labeled by λ. Also, we let $\langle\lambda\rangle$ be an irreducible constituent of $[\lambda]_S$. Since $p > 2$, then $[\lambda]$ has degree divisible by p if and only if $\langle\lambda\rangle$ has degree divisible by p.

If p does not divide n, then we set $\alpha = (n-p+1, 1^{p-1})$. Then $[\alpha]$ has degree divisible by p. Indeed,

$$\lfloor (n-p)/p \rfloor \leq \lfloor (n-p-1)/p \rfloor = \lfloor (n-1)/p \rfloor - 1,$$

and so p divides $[\alpha](1) = \binom{n-1}{p-1}$. Also, $\langle\alpha\rangle(1) = [\alpha](1)$ unless α is self-conjugate, which happens exactly when $n = 2p-1$.

If p does not divide $n(n+1)$, then we set $\beta = (n-p+2, 1^{p-2})$. Then $[\beta]$ has degree divisible by p. Indeed,

$$\lfloor (n-p+1)/p \rfloor \leq \lfloor (n-p-1)/p \rfloor = \lfloor (n-1)/p \rfloor - 1,$$

and so p divides $[\beta](1) = \binom{n-1}{p-2}$. Also, $\langle\beta\rangle(1) = [\beta](1)$ unless β is self-conjugate, which happens exactly when $n = 2p-3$.

Now assume that p does not divide $n(n+1)$ and $n \neq 2p-2$. Then $[\alpha]$, $[\beta]$ have degrees divisible by p, and $[\alpha](1)/[\beta](1) = (n-p+1)/(p-1) \neq 1$. So we are done if $G = \mathsf{S}_n$. Observe that $n \neq 2p-1$. If furthermore $n \neq 2p-3$, then since $[\alpha]$ and $\langle\alpha\rangle$, respectively $[\beta]$ and $\langle\beta\rangle$, have the same degree, we are also done if $G = \mathsf{A}_n$. Assume that $n = 2p-3 > 3$. Then

$$\frac{\langle\alpha\rangle(1)}{\langle\beta\rangle(1)} = \frac{2(n-p+1)}{p-1} = \frac{2p-4}{p-1} > 1.$$

(2) Here we consider the case $5 \leq p \,|\, (n+1)$. Since $p \leq n$, we must have $n \geq 2p-1$. Setting $\gamma = (n-p+2, 2, 1^{p-4})$, we observe that p divides

$$[\gamma](1) = \binom{n-2}{p-4} \cdot \frac{n(n+1-p)}{p-2}\ .$$

As in (1), we have that $[\alpha]$ has degree divisible by p. We claim that $[\alpha]$ and $[\gamma]$, respectively $\langle\alpha\rangle$ and $\langle\gamma\rangle$, have distinct degrees. Assume the contrary. Then there

are $r, s \in \{0, 1\}$ such that

$$1 = \frac{2^s \cdot \binom{n-1}{p-1}}{2^r \cdot \binom{n-2}{p-4} \cdot n(n+1-p)/(p-2)} = \frac{2^s(n-1)(n-p+2)}{2^r n(p-1)(p-3)}.$$

It follows that n divides $2(n-p+2)$, which is a contradiction as $n \geq 2p-1$.

Next we assume that $5 \leq p \mid n$. Then $[(n-2,2)]$ and $\langle(n-2,2)\rangle$ have degree $n(n-3)/2$ divisible by p, and $[(n-3,2,1)]$ and $\langle(n-3,2,1)\rangle$ have degree $n(n-2)(n-4)/3$, also divisible by p. These degrees are distinct since $n > 5$.

(3) Here we consider the case where $p = 3|n(n+1)$. First assume that $3|(n+1)$. The statement is clear in the case $n = 8$ (see the [Atlas]), so we may assume $n \geq 11$. Then $[\alpha]$ and $\langle\alpha\rangle$ have degree $(n-1)(n-2)/2$ divisible by 3. Also, $[(n-5,1^5)]$ has degree $\binom{n-1}{5}$ divisible by 3, which is greater than $(n-1)(n-2)$, so we are done. Now assume that $3|n$ and $n \geq 9$. Then $[(n-2,2)]$ and $\langle(n-2,2)\rangle$ have degree $n(n-3)/2$ divisible by 3, and $[(n-4,2,1^2)]$ and $\langle(n-4,2,1^2)\rangle$ have degree $n(n-2)(n-3)(n-5)/8$ divisible by 3. These degrees are distinct since $n > 6$.

(4) Finally, assume that $n = 2p-2$ and $p \geq 5$. We already mentioned in (1) that $[\alpha]$ and $\langle\alpha\rangle$ have degree $\binom{2p-3}{p-1}$ divisible by p. Also, $[(p-3,2,1^{p-1})]$ and $\langle(p-3,2,1^{p-1})\rangle$ have degree $\binom{2p-4}{p-1} \cdot (2p-2)(p-4)/(p+1)$ divisible by p, which is different from $[\alpha](1)$. □

Theorem 7.3. *Suppose that the socle of G is a finite nonabelian simple group S, and let p be any odd prime divisor of $|S|$. Then one of the following holds.*

(i) *G has two faithful irreducible characters of distinct degrees divisible by p.*
(ii) *$S = PSL_2(q)$.*
(iii) *$(S,p) = (M_{11},3)$, $(J_1,3)$, or $(J_1,5)$.*

Proof. (1) The case where S is a sporadic simple group can be directly verified by using [Atlas] or GAP. On the other hand, the case of alternating groups is done in Proposition 7.2. Recall that $\mathsf{A}_5 \cong PSL_2(5)$ and $\mathsf{A}_6 \cong PSL_2(9)$.

If we assume that S is a finite group of Lie type in characteristic p, then the statement follows from Proposition 6.6. So we may assume that S is a finite group of Lie type in characteristic $r \neq p$ and not of type A_1.

We claim that it is enough to show that there exists some group H with $S \lhd H \leq \mathrm{Aut}(S) = A$, possessing characters $\gamma, \delta \in \mathrm{Irr}(H)$ such that

(B1) $\gamma(1)_p\ ,\ \delta(1)_p > |H/S|_p$, and

(B2) either $\gamma(1)/\delta(1) > |\mathrm{Out}(S)|$,

or there is some prime ℓ that divides $\gamma(1)$ but not $\delta(1) \cdot |\mathrm{Out}(S)|$.

Indeed, writing $\gamma_S = \sum_{i=1}^t \gamma_i$ for some $\gamma_i \in \mathrm{Irr}(S)$, we know that t divides $|H/S|$. But $\gamma(1)_p > |H/S|_p$, hence $p|\gamma_i(1)$. Now choose $\alpha \in \mathrm{Irr}(G)$ to be an irreducible constituent of $(\gamma^A)_G$ such that α_S contains γ_1. Since $S \lhd G$, we conclude that $p|\alpha(1)$ and α is faithful on S. Similarly, there is a faithful character $\beta \in \mathrm{Irr}(G)$ of

degree divisible by p which is an irreducible constituent of $(\delta^A)_G$. Observe that

$$\alpha(1) \geq \gamma_1(1) = \gamma(1)/t \geq \frac{\gamma(1)}{|H/S|} > \frac{\delta(1)\cdot|\mathrm{Out}(S)|}{|H/S|} = \delta(1)\cdot|A:H| = \delta^A(1) \geq \beta(1),$$

and so $\alpha(1) > \beta(1)$ if $\gamma(1)/\delta(1) > |\mathrm{Out}(S)|$. Consider the case when the prime ℓ in (B2) exists. Since $(t,\ell)=1$, $\ell|\gamma_1(1)$, and so $\ell|\alpha(1)$. On the other hand, $\beta(1) = s\delta_1$ for some divisor s of $|G/S|$ and some irreducible constituent δ_1 of δ_S. Now ℓ is coprime to both $|G/S|$ and $\delta(1)$, so it is coprime to $\beta(1)$. Thus $\alpha(1) \neq \beta(1)$ in this case as well.

In what follows we will usually use this claim in the following set-up. Consider a simple algebraic group $\mathcal{G}$ of adjoint type and a Frobenius map F on $\mathcal{G}$ such that $S = [H,H]$ for $H = \mathcal{G}^F$. Let L denote the dual group of H. Since H is of adjoint type, any semisimple element s in L has a connected centralizer (in the dual group $\mathcal{G}^*$), and so it defines an irreducible character χ_s of H of degree $|L:\mathbf{C}_L(s)|_{r'}$. We will also frequently choose γ or δ to be some unipotent characters of H.

(2) Consider the case $H = E_8(q)$. Notice that $H = S$ and $|\mathrm{Out}(S)| \leq q/2$. According to [C, p. 487], H has unipotent characters γ, δ, labeled as $(E_6[\theta], \varphi''_{1,3})$ and $(E_6[\theta], \varphi'_{1,3})$, with

$$\delta(1) = \frac{1}{3}q^8\Phi_1^6\Phi_2^6\Phi_4^4\Phi_5^2\Phi_7\Phi_8^2\Phi_{10}^2\Phi_{14}\Phi_{15}\Phi_{20}\Phi_{30},\ \gamma(1)/\delta(1) = q^{24}.$$

By the claim in (1), we are done unless $p|\Phi_i$ for $i = 3,6,9,12,18,24$. In this latter case, choose γ and δ to be the unipotent characters labeled as $\varphi_{2835,14}$ and $\varphi_{567,6}$ in [C, p. 484], with

$$\delta(1) = q^6\Phi_3^3\Phi_6^3\Phi_7\Phi_9\Phi_{12}^2\Phi_{14}\Phi_{15}\Phi_{18}\Phi_{24}\Phi_{30},\ q^8 < \gamma(1)/\delta(1) \in \mathbb{Z}.$$

The other exceptional groups over $\mathbb{F}_q$ can be dealt with similarly. In all cases, $|\mathrm{Out}(S)| \leq 3q$. For each of them, we will indicate a few pairs of unipotent characters $(\gamma_i,\ \delta_i)$ such that, for each prime divisor $p \neq r$ of $|S|$, the assumptions (B1), (B2) in (1) are satisfied for at least one pair. In the cases when $\mathcal{G}$ gives rise to different isogenous finite groups of the same order, the notation for H will carry the subscript ad.

If $H = E_7(q)_{ad}$, then we consider unipotent characters γ_1, δ_1, labeled as $(E_6[\theta],\varepsilon)$ and $(E_6[\theta],1)$, and γ_2, δ_2, labeled as $\varphi_{189,5}$ and $\varphi_{27,2}$. If $H = E_6(q)_{ad}$, then we consider unipotent characters γ_1, δ_1, labeled as $\varphi_{64,13}$ and $\varphi_{64,4}$, and γ_2, δ_2, labeled as (D_4,ε) and $(D_4,1)$. If $H = {}^2E_6(q)_{ad}$, then consider unipotent characters γ_1, δ_1, labeled as $({}^2A_5,\varepsilon)$ and $({}^2A_5,1)$, and γ_2, δ_2, labeled as $\varphi''_{8,9}$ and $\varphi'_{8,3}$. If $H = F_4(q)$, then consider unipotent characters γ_1, δ_1, labeled as $\varphi'_{8,9}$ and $\varphi'_{8,3}$, γ_2, δ_2, labeled as (B_2,ε), and $(B_2,1)$, and γ_3, δ_3, labeled as $\varphi_{4,13}$ and $\varphi_{4,1}$. For $H = {}^2F_4(q)$, we consider unipotent characters γ_1, δ_1, labeled as $({}^2B_2[a],\varepsilon)$ and $({}^2B_2[a],1)$, γ_2, δ_2, labeled as ε'' and ε', and γ_3, labeled as ρ_2, and a cuspidal unipotent character δ_3 of degree $\frac{1}{3}q^2\Phi_1^2\Phi_2^2\Phi_4^2$.

Assume that $H = G_2(q)$ with $q \geq 3$; in particular $H = S$. Then the chosen pairs (γ,δ) have degrees $(q\Phi_1^2\Phi_6/6, q\Phi_1^2\Phi_2^2/3)$ when $p|\Phi_1$, $(q\Phi_2^2\Phi_6/2, q\Phi_1^2\Phi_2^2/3)$ when $p|\Phi_2$, and $(q\Phi_3\Phi_6/3, q\Phi_1^2\Phi_3/2)$ when $p|\Phi_3$; in all cases ℓ can be taken to be a Zsigmondy prime divisor of q^6-1. Finally, assume $p|\Phi_6$ (so $p \geq 5$). Then consider unipotent

characters γ, δ of degree $q\Phi_3\Phi_6/3$ and $q\Phi_1^2\Phi_6/6$, and take $\ell = 7$ if $q = 4$ and a Zsigmondy prime divisor of $q^3 - 1$ if $q \neq 4$.

If $H = {}^3D_4(q)$, we choose (γ, δ) to have degrees $((q^6-1)^2, q^3(q^3 \pm 1)^2/2)$ and $(q^3(q-1)(q^8+q^4+1), (q-1)(q^8+q^4+1))$. If $H = {}^2B_2(q)$, then (γ, δ) is chosen to have degrees $((q+2t+1)(q-1), t(q-1))$ with $t = \sqrt{q/2}$, and $((q-1)(q \pm 2t+1), q^2+1)$. For $H = {}^2G_2(q)$, take (γ, δ) to have degrees $((q+3t+1)(q^2-1), t(q^2-1))$ with $t = \sqrt{q/3}$, and $(q(q^2-q+1), q^2-q+1)$.

(3) Now we handle the classical groups. Among them, the linear groups and the unitary groups will require most of our attention. First we consider the case $S = PSL_n(q)$ with $q = r^f$. The case $n = 2$ is the exception (ii) mentioned in the theorem, so we will assume $n \geq 3$; in particular, $|\mathrm{Out}(S)| = 2f(n, q-1)$ and $|H/S| = (n, q-1)$.

(3a) Assume that $n = 3$. Checking the cases $q \leq 4$ directly using [Atlas], we may assume $q \geq 5$. It is well known that $\mathrm{Irr}(H)$ contains a unipotent character τ_0 of degree $q(q+1)$, and characters χ_i, $i = 1, \ldots, 5$, of degree $(q-1)(q^2-1)$, q^2+q+1, $q(q^2+q+1)$, $(q+1)(q^2+q+1)$, and q^3-1, respectively. Choose ℓ_1 to be a Zsigmondy prime divisor of $r^{3f}-1$. Now if $p|(q-1)$, then choose $(\ell, \gamma, \delta) = (\ell_1, \chi_5, \chi_1)$. If p divides q^2-1 but not $q-1$, choose $(\ell, \gamma, \delta) = (\ell_1, \chi_4, \tau_0)$. Finally, suppose p divides q^3-1 but not q^2-1 (in particular, $p \geq 5$). If $q \neq 16$, then $q > |\mathrm{Out}(S)|$, so we may choose $(\gamma, \delta) = (\chi_3, \chi_2)$. If $q = 16$, then choose $(\ell, \gamma, \delta) = (17, \chi_4, \chi_2)$.

(3b) Next we suppose $n \geq 4$. If $(n, q) \neq (6, 2)$, we can consider a Zsigmondy prime divisor ℓ_1 of $r^{nf}-1$, a semisimple element $s_1 \in L$ of order ℓ_1, and the character $\chi_1 = \chi_{s_1}$ of H of degree $\prod_{i=1}^{n-1}(q^i-1)$. On the other hand, if $(n, q) \neq (7, 2)$, $(4, 4)$, we can consider a Zsigmondy prime divisor ℓ_2 of $r^{(n-1)f}-1$, an element $s_2 \in L$ of order ℓ_2, and the character $\chi_2 = \chi_{s_2}$ of H of degree $(q^n-1)\prod_{i=2}^{n-2}(q^i-1)$. Observe that both ℓ_1, ℓ_2 are coprime to $|\mathrm{Out}(S)|$ (when they exist). Also, choose $\mu \in \mathbb{F}_{q^2}^{\bullet}$ of order $q+1$, $s_3 \in L$ conjugate to $\mathrm{diag}(I_{n-2}, \mu, \mu^q)$, and the characters $\chi_3 = \chi_{s_3}$, respectively χ_4, labeled by s_3 and the trivial, respectively the Steinberg, character of $\mathbf{C}_L(s_3) = SL_{n-2}(q) \cdot C_{q^2-1}$, of degree $(q^n-1)(q^{n-1}-1)/(q^2-1)$, respectively $q^{(n-2)(n-3)/2}(q^n-1)(q^{n-1}-1)/(q^2-1)$.

Assume that $(n, q) \neq (7, 2)$, $(6, 2)$, $(4, 4)$. If p divides $\prod_{i=1}^{n-2}(q^i-1)$, choose $(\ell, \gamma, \delta) = (\ell_1, \chi_2, \chi_1)$. If p does not divide $\prod_{i=1}^{n-2}(q^i-1)$ and $q^{(n-2)(n-3)/2} > |\mathrm{Out}(S)|$, choose $(\gamma, \delta) = (\chi_4, \chi_3)$. In the remaining cases, $n = 4$ and $q \in \{2, 3, 4, 5, 9\}$; in particular $\mathrm{Out}(S)$ is a 2-group and p divides $(q^2+q+1)(q^2+1)$ but not q^2-1. Hence if $r > 2$, we choose $(\ell, \gamma, \delta) = (r, \chi_4, \chi_3)$. If $q = 2$, we can choose $(\ell, \gamma(1), \delta(1)) = (7, 35, 20)$ if $p = 5$, and $(5, 70, 14)$ if $p = 7$.

(3c) It remains to consider the exceptions $SL_7(2)$, $SL_6(2)$, and $SL_4(4)$. In all these cases, $H = S$ and $\mathrm{Out}(S)$ is a 2-group (of order at most 4). For them, we will also look at the unipotent characters τ_5 and τ_6, labeled by the partitions $(n-2, 1^2)$ and $(n-2, 2)$, respectively. These have degrees $(q^n-q)(q^n-q^2)/(q-1)(q^2-1)$ and $(q^n-1)(q^{n-1}-q^2)/(q-1)(q^2-1)$, respectively. First assume $S = SL_7(2)$; in particular, ℓ_1, χ_1, χ_3, and χ_4 exist. If $p = 3, 7, 127$ choose (γ, δ) to be (χ_4, χ_3). If $p = 31$, take them to be (χ_1, τ_5), and if $p = 5$, take (γ, δ) to be (χ_1, τ_6).

Next assume $S = SL_6(2)$; in particular, ℓ_2, χ_2, χ_3, and χ_4 exist. Then choose (γ, δ) to be (χ_4, χ_3) if $p = 3, 7, 31$, and (χ_2, τ_5) if $p = 5$.

Finally, suppose $S = SL_4(4)$; in particular, ℓ_1, χ_1, and χ_3 exist. Then choose (γ, δ) to be (χ_1, τ_5) if $p = 3, 7$ and (χ_3, τ_6) if $p = 17$. If $p = 5$, choose $\gamma = \chi_1$ and δ to be a semisimple character of degree $(q^n-1)/(q-1)$.

(4) Here we treat the case $S = PSU_n(q)$ with $q = r^f$ and $n \geq 3$; in particular $|\mathrm{Out}(S)| = 2f(n, q+1)$ and $|H/S| = (n, q+1)$. Notice that the cases $(n, q) = (6, 2)$, $(5, 2)$, $(4, 2)$, $(4, 3)$, and $(n = 3, 3 \leq q \leq 8)$ can be verified directly using [Atlas].

(4a) Assume that $n = 3$ and $q \geq 9$. It is well known that $\mathrm{Irr}(H)$ contains a unipotent character τ_0 of degree $q(q-1)$ and characters χ_i for $i = 1, 2, 3$, of degree $(q+1)(q^2-1)$, $q^2 - q + 1$, and $q^3 + 1$, respectively. Choose ℓ_1 to be a Zsigmondy prime divisor of $r^{6f} - 1$. Now if $p|(q+1)$, then choose $(\ell, \gamma, \delta) = (\ell_1, \chi_3, \chi_1)$. If p divides $q-1$, choose $(\gamma, \delta) = (\chi_1, \tau_0)$. If p divides q^3+1 but not q^2-1, then choose $(\gamma, \delta) = (\chi_3, \chi_2)$. Note that $\gamma(1)/\delta(1) \geq q + 1 > |\mathrm{Out}(S)|$ in the last two cases.

(4b) Here we assume $n \geq 5$ is odd and $(n, q) \neq (5, 2)$. Then we consider a Zsigmondy prime divisor ℓ_1 of $r^{2nf} - 1$, a semisimple element $s_1 \in L$ of order ℓ_1, and the semisimple character $\chi_1 = \chi_{s_1}$ of H of degree $\prod_{i=1}^{n-1}(q^i - (-1)^i)$. Next, consider a Zsigmondy prime divisor ℓ_2 of $r^{2(n-2)f} - 1$, an element $s_2 \in L$ of order ℓ_2, and the character $\chi_2 = \chi_{s_2}$ of H of degree $(q^n+1)(q^{n-1}-1)\prod_{i=3}^{n-3}(q^i - (-1)^i)$. These characters exist by Lemma 6.2. Observe that both ℓ_1, ℓ_2 are coprime to $|\mathrm{Out}(S)|$. We will also look at the unipotent characters τ_3 and τ_4, labeled by the partitions $(n-2, 1^2)$ and $(n-2, 2)$, respectively. These have degrees

$$(q^n + (-1)^n q)(q^n - (-1)^n q^2)/(q+1)(q^2-1) \text{ and}$$
$$(q^n - (-1)^n)(q^{n-1} + (-1)^n q^2)/(q+1)(q^2-1),$$

respectively. Let k be the smallest positive integer such that $p|(q^k - (-1)^k)$. Now if $k \leq n-3$ or $k = n-1$, then choose $(\ell, \gamma, \delta) = (\ell_1, \chi_2, \chi_1)$. If $k = n-2$, choose $(\gamma, \delta) = (\chi_1, \tau_3)$. If $k = n$, choose $(\gamma, \delta) = (\chi_2, \tau_4)$. Again, $\gamma(1)/\delta(1) > q(q+1) \geq |\mathrm{Out}(S)|$ in the last two cases.

(4c) Here we assume $n \geq 6$ is even and $(n, q) \neq (6, 2)$. Then we consider a Zsigmondy prime divisor ℓ_1 of $r^{2(n-1)f} - 1$, an element $s_1 \in L$ of order ℓ_1, and the character $\chi_1 = \chi_{s_1}$ of H of degree $(q^n - 1)\prod_{i=2}^{n-2}(q^i - (-1)^i)$. Next, consider a Zsigmondy prime divisor ℓ_2 of $r^{2(n-3)f} - 1$, an element $s_2 \in L$ of order ℓ_2, and the character $\chi_2 = \chi_{s_2}$ of H of degree $\prod_{i=4}^{n}(q^i - (-1)^i)/(q^{n-3}+1)$. (See Lemma 6.2.) Observe that both ℓ_1, ℓ_2 are coprime to $|\mathrm{Out}(S)|$. Let τ_3, τ_4, and k be defined as in (4b). Now if $k \neq n-3, n-1$, then choose $(\ell, \gamma, \delta) = (\ell_1, \chi_2, \chi_1)$. If $k = n-3$, choose $(\gamma, \delta) = (\chi_1, \tau_4)$. If $k = n-1$, choose $(\gamma, \delta) = (\chi_2, \tau_3)$. Here, too, $\gamma(1)/\delta(1) > q(q+1) \geq |\mathrm{Out}(S)|$ in the last two cases.

(4d) Finally, we consider the case $n = 4$ and $q \geq 4$. We can consider ℓ_1, χ_1 of degree $(q^2-1)(q^4-1)$ and the integer k as in (4c). Next, τ_0 denotes the unipotent character of degree $q(q^2 - q + 1)$. Consider the semisimple element $s_2 = \mathrm{diag}(I_2, \mu, \mu^{-1}) \in L$ with $\mu \in \mathbb{F}_{q^2}^{\bullet}$ of order $q+1$ and the character $\chi_2 = \chi_{s_2}$ of degree $(q^2 - q + 1)(q^2+1)(q-1)$. Finally, choose $\theta \in \mathbb{F}_q^{\bullet}$ of order $q-1$, $s_3 \in L$ conjugate to $\mathrm{diag}(I_2, \theta, \theta^{-q})$ and the character $\chi_3 = \chi_{s_3}$ of degree $(q^3+1)(q^2+1)$. Now, choose $(\ell, \gamma, \delta) = (\ell_1, \chi_3, \chi_1)$ if $k = 1$ or $k = 4$ and $(\ell, \gamma, \delta) = (\ell_1, \chi_2, \chi_1)$ if $k = 2$. If $k = 3$, choose $(\gamma, \delta) = (\chi_3, \tau_0)$, and again $\gamma(1)/\delta(1) > q(q+1) \geq |\mathrm{Out}(S)|$.

(5) Suppose $S = PSp_{2n}(q)$ or $\Omega_{2n+1}(q)$ with $q = r^f$ and $n \geq 2$. Then $|H/S| \leq 2$. Using [Atlas] we may assume $(n, q) \neq (2, 2)$, $(2, 3)$, $(3, 2)$, and $(4, 2)$. Hence we may consider a Zsigmondy prime divisor ℓ_1 of $r^{2nf} - 1$, a semisimple element $s_1 \in L$ of order ℓ_1, and the character $\chi_1 = \chi_{s_1}$ of H of degree $(q^n - 1)\prod_{i=1}^{n-1}(q^{2i} - 1)$. If

there exists a Zsigmondy prime divisor ℓ_2 of $r^{(2n-2)f}-1$, then by Lemma 6.2 we can find an element $s_2 \in L$ of order ℓ_2 and consider the character $\chi_2 = \chi_{s_2}$ of H of degree $\prod_{i=2}^{n}(q^{2i}-1)/(q^{n-1}+1)$. We will also consider unipotent characters τ_3, τ_4, and τ_5 of H, of degrees $(q^n-1)(q^n-q)/2(q+1)$, $(q^n+1)(q^n+q)/2(q+1)$, and $(q^n+1)(q^n-q)/2(q-1)$, respectively. Let k be the smallest positive integer such that $p|(q^{2k}-1)$. First assume $n \geq 3$. Then ℓ_2 and χ_2 exist as $(n,q) \neq (4,2)$. If $1 \leq k \leq n-2$, choose $(\ell,\gamma,\delta) = (\ell_1,\chi_2,\chi_1)$. If $k = n-1$, choose $\gamma = \chi_1$ and $\delta \in \{\tau_3,\tau_4\}$. If $k = n$, choose $\gamma = \chi_2$ and $\delta \in \{\tau_3,\tau_4\}$. In the last two cases, $\gamma(1)/\delta(1) > q \geq |\mathrm{Out}(S)|$.

Now we assume $n = 2$ and $q \geq 4$; in particular $|\mathrm{Out}(S)| = 2f$. Then choose $(\gamma,\delta) = (\chi_1,\tau_3)$ if $p|(q-1)$ and (χ_1,τ_4) if $p|(q+1)$; in both cases $\gamma(1)/\delta(1) > |\mathrm{Out}(S)|$. In the remaining case $p|(q^2+1)$, and $\mathrm{Irr}(H)$ contains a character χ_2 of degree $(q-1)(q^2+1)$ and a character χ_6 of degree $(q+1)(q^2+1)$. Assuming the existence of ℓ_2, we may choose $(\ell,\gamma,\delta) = (\ell_2,\chi_6,\tau_4)$. Assume that ℓ_2 does not exist. Then either $f = 1$, in which case choose $(\gamma,\delta) = (\chi_6,\tau_4)$, or $q = 8$, in which case take $(\ell,\gamma,\delta) = (7,\chi_2,\tau_4)$.

(6) Suppose $S = P\Omega_{2n}^{-}(q)$ with $q = r^f$ and $n \geq 4$. Then $|H/S| = (4,q^n+1)$ and $|\mathrm{Out}(S)| = 2f \cdot (4,q^n+1)$. Using [Atlas] we may assume $(n,q) \neq (4,2)$. Hence by Lemma 6.2 we may consider a Zsigmondy prime divisor ℓ_1 of $r^{2nf}-1$, a semisimple element $s_1 \in L$ of order ℓ_1, and the character $\chi_1 = \chi_{s_1}$ of H of degree $\prod_{i=1}^{n-1}(q^{2i}-1)$. We may also consider a Zsigmondy prime divisor ℓ_2 of $r^{(2n-2)f}-1$, an element $s_2 \in L$ of order ℓ_2, and the character $\chi_2 = \chi_{s_2}$ of H of degree $(q+1)(q^{n-1}-1)(q^n+1)\prod_{i=2}^{n-2}(q^{2i}-1)$. We will also consider unipotent characters τ_3 and τ_4 of degrees $(q^n+1)(q^{n-1}-q)/(q^2-1)$ and $(q^{2n}-q^2)/(q^2-1)$. Let k be as defined in (5). If $1 \leq k \leq n-2$, choose $(\ell,\gamma,\delta) = (\ell_1,\chi_2,\chi_1)$. If $k = n-1$, then choose $(\gamma,\delta) = (\chi_1,\tau_4)$, and if $k = n$, then choose $(\gamma,\delta) = (\chi_2,\tau_3)$. In the last two cases, $\gamma(1)/\delta(1) > q^3 \geq |\mathrm{Out}(S)|$.

(7) Suppose $S = P\Omega_{2n}^{+}(q)$ with $q = r^f$ and $n \geq 4$. Then $|H/S| = (4,q^n-1)$, and using [Atlas] we may assume $(n,q) \neq (4,2)$. By Lemma 6.2 we may consider a Zsigmondy prime divisor ℓ_1 of $r^{(2n-2)f}-1$, a semisimple element $s_1 \in L$ of order ℓ_1, and the character $\chi_1 = \chi_{s_1}$ of H of degree $(q-1)(q^{n-1}-1)(q^n-1)\prod_{i=2}^{n-2}(q^{2i}-1)$. We will consider unipotent characters τ_3 and τ_4 of degrees $(q^n-1)(q^{n-1}+q)/(q^2-1)$ and $(q^{2n}-q^2)/(q^2-1)$. Let k be as defined in (5).

First we handle the case where $n \geq 5$ is odd. By Lemma 6.2 we may consider a Zsigmondy prime divisor ℓ_2 of $r^{nf}-1$, an element $s_2 \in L$ of order ℓ_2, and the character $\chi_2 = \chi_{s_2}$ of H of degree $\prod_{i=1}^{n-1}(q^{2i}-1)$. Now if $1 \leq k \leq n-2$, choose $(\ell,\gamma,\delta) = (\ell_1,\chi_2,\chi_1)$. If $k = n-1$, then choose $(\gamma,\delta) = (\chi_2,\tau_4)$, and if $k = n$, then choose $(\gamma,\delta) = (\chi_1,\tau_3)$. In the last two cases, $\gamma(1)/\delta(1) > q^4 \geq |\mathrm{Out}(S)|$.

Finally, we consider the case where $n \geq 4$ is even; in particular $k \leq n-1$. Assume that $(n,q) \neq (4,4)$. Then by Lemma 6.2 we may consider a Zsigmondy prime divisor ℓ_2 of $r^{(n-1)f}-1$, an element $s_2 \in L$ of order ℓ_2, and the character $\chi_2 = \chi_{s_2}$ of H of degree $(q+1)(q^{n-1}+1)(q^n-1)\prod_{i=2}^{n-2}(q^{2i}-1)$. Now if $1 \leq k \leq n-2$, choose $(\ell,\gamma,\delta) = (\ell_1,\chi_2,\chi_1)$. If $k = n-1$, then choose $\gamma \in \{\chi_1,\chi_2\}$ and $\delta = \tau_4$, where in both cases $\gamma(1)/\delta(1) > (q-1)(q^4-1) > |\mathrm{Out}(S)|$. Now assume that $S = \Omega_8^{+}(4)$. Then H has a unipotent character τ_5 of degree $q^3(q+1)^3(q^3+1)/2$, and $|\mathrm{Out}(H)| = 12$. Then choose $(\ell,\gamma,\delta) = (17,\chi_1,\tau_4)$ if $p = 3,7$, $(17,\chi_1,\tau_5)$ if $p = 5$, $(7,\tau_4,\tau_5)$ if $p = 13$, and $(7,\chi_1,\tau_3)$ if $p = 17$. This completes the proof of Theorem 7.3. $\square$

Corollary 7.4. *Suppose the socle of G is a finite nonabelian simple group S and let p be any prime divisor of $|S|$. Then one of the following holds.*

(i) *G has two faithful irreducible characters of distinct degrees divisible by p.*
(ii) *Either $S \cong PSL_2(q)$ with $p|q$, or $S \cong PSL_2(q)$ and $p > 2$ is coprime to q, or $(G, p) \in \{(M_{11}, 3), (J_1, 3), (J_1, 5)\}$.*

Proof. Assume that (i) does not hold. First we consider the case $p = 2$. Observe that if $\alpha, \beta \in \mathrm{Irr}(S)$ satisfy the conclusion (i) of Theorem 6.7, then G satisfies (i). Choosing $\gamma \in \mathrm{Irr}(G|\alpha)$ and $\delta \in \mathrm{Irr}(G|\beta)$ we see that $\gamma(1) \neq \delta(1)$. Hence by Theorem 6.7, $S \cong PSL_2(q)$ with $2|q$. If $p > 2$, then we can apply Theorem 7.3 and arrive at the possibilities for (S, p) mentioned in (ii). □

We will say more about the almost simple one-p-degree groups G.

Corollary 7.5. *Suppose that the socle of G is a finite nonabelian simple group S and that G has exactly one irreducible character degree n divisible by the prime p. Then p divides $|S|$ but does not divide $|G/S|$. Also, $n_p = |S|_p$, and one of the following holds.*

(i) *$S \cong PSL_2(q)$ with $p|q$, and $n = q$.*
(ii) *$S \cong PSL_2(q)$, $q = r^f$ for some prime $r \neq p$, $2 < p|(q - \epsilon)$ for some $\epsilon = \pm 1$, and $n|(q - \epsilon)f$.*
(iii) *$(G, p, n) \in \{(M_{11}, 3, 45), (J_1, 3, 120), (J_1, 5, 120)\}$.*

Proof. It is clear that p divides $|G|$. By Theorem 7.1, p divides $|S|$. Now we apply Corollary 7.4 to G. Notice that the statements are obvious if $S = M_{11}$ or J_1, so we will assume that $S = PSL_2(q)$ with $q = r^f$. In particular, $\mathrm{Out}(S)$ is abelian of order $(2, q - 1)f$.

First we consider the case $p = r$. Then the Steinberg character of degree q of S extends to G, whence $n = q$. We claim that G/S is a p'-group. Assume the contrary. Then G induces an outer automorphism σ of order p (modulo $\mathrm{Inn}(S)$). Recall (see [GLS]) that the subgroup of inner-diagonal automorphisms of S is induced by $H = PGL_2(q)$. By Corollary 7.4, $p = 2$ implies $2|q$, and so $H = S$. It follows that $\sigma \notin H$. Hence, σ does not fix some character $\alpha \in \mathrm{Irr}(S)$ of degree $q - 1$ (and some character $\beta \in \mathrm{Irr}(S)$ of degree $q + 1$). Thus $\mathrm{cd}_p(G) \ni n'$ with $p(q \pm 1)|n'$, and so $n' \neq n$, which is a contradiction.

Now we may assume $p \neq r$, and so $p \neq 2$ and $p|(q - \epsilon)$, where $\epsilon = \pm 1$. Assume that p divides $|G/S|$. Then arguing as above, we see that $\mathrm{Irr}(G)$ contains characters of degrees n_1 and n_2, where $p(q - 1)|n_1$ and $n_1|2f(q - 1)$, and where $p(q + 1)|n_2$ and $n_2|2f(q + 1)$. It follows that $n = n_1 = n_2$ is divisible by $p(q^2 - 1)/(2, q - 1)$. But in this case $n_1 > 2f(q - 1)$, which is a contradiction. Thus in all cases G/S is a p'-group, and so $n_p = |S|_p$. Finally, observe that $\mathrm{Irr}(S)$ contains a character γ of degree $q - \epsilon$ which extends to $H = PGL_2(q)$. Since $\mathrm{Aut}(S)/H$ is cyclic of order f, we see that $\mathrm{Aut}(S)$ has an irreducible character δ of degree dividing $(q - \epsilon)f$ such that $[\delta_S, \gamma] \neq 0$. Since $\mathrm{Out}(S)$ is abelian, $G \lhd \mathrm{Aut}(S)$. Choosing $\chi \in \mathrm{Irr}(G)$ to be a constituent of δ_G, we conclude that $n = \chi(1)$ divides $(q - \epsilon)f$. □

Remark 7.6. As shown by the examples of $(G, p) = (PGL_2(11), 5)$, $(SL_2(8) \cdot 3, 7)$, it may happen that an almost simple group G is a one-p-degree group but its socle S is not, or vice versa, even under the condition that $(p, |G/S|) = 1$.

Now we are ready to prove Theorems 2.1 and 5.1, which we reformulate below.

Theorem 7.7. *Let S be the socle of G, and assume that S is a finite nonabelian simple group. The following then hold.*

(a) *G has faithful irreducible characters α and β with distinct degrees.*
(b) *If p is a prime divisor of $|G : S|$, then α and β can be chosen to have degrees divisible by p.*

Proof. Suppose (a) does not hold. By choosing $p = 2$ and applying Corollary 7.4, we see that $S = PSL_2(q)$ for some $q = 2^f > 2$. But then $\mathrm{Irr}(G)$ contains a character of degree q and a character of degree divisible by $q + 1$, a contradiction.

For (b), suppose that p is a prime divisor of $|G : S|$. If p does not divide $|S|$, then (b) follows from Theorem 7.1. If p divides $|S|$, then (b) follows from Corollary 7.5. □

Theorem 7.8. *Let S be the socle of G, and assume that S is a finite nonabelian simple group of order divisible by the prime p. Assume that n is the only multiple of p that occurs as the degree of a faithful irreducible character of G. Then the Sylow p-subgroups of G are abelian TI-sets of order n_p.*

Proof. Apply Corollary 7.5 to G. Since $(p, |G/S|) = 1$, every Sylow p-subgroup of G is contained in S, and we are done. □

References

[C] R. Carter, *Finite Groups of Lie Type: Conjugacy Classes and Complex Characters*, Wiley, Chichester, 1985. MR794307 (87d:20060)

[Atlas] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson, *An ATLAS of Finite Groups*, Clarendon Press, Oxford, 1985. MR827219 (88g:20025)

[DM] F. Digne and J. Michel, *Representations of Finite Groups of Lie Type*, London Mathematical Society Student Texts 21, Cambridge University Press, Cambridge 1991. MR1118841 (92g:20063)

[DNT] S. Dolfi, G. Navarro, and P. H. Tiep, Primes dividing the degrees of the real characters of finite groups, *Math. Z.* **259** (2008), no. 4, 755–774. MR2403740

[F] W. Feit, Extending Steinberg characters, in: *Linear algebraic groups and their representations* (Los Angeles, CA, 1992), *Contemp. Math.* **153** (1993), pp. 1–9. MR1247494 (94k:20012)

[GLS] D. Gorenstein, R. Lyons, and R. Solomon, *The Classification of the Finite Simple Groups*, Number 3, Mathematical Surveys and Monographs, Amer. Math. Soc., Providence, 1994. MR1303592 (95m:20014)

[GT] R. M. Guralnick and P. H. Tiep, Cross characteristic representations of even characteristic symplectic groups, *Trans. Amer. Math. Soc.* **356** (2004), 4969–5023. MR2084408 (2005j:20012)

[H1] B. Huppert, *Endliche Gruppen I*, Springer-Verlag, Berlin 1967. MR0224703 (37:302)

[H2] B. Huppert, *Character Theory of Finite Groups*, de Gruyter, Berlin/New York, 1998. MR1645304 (99j:20011)

[HB] B. Huppert and N. Blackburn, *Finite Groups II*, Springer-Verlag, New York, 1982. MR650245 (84i:20001a)

[IP] I. M. Isaacs and D. S. Passman, Half-transitive automorphism groups, *Can. J. Math.* **18** (1966), 1243–1250. MR0200343 (34:239)

[I1] I. M. Isaacs, The p-parts of character degrees in p-solvable groups. *Pacific J. Math.* **36** (1971), 677–691. MR0313372 (47:1927)

[I2] I. M. Isaacs, *Character Theory of Finite Groups*, Dover, New York, 1994. MR1280461

[KL] P. B. Kleidman and M. W. Liebeck, *The Subgroup Structure of the Finite Classical Groups*, London Math. Soc. Lecture Note Ser. No. 129, Cambridge University Press, Cambridge 1990. MR1057341 (91g:20001)

[M1] A. Moretó, Heights of characters and defect groups, in: *Finite Groups 2003*, Eds. C. Y. Ho, P. Sin, P. H. Tiep and A. Turull, de Gruyter, Berlin 2004, pp. 267–273. MR2125078 (2005j:20011)

[M2] A. Moretó, Derived length and character degrees of solvable groups. *Proc. Amer. Math. Soc.* **132** (2004), 1599–1604. MR2051119 (2005d:20017)

[MT] A. Moretó and P. H. Tiep, Prime divisors of character degrees, *J. Group Theory* **11** (2008), no. 3, 341–356. MR2419005

[ST] P. Sin and P. H. Tiep, Rank 3 permutation modules for finite classical groups, *J. Algebra* **291** (2005), 551–606. MR2163483 (2006j:20019)

[Zs] K. Zsigmondy, Zur Theorie der Potenzreste, *Monath. Math. Phys.* **3** (1892), 265–284. MR1546236

Department of Mathematics, University of Wisconsin, 480 Lincoln Drive, Madison, Wisconsin 53706

E-mail address: isaacs@math.wisc.edu

Departament d'Àlgebra, Universitat de València, 46100 Burjassot, València, Spain

E-mail address: alexander.moreto@uv.es

Departament d'Àlgebra, Universitat de València, 46100 Burjassot, València, Spain

E-mail address: gabriel@uv.es

Department of Mathematics, University of Arizona, 617 N. Santa Rita Avenue, P.O. Box 210089, Tucson, Arizona 85721

E-mail address: tiep@math.arizona.edu