J. Group Theory **20** (2017), 1175–1190
DOI 10.1515/jgth-2017-0023

Brauer characters and fields of values

Dan Rossi

Communicated by Robert M. Guralnick

Abstract. For a prime number p and a finite group G, we consider the set of p-Brauer characters of G taking values in some field $\mathbb{F}$ (called $\mathbb{F}$-Brauer characters) and the set of conjugacy classes of p-regular elements of G whose value at every Brauer character lies in $\mathbb{F}$ (called $\mathbb{F}$-conjugacy classes). We show that these sets for G and for G/N are closely related, for certain normal subgroups N of G. This is a p-modular version of a result of Isaacs and Navarro in characteristic 0 (see [3]).

1 Introduction

Let G be a finite group and let $\mathbb{F} \subseteq \mathbb{C}$ be any subfield of the field of complex numbers. If χ is a complex character of G such that $\chi(x) \in \mathbb{F}$ for every element $x \in G$, then we say χ is an $\mathbb{F}$-*character* and we write $\mathrm{Irr}_{\mathbb{F}}(G)$ for the set of all irreducible $\mathbb{F}$-characters. Analogously, if $\chi(x) \in \mathbb{F}$ for every complex character χ, then we say x is an $\mathbb{F}$-*element*. Since characters are constant on conjugacy classes, we may unambiguously say that the conjugacy class x^G is an $\mathbb{F}$-*class*; we write $\mathrm{Cl}_{\mathbb{F}}(G)$ for the set of $\mathbb{F}$-classes of G. If $H \subseteq G$ is any subset and H contains no non-trivial $\mathbb{F}$-elements of G, then we say H is $\mathbb{F}$-*free* in G. We emphasize that the notion of H being $\mathbb{F}$-free is always relative to some overgroup G.

In [3] Isaacs and Navarro prove that the sets $\mathrm{Irr}_{\mathbb{F}}(G)$ and $\mathrm{Irr}_{\mathbb{F}}(G/N)$, respectively $\mathrm{Cl}_{\mathbb{F}}(G)$ and $\mathrm{Cl}_{\mathbb{F}}(G/N)$, are closely related whenever $N \lhd G$ is an $\mathbb{F}$-free normal subgroup. More precisely, they show the following.

Theorem 1.1 ([3, Theorem A]). *Let $\mathbb{F}$ be a subfield of the complex numbers and suppose that N is an $\mathbb{F}$-free normal subgroup of the finite group G. Then the canonical homomorphism $G \to G/N$ defines a bijection from $\mathrm{Cl}_{\mathbb{F}}(G)$ to $\mathrm{Cl}_{\mathbb{F}}(G/N)$.*

Theorem 1.2 ([3, Theorem B]). *Let $\mathbb{F}$ be a subfield of the complex numbers and let G be a finite group. Then G contains a unique largest $\mathbb{F}$-free normal subgroup N, and N is contained in the kernel of every irreducible $\mathbb{F}$-character of G.*

Partially supported by NSF Grant DMS-1201374.

In this paper we prove analogues of these Isaacs–Navarro theorems in the modular setting. Fix a prime number p. We write G° for the set of p-regular elements of G, i.e. the elements with order coprime to p. If $S \subseteq G$ is any subset, we define $S^\circ := S \cap G^\circ$. We choose a maximal ideal of the ring of algebraic integers that contains p. We denote by $\mathrm{IBr}_p(G)$ the set of irreducible p-Brauer characters of G, calculated with respect to this ideal. When the prime p is understood, we will write Brauer character in place of p-Brauer character and $\mathrm{IBr}(G)$ in place of $\mathrm{IBr}_p(G)$.

As in the ordinary character setting, if ϕ is any Brauer character of G, we say ϕ is an $\mathbb{F}$*-Brauer character* if $\phi(x) \in \mathbb{F}$ for every $x \in G^\circ$. The set of irreducible $\mathbb{F}$-Brauer characters of G is denoted $\mathrm{IBr}_{\mathbb{F}}(G)$, or $\mathrm{IBr}_{p,\mathbb{F}}(G)$ when it is necessary to emphasize the prime. Similarly, if $x \in G^\circ$ and $\phi(x) \in \mathbb{F}$ for every Brauer character of G, then we say x is an $\mathbb{F}$*-element*, x^G is an $\mathbb{F}$*-class*, and write $\mathrm{Cl}^\circ_{\mathbb{F}}(G)$ for the set of $\mathbb{F}$-classes of p-regular elements in G. At the moment it appears we have defined "$\mathbb{F}$-element" in two different ways, once in terms of ordinary characters and once in terms of Brauer characters. There is actually no cause for confusion, as the two notions agree whenever $x \in G^\circ$. If χ is an ordinary character of G, then we write χ° for the restriction of χ to G°. Every Brauer character is a $\mathbb{Z}$-linear combination of $\{\chi^\circ : \chi \in \mathrm{Irr}(G)\}$; and conversely every χ°, for $\chi \in \mathrm{Irr}(G)$, is a $\mathbb{Z}$-linear combination of $\mathrm{IBr}(G)$ (see e.g. [5, Chapter 2]). Thus, for any $x \in G^\circ$, it follows that $\chi(x) \in \mathbb{F}$ for every ordinary character χ if and only if $\phi(x) \in \mathbb{F}$ for every Brauer character ϕ.

Now we can state our main results.

Theorem A. *Let p be a prime number and $\mathbb{F}$ any subfield of the field of complex numbers. Let $N \lhd G$ and assume that N° is $\mathbb{F}$-free in G. Then the canonical homomorphism $G \to G/N$ induces a bijection from $\mathrm{Cl}^\circ_{\mathbb{F}}(G)$ to $\mathrm{Cl}^\circ_{\mathbb{F}}(G/N)$.*

Theorem B. *Let p be a prime number and $\mathbb{F}$ any subfield of the field of complex numbers. Then G has a unique largest normal subgroup N with the property that N° is $\mathbb{F}$-free in G; N is contained in the kernel of every $\phi \in \mathrm{IBr}_{\mathbb{F}}(G)$.*

A word of caution is necessary here: The set $\mathrm{IBr}(G)$ is not canonically defined, depending on the choice of a maximal ideal made above. However, we recall that any two choices of $\mathrm{IBr}(G)$ are Galois conjugate (see [5, Theorem 2.34]). In particular, fields of values for the entire set of all Brauer characters are canonically defined. Thus Theorems A and B hold true for any choice of $\mathrm{IBr}(G)$.

The paper is organized as follows. Section 2 collects some preliminary results. In Section 3 we prove the surjectivity assertion in Theorem A and the first part of Theorem B. We complete the proof of Theorem B in Section 4. Section 5 establishes the injectivity assertion in Theorem A, thereby completing the proof; it constitutes the bulk of the work in the paper.

2 Preliminaries

Assumption 2.1. For the remainder of this paper we fix a field $\mathbb{F} \subseteq \mathbb{C}$ and a prime number p.

We begin with a useful lemma that will help control the structure of subgroups $N \lhd G$ when N° is $\mathbb{F}$-free in G.

Lemma 2.2. *Let S be a non-abelian simple group. Then S has a rational element of order* 3 *or* 5 *unless $S = \mathrm{PSL}_2(3^{2n+1})$, $n \geq 1$, which has no non-trivial rational elements of odd order.*

Proof. See [6, Theorems 11.1 and 11.2]. □

In the proofs of Theorems A and B later on, the first step will be to reduce to the situation where N is minimal normal in G and N° is $\mathbb{F}$-free in G. In this case $N \simeq S_1 \times \cdots \times S_r$ with each $S_i \simeq S$, a simple group. It turns out that if N is solvable, then Theorems A and B can be proved in basically the same way as the analogous Isaacs–Navarro results above. Now if N° is $\mathbb{F}$-free in G, then certainly it is $\mathbb{Q}$-free in G and, since involutions are automatically rational, if $p > 2$, then it follows that $|N|$ is odd and thus N is solvable. When $p = 2$, it is no longer the case that N must be solvable – this is the main obstacle we must overcome in order to prove Theorems A and B. In this situation, Lemma 2.2 forces that $S = \mathrm{PSL}_2(3^{2n+1})$ and we shall exploit this observation in Sections 4 and 5.

Before proceeding further we must recall some notions from [3]. For any integer n, $\mathbb{Q}_n$ denotes the cyclotomic field obtained by adjoining to $\mathbb{Q}$ a primitive nth root of unity. If ζ is any nth root of unity and $\sigma \in \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})$, then $\zeta^\sigma = \zeta^k$ for some integer k coprime to n. If G is a group with exponent dividing n, then $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})$ acts on G by $x^\sigma = x^k$, with k as in the previous sentence. This also induces actions on $\mathrm{Cl}(G)$ and $\mathrm{Cl}^\circ(G)$ by $(x^G)^\sigma = (x^k)^G$. If G is abelian, then the action of $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})$ on G is by automorphisms. In particular, if C is cyclic of order n, then this action defines a natural map $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}) \to \mathrm{Aut}(C)$, which is in fact an isomorphism. Now write $\mathbb{K} = \mathbb{F} \cap \mathbb{Q}_n$, so $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{K}) \leq \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})$. Furthermore, we write $\mathrm{Aut}_{\mathbb{F}}(C)$ for the image of this subgroup under the isomorphism $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}) \to \mathrm{Aut}(C)$ just described. If $C \leq G$, then we say C is $\mathbb{F}$*-cyclic* in G if the subgroup of $\mathrm{Aut}(C)$ induced by $N_G(C)$ contains $\mathrm{Aut}_{\mathbb{F}}(C)$. In particular, we see that C is $\mathbb{F}$-cyclic in G if and only if it is $\mathbb{K}$-cyclic.

An easy consequence of the definitions is the following.

Lemma 2.3. *Let $x \in G$ and write $X = \langle x \rangle$. If x is an $\mathbb{F}$-element in G, then X is $\mathbb{F}$-cyclic in G. Conversely, if X is $\mathbb{F}$-cyclic in G, then every element of X is an $\mathbb{F}$-element in G.*

Proof. This is [3, Lemma 2.1]. □

The next statement is an almost trivial, but useful, observation.

Lemma 2.4. *Let $X = \langle x \rangle$ and $Y = \langle y \rangle$ be cyclic groups of order m and n, respectively, and assume that m divides n. If $y \mapsto y^t$ is an automorphism in $\mathrm{Aut}_{\mathbb{F}}(Y)$, then $x \mapsto x^t$ is an automorphism in $\mathrm{Aut}_{\mathbb{F}}(X)$. Moreover, every element of the group $\mathrm{Aut}_{\mathbb{F}}(X)$ arises in this way.*

Proof. Let $\mathbb{K} = \mathbb{F} \cap \mathbb{Q}_n$ and $\mathbb{E} = \mathbb{F} \cap \mathbb{Q}_m = \mathbb{K} \cap \mathbb{Q}_m$. By basic Galois theory, restriction to $\mathbb{E}$ defines a surjection from $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{K})$ onto $\mathrm{Gal}(\mathbb{Q}_m/\mathbb{E})$. Now the lemma follows from the definitions of $\mathrm{Aut}_{\mathbb{F}}(X)$ and $\mathrm{Aut}_{\mathbb{F}}(Y)$. □

We conclude this section with one more lemma.

Lemma 2.5. *Let M and N be normal subgroups of the finite group G and assume that $N \cap M = 1$. Let $\overline{G} = G/M$. Then $n \in N$ is an $\mathbb{F}$-element in G if and only if $\bar{n}$ is an $\mathbb{F}$-element in $\overline{G}$.*

Proof. Clearly, if n is an $\mathbb{F}$-element in G, then $\bar{n}$ is one in $\overline{G}$.

So assume that $\bar{n}$ is an $\mathbb{F}$-element in $\overline{G}$. Let $\psi_t : n \mapsto n^t$ be any automorphism in $\mathrm{Aut}_{\mathbb{F}}(\langle n \rangle)$. Because $N \cap M = 1$, we have $o(n) = o(\bar{n})$ and so, by Lemma 2.4, the map $\phi_t : \bar{n} \mapsto \bar{n}^t$ is in $\mathrm{Aut}_{\mathbb{F}}(\langle \bar{n} \rangle)$. Thus there is some $g \in G$ with $\bar{n}^{\bar{g}} = \bar{n}^t$. Then $n^g = n^t m$ for some $m \in M$. But then $m = n^g n^{-t} \in M \cap N = 1$ and so $n^g = n^t$. Thus g induces on $\langle n \rangle$ the automorphism ψ_t and we conclude that n is an $\mathbb{F}$-element of G. □

3 Lifts

We are now ready to begin proving the main results. We start by proving the surjectivity assertion in Theorem A. Interestingly, for this we do not need to separately consider the case $p = 2$ and N non-solvable. All of the proofs in this section follow [3] nearly exactly; we need only check that certain elements are actually p-regular. We include the arguments in full in order to give a sense of just how similar they are. Later on, we will include less detail whenever we mimic the proofs contained in [3].

Theorem 3.1. *Let $N \lhd G$ and assume that N° is $\mathbb{F}$-free in G. Then the canonical homomorphism $G \to G/N$ induces a surjection $\mathrm{Cl}^\circ_{\mathbb{F}}(G) \to \mathrm{Cl}^\circ_{\mathbb{F}}(G/N)$.*

Proof. Identifying the Brauer characters of G/N with a subset of the Brauer characters of G, it is clear that images of $\mathbb{F}$-elements of G are $\mathbb{F}$-elements of G/N.

And clearly images of p-regular elements are p-regular. Thus, to prove the theorem we must show that if $Nx \in G/N$ is a p-regular $\mathbb{F}$-element, then the coset Nx contains a p-regular $\mathbb{F}$-element of G. Assume this is false and let G have minimal order among counterexamples. Also assume that N has minimal order among normal subgroups K such that K° is $\mathbb{F}$-free in G and K gives rise to a counterexample.

Suppose that $1 < M < N$ with $M \triangleleft G$ and note that M° is $\mathbb{F}$-free in G. We claim that $(N/M)^\circ$ is $\mathbb{F}$-free in G/M. To see this, let $My \in N/M$ be p-regular and assume My is an $\mathbb{F}$-element in G/M. By the minimality of N among counterexamples, My contains a p-regular $\mathbb{F}$-element x of G. Since $My \subseteq N$ and N° is $\mathbb{F}$-free in G, it follows that $x = 1$ and My is the identity in G/M, i.e. $(N/M)^\circ$ is $\mathbb{F}$-free in G/M, as claimed.

Now set $\overline{G} = G/M$. Then $G/N \simeq \overline{G}/\overline{N}$ and $\overline{Nx}$ is a p-regular $\mathbb{F}$-element of $\overline{G}/\overline{N}$. By minimality of G among counterexample groups and since $\overline{N}^\circ$ is $\mathbb{F}$-free in $\overline{G}$, it follows that there is a p-regular $\mathbb{F}$-element of $\overline{G}$ contained in $\overline{Nx}$, call it $\bar{y}$. Equivalently, My is a p-regular $\mathbb{F}$-element in G/M. Again by the minimality of N we deduce that My contains a p-regular $\mathbb{F}$-element z of G. Finally, $My \subseteq Nx$, so $z \in Nx$ is a p-regular $\mathbb{F}$-element of G. This contradicts our assumption about N and so we must have that N is minimal normal in G.

Next, we argue that $N \leq \Phi(G)$, the Frattini subgroup. To see this, let H be a maximal subgroup of G and assume, aiming for a contradiction, that $N \nleq H$. Then $NH = G$ and $Nx = Nh$ for some $h \in H$. Let $D = N \cap H$ and note that the natural isomorphism $G/N \to H/D$ sends Nx to Dh. Since Nx is a p-regular $\mathbb{F}$-element in G/N, it follows that Dh is a p-regular $\mathbb{F}$-element in H/D. Also, $\mathbb{F}$-elements of H are automatically $\mathbb{F}$-elements of G and so it follows that D° is $\mathbb{F}$-free in H. By the minimality of G we conclude that $Dh \subseteq Nx$ contains a p-regular $\mathbb{F}$-element of G, but we are assuming that this is not the case. This contradiction implies that $N \leq H$ and so $N \leq \Phi(G)$. In particular, N is nilpotent and thus, since N is minimal normal in G, N is an elementary abelian ℓ-group for some prime ℓ.

Let $U = N\langle x\rangle$. We argue that $U \triangleleft G$. Now U/N is $\mathbb{F}$-cyclic in G/N and thus it is $\mathbb{F}$-cyclic in L/N, where $L/N = N_{G/N}(U/N)$. Aiming for a contradiction, suppose that $L < G$. Then by minimality of G, the coset Nx contains a p-regular $\mathbb{F}$-element of L, which is automatically a p-regular $\mathbb{F}$-element of G. But we are assuming Nx contains no such element and this contradiction implies that $L = G$, i.e. $U \triangleleft G$. Also note that U/N is cyclic and $N \leq \Phi(G)$, whence U is nilpotent (by [2, Lemma 9.19]).

Assume that $\ell = p$, i.e. N is a p-group. Since U is nilpotent and x is p-regular, it follows that $V := \langle x\rangle$ is the p-complement in U. In particular, $V \triangleleft G$. Since $V \simeq U/N$ as G-sets (under the conjugation action of G) and U/N is $\mathbb{F}$-cyclic in G/N, we conclude that V is $\mathbb{F}$-cyclic in G. By Lemma 2.3, every element of V is an $\mathbb{F}$-element. In particular, x is an $\mathbb{F}$-element in G and x is p-regular.

If instead $\ell \neq p$, then every element of N is p-regular and $N^\circ = N$ is $\mathbb{F}$-free in G. Thus by the Isaacs–Navarro Theorem 1.1 Nx contains an $\mathbb{F}$-element y of G. Now $Nx = Ny$ and, since $\langle y \rangle$ is $\mathbb{F}$-cyclic in G, by Lemma 2.3 it follows that $\langle y \rangle \cap N = 1$. We conclude that $o(y) = o(Ny)$, so y is p-regular. This is our final contradiction, and the proof is complete. □

We obtain the following useful corollary. The reductions in Theorems 4.5 and 5.6 to the case N is minimal normal in G rely on this statement. It is the p-modular analogue of [3, Corollary 3.4].

Corollary 3.2. *Let M and N be normal subgroups of the finite group G with $M \leq N$ and suppose that N° is $\mathbb{F}$-free in G. Then $(N/M)^\circ$ is $\mathbb{F}$-free in G/M.*

Proof. Suppose that Mx is a p-regular $\mathbb{F}$-element of G/M, where $Mx \in N/M$. Then by Theorem 3.1 Mx contains a p-regular $\mathbb{F}$-element y of G. Since $Mx \subseteq N$ and N° is $\mathbb{F}$-free in G, it follows that $y = 1$ and thus Mx is the identity of G/M, as required. □

Also, the first part of Theorem B follows easily. We can actually prove something slightly more general.

Corollary 3.3. *Assume that M and N are normal subgroups of G and that M° and N° are $\mathbb{F}$-free in G. Then $MN \lhd G$ and $(MN)^\circ$ is $\mathbb{F}$-free in G. In particular, G has a unique largest normal subgroup K such that K° is $\mathbb{F}$-free in G.*

Proof. The second statement follows from the first by taking K to be the subgroup of G generated by all normal subgroups N of G such that N° is $\mathbb{F}$-free in G.

For the first statement, obviously $MN \lhd G$. Let ψ be the natural G-isomorphism from MN/M to $N/(N \cap M)$. We make the following general observation: If C/M is $\mathbb{F}$-cyclic in G/M, with $M \leq C \leq MN$, and if C/M has order coprime to p, then $\psi(C/M)$ is $\mathbb{F}$-cyclic in $G/(M \cap N)$ and so all the elements of $\psi(C/M)$ are p-regular $\mathbb{F}$-elements of $G/(M \cap N)$.

Now let $x \in MN$ be a p-regular $\mathbb{F}$-element of G. We must show that $x = 1$. Note that Mx is a p-regular $\mathbb{F}$-element in G/M and we let C/M be the cyclic subgroup of G/M generated by Mx. By the previous paragraph, $\psi(C/M)$ is $\mathbb{F}$-cyclic in $G/(M \cap N)$ and $\psi(C/M)$ has order coprime to p. But $\psi(C/M)$ is contained in $N/(M \cap N)$ and $(N/(M \cap N))^\circ$ is $\mathbb{F}$-free in $G/(M \cap N)$, by Corollary 3.2. It follows that $\psi(C/M)$ is the identity in $G/(M \cap N)$, so C/M is the identity in G/M, i.e. $C = M$. Thus $x \in M$ and since M° is $\mathbb{F}$-free in G we conclude $x = 1$, as needed. □

4 Character kernels

It takes a bit more work to complete the proof of Theorem B. As mentioned earlier, the critical case for us will be when N is a non-abelian minimal normal subgroup of G and N° is $\mathbb{F}$-free in G. By the remarks following Lemma 2.2, we must have $p = 2$ and $N = S_1 \times \cdots \times S_r$, where $S_i \simeq S$ and $S = \mathrm{PSL}_2(3^{2n+1})$. As is well known, if σ is a Galois automorphism and ϕ a Brauer character, then in general ϕ^σ need not be a Brauer character. But it turns out that $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ does actually act on $\mathrm{IBr}_2(S)$ (see [7, Proposition 3.2 (ii)]). In fact, as we shall soon see, more is true. The next three results will allow us to adapt an important step in the proof of [3, Theorem 4.1] to work in our critical situation.

We establish some notation to be used in the next lemma: Let $S = \mathrm{PSL}_2(q)$, where $q = 3^{2n+1}$ and $n \geq 1$. Let $N_q := 3(q^2-1)/8 = \exp(S)_{2'}$ and let ϵ be a primitive N_qth root of unity. Then every $\phi \in \mathrm{IBr}(S)$ has values in $\mathbb{Q}(\epsilon)$.

Lemma 4.1. *In the above notation, there is a bijection $\phi \mapsto C_\phi$ between irreducible 2-Brauer characters of the group $S = \mathrm{PSL}_2(3^{2n+1})$ and conjugacy classes of odd-order elements in S that is compatible with the actions of $\mathrm{Aut}(S)$ and $\mathrm{Gal}(\mathbb{Q}(\epsilon)/\mathbb{Q})$, in the following sense. If $C_\phi = x^S$ for $\phi \in \mathrm{IBr}_2(S)$ and $x \in S$, then the following statements hold:*

(i) *for any $\tau \in \mathrm{Aut}(S)$, $C_{\phi^\tau} = (x^\tau)^S$,*

(ii) *for any $\sigma \in \mathrm{Gal}(\mathbb{Q}(\epsilon)/\mathbb{Q})$, $C_{\phi^\sigma} = (x^\sigma)^S$,*

(iii) *for any $\tau \in \mathrm{Aut}(S)$, $\sigma \in \mathrm{Gal}(\mathbb{Q}(\epsilon)/\mathbb{Q})$, and $\phi \in \mathrm{IBr}_2(S)$, $\phi^\sigma = \phi^\tau$ if and only if $C_\phi^\sigma = C_\phi^\tau$.*

Proof. The existence of the bijection and statements (i)–(ii) are [7, Lemma 3.4], and statement (iii) is an immediate consequence of (i) and (ii). □

Corollary 4.2. *Let N be a minimal normal subgroup of G and suppose that $N = S_1 \times \cdots \times S_r \simeq S^r$, where $S = \mathrm{PSL}_2(3^{2n+1})$. For $\phi = \phi_1 \times \cdots \times \phi_r \in \mathrm{IBr}_2(N)$, let $x = (x_1, \ldots, x_r) \in N$, where $C_{\phi_i} = (x_i)^{S_i}$ in the notation of Lemma 4.1. Set $C_\phi := x^N$. Then the map $\phi \mapsto C_\phi$ is a bijection between $\mathrm{IBr}_2(N)$ and $\mathrm{Cl}^\circ(N)$ that is compatible with the actions of G and $\mathrm{Gal}(\mathbb{Q}(\epsilon)/\mathbb{Q})$, in the sense of (i)–(iii) in Lemma 4.1.*

Proof. See [7, Corollary 3.5]. As in Lemma 4.1, statement (iii) follows at once from (i) and (ii). □

In the next statement, we use the following notation. If X is any group, then for any $\eta \in \mathrm{IBr}(X)$ we define $\mathbb{Q}(\eta)$ to be the field obtained by adjoining to $\mathbb{Q}$ all of the values $\eta(g)$ for $g \in X$. Similarly, if $g \in X$, then we define $\mathbb{Q}(g^X)$ to be the field obtained by adjoining to $\mathbb{Q}$ all of the values $\eta(g)$ for $\eta \in \mathrm{IBr}(X)$.

Corollary 4.3. *Let N be a minimal normal subgroup of G and suppose that $N = S_1 \times \cdots \times S_r \simeq S^r$, where $S = \mathrm{PSL}_2(3^{2n+1})$. Let $\phi \in \mathrm{IBr}_2(N)$ and let C_ϕ be as in Corollary 4.2. Then $\mathbb{Q}(\phi) = \mathbb{Q}(C_\phi)$.*

Proof. Let $\phi = \phi_1 \times \cdots \times \phi_r$, $C_\phi = (x_1, \ldots, x_r)^N$. Now $\mathbb{Q}(\phi) = \mathbb{Q}(\phi_1, \ldots, \phi_r)$ (by evaluating $\phi(y)$ for elements $y \in N$ with all but one component equal to $1 \in S$) and likewise $\mathbb{Q}(C_\phi) = \mathbb{Q}(x_1^S, \ldots, x_r^S)$ (by evaluating $\eta(x)$ for characters $\eta \in \mathrm{IBr}_2(N)$ with all but one component equal to $1_S \in \mathrm{IBr}_2(S)$). Thus it suffices to prove the claim for $r = 1$. This follows by inspecting the character table of $\mathrm{SL}_2(3^{2n+1})$, which can be found e.g. in [1, Chapter 38], and the explicit description of the map $\phi \mapsto C_\phi$, as given in [7]. □

Proposition 4.4. *Assume that $N = S_1 \times \cdots \times S_r \simeq S^r$ is a minimal normal subgroup of G, where $S = \mathrm{PSL}_2(3^{2n+1})$ for some $n \geq 1$. Assume that $\theta \in \mathrm{IBr}_{2,\mathbb{F}}(G)$ and $N \not\leq \ker\theta$. Then N° contains a non-trivial $\mathbb{F}$-element of G.*

Proof. Let $\phi \in \mathrm{IBr}_2(N)$ be a non-trivial constituent of the restriction θ_N. Let $N = \exp(S)_{2'}$, $n = |G|$, $\mathbb{K} = \mathbb{F} \cap \mathbb{Q}_N$, and $\mathbb{E} = \mathbb{F} \cap \mathbb{Q}_n$. Then $\mathbb{K} = \mathbb{E} \cap \mathbb{Q}_N$ and so restriction to $\mathbb{Q}_N$ defines a surjection from $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{E})$ onto $\mathrm{Gal}(\mathbb{Q}_N/\mathbb{K})$. Note that θ is an $\mathbb{E}$-character and that $x \in N^\circ$ is an $\mathbb{F}$-element in G if and only if it is a $\mathbb{K}$-element.

Now let $\sigma \in \mathrm{Gal}(\mathbb{Q}_N/\mathbb{K})$ and choose $\tau \in \mathrm{Gal}(\mathbb{Q}_n/\mathbb{E})$ whose restriction to $\mathbb{Q}_N$ is σ. Since $\theta^\tau = \theta$, it follows that $\phi^\tau = \phi^\sigma$ also enters θ_N ($\phi^\sigma \in \mathrm{IBr}_2(N)$ by [7, Proposition 3.2 (ii)]) and thus there is some $g \in G$ with $\phi^g = \phi^\sigma$. Let C_ϕ be the conjugacy class of N corresponding to ϕ under the bijection of Corollary 4.2. Then by Corollary 4.2 we have $C_\phi^g = C_\phi^\sigma$ and, by Corollary 4.3, we conclude that any $x \in C_\phi$ is a $\mathbb{K}$-element in G, whence it is an $\mathbb{F}$-element. Since $\phi \neq 1_N$, C_ϕ is non-trivial and so the proof is complete. □

We can now prove the assertion in Theorem B about character kernels.

Theorem 4.5. *Let $\phi \in \mathrm{IBr}_{\mathbb{F}}(G)$ and assume that N is a normal subgroup of G and that N° is $\mathbb{F}$-free in G. Then $N \leq \ker\phi$.*

Proof. Assume that the theorem is false. Arguing as in [3, Theorem 4.1], we may assume N is minimal normal in G. If N is not solvable, then, by the remarks following Lemma 2.2, we must have $p = 2$ and $N \simeq S^r$, where $S = \mathrm{PSL}_2(3^{2n+1})$. Applying Proposition 4.4, we obtain a contradiction.

So N is solvable and thus N is an elementary abelian ℓ-group for some prime ℓ. We have $\ell \neq p$, as otherwise $N \leq O_p(G) \leq \ker \phi$, e.g. by [5, Lemma 2.32]. Now the remainder of the proof of [3, Theorem 4.1] goes through unchanged (the point is, since N is a p'-group, we can identify $\mathrm{IBr}(N)$ with $\mathrm{Irr}(N)$). □

5 Conjugacy

Now we work toward proving the injectivity assertion in Theorem A, which is the major part of the paper. As usual, the critical case is $N = \mathrm{PSL}_2(3^{2n+1})^r$ and $p = 2$.

Lemma 5.1. *Suppose that $M, N \lhd G$, $M \cap N = 1$, and N° is $\mathbb{F}$-free in G. Let $x, y \in G^\circ$ be $\mathbb{F}$-elements such that $Nx = Ny \in G/N$. If $x \in M$, then $x = y$.*

Proof. We have $xn^{-1} = y$ for some $n \in N$. Also, $[M, N] \leq M \cap N = 1$ and so $[x, n] = 1$. Thus

$$1 = y^{o(y)} = x^{o(y)} n^{-o(y)} \implies n^{o(y)} = x^{o(y)} \in N \cap M = 1.$$

It follows that $o(n) \mid o(y)$ and thus $n \in N^\circ$. Now $A := N_G(\langle y \rangle)$ induces on $\langle y \rangle$ a group of automorphisms containing $\mathrm{Aut}_{\mathbb{F}}(\langle y \rangle)$. Let $n \mapsto n^t$ be any automorphism in $\mathrm{Aut}_{\mathbb{F}}(\langle n \rangle)$. By Lemma 2.4 we may express t in such a way that some $g \in A$ induces on $\langle y \rangle$ the map $y \mapsto y^t$. Then

$$x^g (n^{-1})^g = (xn^{-1})^g = y^g = y^t = (xn^{-1})^t = x^t n^{-t},$$

so $(n^{-1})^g n^t = (x^{-1})^g x^t \in N \cap M = 1$. We conclude that $n^g = n^t$, so n is an $\mathbb{F}$-element in G. Thus $n = 1$ and $x = y$. □

Lemma 5.2. *Fix an integer n and assume that $x \in H \leq \mathrm{Sym}(n)$ has prime order ℓ and is an $\mathbb{F}$-element in H. Let $t = |\mathbb{Q}_\ell : \mathbb{F} \cap \mathbb{Q}_\ell|$. Then there is some $h \in H$ such that the natural action of $\langle h \rangle$ on n points has an orbit of length t.*

Proof. We will identify $\{0, 1, \ldots, (\ell - 1)\} = \mathbb{F}_\ell$, the field with ℓ elements.

Since x is an $\mathbb{F}$-element, there is some $g \in H$ with $gxg^{-1} = x^a$, where a has order t in $\mathbb{F}_\ell^\times$. Also, since x has order ℓ, the non-trivial orbits of $\langle x \rangle$ all have length ℓ. Let $\Omega_1, \ldots, \Omega_m$ denote these orbits.

Now g permutes the Ω_i. We may assume that

$$g : \Omega_1 \to \Omega_2 \to \cdots \to \Omega_j \to \Omega_1$$

(possibly $j = 1$). We label the points of Ω_i by α_i, where $\alpha \in \mathbb{F}_\ell$, and choose the labeling in such a way that x acts on Ω_i via the cycle $(0_i, 1_i, \ldots, (\ell - 1)_i)$ and also

$$g : 0_1 \mapsto 0_2 \mapsto \cdots \mapsto 0_j \mapsto b_1 \quad \text{for some } b \in \mathbb{F}_\ell.$$

Thus x acts on $\Omega := \bigcup_{i=1}^{j} \Omega_i$ via

$$x = (0_1, 1_1, \ldots, (\ell-1)_1)(0_2, 1_2, \ldots, (\ell-1)_2) \ldots (0_j, 1_j, \ldots, (\ell-1)_j).$$

Now on the one hand we have, on Ω,

$$\begin{aligned} gxg^{-1} = (b_1, g(1_j), \ldots, g((\ell-1)_j))(0_2, g(1_1), \ldots, g((\ell-1)_1)) \\ \ldots (0_j, g(1_{j-1}), \ldots, g((\ell-1)_{j-1})) \end{aligned}$$

and on the other we have

$$\begin{aligned} x^a =& (b_1, (b+a)_1, (b+2a)_1, \ldots, (b+(\ell-1)a)_1)(0_2, a_2, \ldots, (\ell-1)a_2) \\ & \ldots (0_j, a_j, \ldots, (\ell-1)a_j). \end{aligned}$$

Thus we see that for any $\alpha_i \in \Omega$,

$$g(\alpha_i) = \begin{cases} (a\alpha)_{i+1}, & \text{if } 1 \le i \le j-1, \\ (b+a\alpha)_1, & \text{if } i = j. \end{cases}$$

Note that for any $\beta \in \Omega$ and any integer s, if $g^s(\beta) = \beta$, then $j \mid s$; also, the length of the $\langle g \rangle$-orbit of β is the minimal s such that $g^s(\beta) = \beta$. Thus, every $\langle g \rangle$-orbit on Ω has length a multiple of j. Finally, observe that to prove the lemma it actually suffices to show that $\langle g \rangle$ has an orbit on Ω with length a multiple of t (as then, for some power h of g, $\langle h \rangle$ has an orbit of exact length t). This is what we now prove.

If $a^j = 1$, then $t \mid j$ (recall that a has order t in $\mathbb{F}_\ell^\times$). By the previous paragraph any $\langle g \rangle$-orbit on Ω has length a multiple of t, and so we are finished. Thus we may assume that $a^j \neq 1$. For any $\alpha \in \mathbb{F}_\ell$ we compute

$$g^j(\alpha_1) = (b + a^j\alpha)_1,$$

so for any integer i we have

$$g^{ij}(\alpha_1) = (b(1 + a^j + \cdots + a^{j(i-1)}) + a^{ij}\alpha)_1.$$

Set $c = a^j \neq 1$ and choose $\alpha_1 \in \Omega_1$ with $\alpha \neq \frac{b}{1-c}$. Choose i minimal with $g^{ij}(\alpha_1) = \alpha_1$. The displayed equation implies that

$$\alpha(1 - c^i) = \frac{b(1-c^i)}{1-c}$$

and thus

$$(1 - c^i)\left(\alpha - \frac{b}{1-c}\right) = 0.$$

Since $\alpha \neq \frac{b}{1-c}$, we have $a^{ij} = c^i = 1$ and thus $t \mid ij$. Since i was chosen minimally, ij is the $\langle g \rangle$-orbit length of α_1 and so again by the previous paragraph we are finished. □

Theorem 5.3. *Let $p = 2$. Let $N = S_1 \times \cdots \times S_r \simeq S^r$, where $S = \mathrm{PSL}_2(3^{2n+1})$ for some $n \geq 1$. Assume that N is a minimal normal subgroup of G, $C_G(N) = 1$, and N° is $\mathbb{F}$-free in G. Let $x \in G^\circ$ be an $\mathbb{F}$-element with odd prime order ℓ and assume that $|\mathbb{Q}_\ell : \mathbb{F} \cap \mathbb{Q}_\ell| = t$. Then there is some $g \in G$ such that $\langle g \rangle$ has an orbit of length t on the factors $\{S_1, \ldots, S_r\}$.*

Proof. By the minimality of N, any $g \in G$ permutes the factors $\{S_1, \ldots, S_r\}$ so the claim makes sense. Let $x \mapsto x^i$ have order t in $\mathrm{Aut}(\langle x \rangle)$, so that $x \mapsto x^i$ is a generator of $\mathrm{Aut}_{\mathbb{F}}(\langle x \rangle)$. Since N° is $\mathbb{F}$-free in G, $\bar{x} \in \overline{G} := G/N$ has order ℓ and of course it is still an $\mathbb{F}$-element. Let $g \in G$ satisfy $x^g = x^i$, so also $\bar{x}^{\bar{g}} = \bar{x}^i$.

Since $C_G(N) = 1$, we may view

$$\overline{G} \leq \mathrm{Out}(N) \simeq \mathrm{Out}(S) \wr \mathrm{Sym}(r).$$

Write $\bar{g} = h\pi$, where $h \in \mathrm{Out}(S)^r$ and $\pi \in \mathrm{Sym}(r)$. Suppose first that x fixes every factor S_m, i.e. that $\bar{x} \in \mathrm{Out}(S)^r$, and write $\bar{x} = (x_1, \ldots, x_r)$, where each $x_i \in \mathrm{Out}(S_i)$. Assume, without loss, that $o(x_1) = \ell$. As $\mathrm{Out}(S)$ is abelian, we have

$$(x_1^i, \ldots, x_r^i) = \bar{x}^i = \bar{x}^g = \bar{x}^{h\pi} = \bar{x}^\pi = (x_{\pi^{-1}(1)}, \ldots, x_{\pi^{-1}(r)})$$

and, for any integer j,

$$(x_1^{i^j}, \ldots, x_r^{i^j}) = \bar{x}^{\pi^j} = (x_{\pi^{-j}(1)}, \ldots, x_{\pi^{-j}(r)}).$$

Since $o(x_1) = \ell = o(x)$, the map $x_1 \mapsto x_1^i$ has order t. Thus the $x_1^{i^j}$ are all distinct for $1 \leq j \leq t$ and we conclude that the $\langle g \rangle$-orbit of S_1 has length at least t. But since $\bar{x}^{g^t} = \bar{x}^{i^t} = \bar{x}$, clearly this orbit has length at most t.

Thus we may assume that x moves some factor S_m. So the image of x under the composition of natural maps

$$G \to G/N \hookrightarrow \mathrm{Out}(S) \wr \mathrm{Sym}(r) \to \mathrm{Sym}(r)$$

is an $\mathbb{F}$-element of order ℓ. Let H denote the image of G under this map, so by Lemma 5.2 there is some $h \in H$ such that $\langle h \rangle$ has an orbit of length t on the factors $\{S_1, \ldots, S_r\}$; equivalently, for any preimage $g \in G$ of h, $\langle g \rangle$ has an orbit of length t on $\{S_1, \ldots, S_r\}$. This completes the proof. □

This next statement is the last major ingredient that we need.

Theorem 5.4. *Fix a prime ℓ. Let $N = S_1 \times \cdots \times S_r \simeq S^r$, where $S = \mathrm{PSL}_2(3^{2n+1})$ for some $n \geq 1$. Further, assume that N is a minimal normal subgroup of G with $C_G(N) = 1$. Assume that some $g \in G$ permutes the factors $\{S_1, \ldots, S_r\}$ with an orbit of length t, where $t = |\mathbb{Q}_\ell : \mathbb{F} \cap \mathbb{Q}_\ell|$. If ℓ divides $|N|$, then there is some $\mathbb{F}$-element of G with order ℓ contained in N.*

Before giving the proof we establish some notation and conventions. In the situation of Theorem 5.4, assume that $g : S_1 \mapsto S_2 \mapsto \cdots \mapsto S_t \mapsto S_1$. Let i_g denote the conjugation-by-g map. Then all of the groups S_i may be identified via appropriate powers of i_g, e.g. $i_g(S_1) = S_2$, etc. We extend this to obtain identifications between all of the groups $\mathrm{Aut}(S_i)$. In order to simplify the notation, we will use these identifications to make sense of products of elements in $\mathrm{Aut}(S_i)$ and $\mathrm{Aut}(S_j)$, and view these products in $\mathrm{Aut}(S_k)$, even when none of i, j, k are necessarily equal.

For example, if $h_1 \in \mathrm{Aut}(S_1)$ and $h_2 \in \mathrm{Aut}(S_2)$, we will make sense of h_1h_2 as an element of any or all of $\mathrm{Aut}(S_1)$, $\mathrm{Aut}(S_2)$, or $\mathrm{Aut}(S_3)$. Here it is to be understood that by h_1h_2 we really mean $h_1(i_{g^{-1}} \circ h_2)$ in the first case, $(i_g \circ h_1)h_2$ in the second, or $(i_{g^2} \circ h_1)(i_g \circ h_2)$ in the third. The intended meaning of a product like h_1h_2 will always be clear from context.

Finally, a bit of notation: if $h_i \in \mathrm{Aut}(S_i)$ for $i = 1, \ldots, r$ and if $a \leq b$ are integers, we define

$$h_{a:b} := \prod_{i=a}^{b} h_i.$$

Proof of Theorem 5.4. We have

$$N \leq G \leq \mathrm{Aut}(N) \simeq \mathrm{Aut}(S) \wr \mathrm{Sym}(r).$$

Write $g = h\pi$, where $h \in \mathrm{Aut}(S)^r$ and $\pi \in \mathrm{Sym}(r)$. Reordering the factors, if necessary, we may assume that

$$g : S_1 \mapsto S_2 \mapsto \cdots \mapsto S_t \mapsto S_1.$$

We will show that there is an element v in $S_1 \times \cdots \times S_t$ with order ℓ and such that $\langle g \rangle$ induces on $\langle v \rangle$ a group of automorphisms containing $\mathrm{Aut}_{\mathbb{F}}(\langle v \rangle)$. Thus, there is no loss to assume that $r = t$. Since $\mathrm{Aut}(S)$ is split over S, by [4], we may choose a complement $O \leq \mathrm{Aut}(S)^t$ for N and identify O with $\mathrm{Out}(S)^t$. Therefore, by replacing g by ng for some appropriate $n \in N$, we may assume that $h \in O$ and that h acts on N via $(h_1, \ldots, h_t) \in \mathrm{Out}(S)^t$. Clearly this new choice of g still has an orbit of length t on the factors S_i. Recall that $\mathrm{Out}(S)$ is abelian.

The cases $\ell = 2$ and $\ell = 3$ are handled differently from the case $\ell > 3$, so we divide the proof into three steps.

Step (1). Assume that $\ell = 2$. Any involution in N is rational, hence an $\mathbb{F}$-element, and we are done.

Step (2). Assume that $\ell = 3$. Then either $\mathbb{Q}_3 \cap \mathbb{F} = \mathbb{Q}_3$, every element of order 3 in N is an $\mathbb{F}$-element, and we are finished; or else $\mathbb{Q}_3 \cap \mathbb{F} = \mathbb{Q}$ and $t = 2$. Let $u \in S$ be any element of order 3. Recall that $u^S \neq (u^{-1})^S$ and any $h \in \mathrm{Aut}(S)$

either fixes both u^S and $(u^{-1})^S$ or else h exchanges these classes. Now g^2 fixes both factors S_1 and S_2 and acts on both via h_1h_2.

If h_1h_2 sends u^S to $(u^{-1})^S$, then choosing $v = (u, 1)$ we have

$$(v^{g^2})^N = (u^{h_1h_2}, 1)^N = (u^{-1}, 1)^N = (v^{-1})^N$$

and so v is rational in G. If instead h_1h_2 fixes both u^S and $(u^{-1})^S$, then either h_1 and h_2 each fix both classes or else h_1 and h_2 each send u^S to $(u^{-1})^S$. In the first case we choose $v = (u, u^{-1})$ and in the second we choose $v = (u, u)$. In either case, $(v^g)^N = (v^{-1})^N$. Again, v is rational. This completes the case $\ell = 3$.

Step (3). Finally, assume that $\ell > 3$. Then ℓ divides $q \pm 1$, where $q = 3^{2n+1}$.

We begin by making an explicit choice for O. Recall that $\mathrm{Out}(S)$ is generated by field and diagonal automorphisms. We choose δ to be the diagonal automorphism of S induced from conjugation by $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$. When $\ell \mid q-1$, we choose ϕ to be the field automorphism induced from $x \mapsto x^3$ on $\mathbb{F}_q$; when $\ell \mid q+1$, we view S as $\mathrm{PSU}_2(q)$ and choose ϕ to be the field automorphism induced from $x \mapsto x^9$ on $\mathbb{F}_{q^2}$. We choose

$$O = (\langle\delta\rangle \times \langle\phi\rangle)^t.$$

If $\ell \mid q-1$, then view $S = \mathrm{PSL}_2(q)$ and if $\ell \mid q+1$, view $S = \mathrm{PSU}_2(q)$. Consider the diagonal torus T of S, which has order $q-1$ or $q+1$, according as $S = \mathrm{PSL}_2(q)$ or $\mathrm{PSU}_2(q)$. Now choose $u \in T$ to have order ℓ. It is clear that u is fixed by δ and $\langle u\rangle$ is $\langle\phi\rangle$-stable. By our choice of u and assumptions about g, $\langle g\rangle$ acts on

$$U = \underbrace{\langle u\rangle \times \cdots \times \langle u\rangle}_{t \text{ times}} \le N.$$

Now g^t acts on N via $(k, \ldots, k)$, where $k = h_{1:t}$ – in particular, g^t fixes every factor S_i. Let $u \mapsto u^a$ be the automorphism of $\langle u\rangle$ induced by k and let s denote the order of this automorphism. Let $d = \gcd(s, t)$ and $f = t/d$. Since $\mathrm{Aut}(\langle u\rangle) \simeq C_{\ell-1}$, t and s both divide $\ell - 1$ and so $fs \mid (\ell-1)$ as well. Thus we may choose an fth root of $u \mapsto u^a$, say $u \mapsto u^i$, so that $k : u \mapsto u^{i^f}$.

We choose an element $v = (v_1, v_2, \ldots, v_t) \in U$ as follows: $v_1 = u =: u_f$ and for $1 \le j \le (f-1)$, we recursively define $v_{jd+1} =: u_j$, where

$$u_j = (u_{j+1}^i)^{h^{-1}_{(jd+1):(j+1)d}}.$$

All other components of v we define to be 1.

We claim that $v^{g^d} = v^i$. Note that the map $u \mapsto u^i$ has order $sf = (s/d)t$ in $\mathrm{Aut}(\langle u\rangle)$, and thus $v \mapsto v^i$ also has order $(s/d)t$. Since $o(v) = \ell$, we have $\mathrm{Aut}_{\mathbb{F}}(\langle v\rangle) \le \langle v \mapsto v^i\rangle$ and so, given the claim, it follows that v is an $\mathbb{F}$-element in G. To prove the claim, observe that the component of v^{g^d} in position m is given by $v_{m-d}^{h_{(m-d):(m-1)}}$. So from the construction of v it is obvious that $v^{g^d} = v^i$, except possibly in the $(d+1)$st component. In other words, to prove the claim we need only check that

$$v_{d+1}^i = v_1^{h_{1:d}}, \quad \text{or equivalently} \quad u_1^i = u^{h_{1:d}}.$$

By repeated back-substitution using the definition of the u_j, we have

$$u_1^i = (u^{i^f})^{h^{-1}_{(d+1):t}} = (u^k)^{h^{-1}_{(d+1):t}} = u^{h_{1:d}},$$

as needed. This completes the proof. □

We need one more lemma, which is an easy consequence of the well-known Schur–Zassenhaus theorem.

Lemma 5.5. *Let $N \lhd G$ and let $x, y \in G$. Further, suppose that $o(x) = o(y)$, that $(|N|, o(x)) = 1$, and that $Nx = Ny \in G/N$. Then x and y are N-conjugate.*

Proof. By the Schur–Zassenhaus theorem there is some $n \in N$ with $\langle x\rangle^n = \langle y\rangle$. Thus $y = (x^k)^n$ for some integer k coprime to $o(x)$. We have

$$Nx = Ny = N(x^k)^n = Nx^k$$

and thus $x^{k-1} \in N$. Since $o(x)$ is coprime to $|N|$, though, we have $\langle x\rangle \cap N = 1$ and thus $x^k = x$. We conclude that $x^n = y$, which completes the proof. □

Finally, we complete the proof of Theorem A.

Theorem 5.6. *Let $N \lhd G$ and assume that N° is $\mathbb{F}$-free in G. Then the canonical homomorphism $G \to G/N$ induces an injection $\mathrm{Cl}_{\mathbb{F}}^\circ(G) \to \mathrm{Cl}_{\mathbb{F}}^\circ(G/N)$.*

Proof. Assume that the theorem is false, let G be a minimal counterexample, and let N be minimal among normal subgroups of G which give rise to a counter-example. This means there are p-regular $\mathbb{F}$-elements $x, y \in G$ such that $x^G \neq y^G$ but $Nx = Ny$. Arguing as in [3, Theorem 5.1], we may assume that N is minimal normal in G.

If N is non-solvable, then, by the remarks following Lemma 2.2, we have $p = 2$ and $N = S_1 \times \cdots \times S_r \simeq S^r$, where $S = \mathrm{PSL}_2(3^{2n+1})$. Let $C = C_G(N)$, let π denote the set of prime divisors of $|N|$, and write $x = x_\pi x_{\pi'}$ and $y = y_\pi y_{\pi'}$.

We claim that $x_\pi \in C$. Assume that this is not the case. We set $\overline{G} = G/C$ and $\overline{N} = NC/C \simeq N$. Now our assumption is that $\bar{x}_\pi$ is non-trivial and, since powers of $\mathbb{F}$-elements are $\mathbb{F}$-elements, there is some $\ell \in \pi$ and some power of $\bar{x}_\pi$ that is an $\mathbb{F}$-element of order ℓ. We have that $\overline{N}^\circ$ is $\mathbb{F}$-free in $\overline{G}$, by Lemma 2.5, and thus by Theorem 5.3 there is some $\bar{g} \in \overline{G}$ permuting the factors S_i of $\overline{N}$ with an orbit of length $t = |\mathbb{Q}_\ell : \mathbb{Q}_\ell \cap \mathbb{F}|$. Theorem 5.4 now guarantees the existence of an $\mathbb{F}$-element of $\overline{G}$ contained in $\overline{N}$ and of order ℓ. This is a contradiction and we conclude that $x_\pi \in C$, as claimed. Thus, by Lemma 5.1, $x_\pi = y_\pi$.

Note that $(Nx)_{\pi'} = Nx_{\pi'}$ and similarly $(Ny)_{\pi'} = Ny_{\pi'}$. By Lemma 2.3 we have

$$\langle x_{\pi'} \rangle \cap N = 1 = \langle y_{\pi'} \rangle \cap N$$

and thus

$$o(x_{\pi'}) = o(Nx_{\pi'}) = o(Ny_{\pi'}) = o(y_{\pi'}).$$

By Lemma 5.5, $x_{\pi'}^n = y_{\pi'}$ for some $n \in N$. Since $x_\pi = y_\pi \in C$, it follows that $x^n = y$, which we assumed is not the case.

The contradiction in the previous paragraph shows that N must be solvable. So N is an elementary abelian ℓ-group for some prime ℓ. In this case, too, we conclude that $x^G = y^G$ – if $\ell = p$, then, since x and y are p-regular, we may apply Lemma 5.5 as above; and if $\ell \neq p$, then $N^\circ = N$ is $\mathbb{F}$-free in G, so we may apply the Isaacs–Navarro Theorem 1.1. □

Acknowledgments. This article is based on some of the results of the author's PhD thesis at the University of Arizona, under the supervision of Pham Huu Tiep. I gratefully acknowledge Professor Tiep's support and thank him for several helpful conversations.

Bibliography

[1] L. Dornhoff, *Group Representation Theory. Part A: Ordinary Representation Theory*, Pure Appl. Math. 7, Marcel Dekker, New York, 1971.

[2] I. M. Isaacs, *Finite Group Theory*, Grad. Stud. Math. 92, American Mathematical Society, Providence, 2008.

[3] I. M. Isaacs and G. Navarro, Group elements and fields of character values, *J. Group Theory* **12** (2009), no. 5, 635–650.

[4] A. Lucchini, F. Menegazzo and M. Morigi, On the existence of a complement for a finite simple group in its automorphism group, *Illinois J. Math.* **47** (2003), no. 1–2, 395–418.

[5] G. Navarro, *Characters and Blocks of Finite Groups*, London Math. Soc. Lecture Note Ser. 250, Cambridge University Press, Cambridge, 1998.

[6] G. Navarro and P. H. Tiep, Rational irreducible characters and rational conjugacy classes in finite groups, *Trans. Amer. Math. Soc.* **360** (2008), no. 5, 2443–2465.

[7] G. Navarro and P. H. Tiep, Brauer characters and rationality, *Math. Z.* **276** (2014), no. 3–4, 1101–1112.

Received May 26, 2017; revised May 31, 2017.

Author information

Dan Rossi, Department of Mathematics, University of Arizona,
Tucson, AZ 85721-0089, USA.
E-mail: drossi@math.arizona.edu