Forum of Mathematics, Pi (2021), **Vol. 9**:e2 1–28
doi:10.1017/fmp.2021.1

CAMBRIDGE
UNIVERSITY PRESS

RESEARCH ARTICLE

The fields of values of characters of degree not divisible by *p*

Gabriel Navarro[1] and Pham Huu Tiep[2]

[1]Department of Mathematics, Universitat de València, València, Spain; E-mail: gabriel@uv.es.
[2]Department of Mathematics, Rutgers University, Piscataway, NJ, USA; E-mail: tiep@math.rutgers.edu.

Received: 2 April 2020; **Revised:** 5 September 2020; **Accepted:** 6 January 2021

2020 Mathematics Subject Classification: *Primary* – 20C15, 20C33

Abstract
We study the fields of values of the irreducible characters of a finite group of degree not divisible by a prime p. In the case where $p = 2$, we fully characterise these fields. In order to accomplish this, we generalise the main result of [ILNT] to higher irrationalities. We do the same for odd primes, except that in this case the analogous results hold modulo a simple-to-state conjecture on the character values of quasi-simple groups.

Dedicated to Gunter Malle on the occasion of his 60th birthday

1. Introduction

It is of great interest to study the values of the complex irreducible characters of a finite group G. If χ is a character (not necessarily irreducible) of a finite group G, the *field of values* $\mathbb{Q}(\chi)$ of χ is the smallest field containing $\chi(g)$ for all $g \in G$. Since $\chi(g)$ is a sum of $o(g)$-th roots of unity, $\mathbb{Q}(\chi)$ is a subfield of the cyclotomic field $\mathbb{Q}_n = \mathbb{Q}(\exp(2\pi i/n))$, where $n = |G|$ and $i = \sqrt{-1}$. Among the numerical invariants which we can associate to an arbitrary character χ of a finite group, the two most important are the *degree* $\chi(1)$ and the *conductor* of χ, which is the smallest positive integer f such that $\mathbb{Q}(\chi) \subseteq \mathbb{Q}_f$ (that is, the absolute or global conductor of the field $\mathbb{Q}(\chi)$). In general, there is nothing special about the subfield $\mathbb{Q}(\chi)$ and the irrationalities admitted by χ: it is not difficult to show that given any finite abelian extension F of $\mathbb{Q}$, there is a finite group G having some $\chi \in \mathrm{Irr}(G)$ such that $\mathbb{Q}(\chi) = F$. (See Theorem 2.2.) Surprisingly, this situation changes drastically if we know that $\chi(1)$ is not divisible by some prime p. For instance, if $\chi(1)$ is odd and $\mathbb{Q}(\chi) = \mathbb{Q}(\sqrt{d})$ for a square-free integer $d \neq -1$, then $d \equiv 1 \pmod 4$. This is a consequence of the recent main result of [ILNT], whose proof uses the classification of finite simple groups: if $\chi(1)$ is odd, then either $\mathbb{Q}(\chi)$ is contained in the cyclotomic field $\mathbb{Q}_m$ for some odd integer m or $i \in \mathbb{Q}(\chi)$.

We consider the following deep problem in representation theory: for a given prime p, what is the set of abelian extensions

$$\mathcal{F}_p = \left\{\mathbb{Q}(\chi)/\mathbb{Q} \mid \chi \in \mathrm{Irr}_{p'}(G),\ G \text{ a finite group}\right\},$$

where $\mathrm{Irr}_{p'}(G)$ is the set of complex irreducible characters of G of degree not divisible by p?

In the first two main theorems in this paper, we solve this problem for $p = 2$. First, we need to vastly generalise the main result in [ILNT] (which is the case $a = 2$ of the following theorem).

Theorem A1. *Suppose that $\chi \in \mathrm{Irr}(G)$ has odd degree and conductor $2^a m$, where m is odd and $a \in \mathbb{Z}_{\geq 0}$. Then $\mathbb{Q}_{2^a} \subseteq \mathbb{Q}(\chi)$.*

Hence, if $\mathbb{F}/\mathbb{Q} \in \mathcal{F}_2$, by Theorem A1 we have that $\mathbb{Q}_{2^a} \subseteq \mathbb{F}$, where 2^a is the 2-part of the conductor of the field $\mathbb{F}$. (In this paper, we simply use *conductor of* $\mathbb{F}$ to denote the smallest $f \geq 1$ such that $\mathbb{F} \subseteq \mathbb{Q}_f$, whenever $\mathbb{F}/\mathbb{Q}$ is an abelian extension in $\mathbb{C}$.) To complete our work, we will show that these are all the possible extensions in $\mathcal{F}_2$. This is not so easy to accomplish. In Section 2 we prove that many abelian field extensions of $\mathbb{Q}$ – for instance, $\mathbb{Q}(\sqrt{57})$ and $\mathbb{Q}(\sqrt{65})$ – cannot be achieved in solvable groups. However, we can prove that these extensions are attained in the realms of general finite (nonsolvable) groups. The following result, together with Theorem A1, provides a complete determination of $\mathcal{F}_2$:

Theorem A2. *Let $\mathbb{F}/\mathbb{Q}$ be an abelian extension of $\mathbb{Q}$ with conductor $n = 2^a m$, where m is odd and $a \in \mathbb{Z}_{\geq 0}$. Suppose that $\mathbb{Q}_{2^a} \subseteq \mathbb{F}$. Then there exist a finite group G and $\chi \in \mathrm{Irr}_{2'}(G)$ such that $\mathbb{F} = \mathbb{Q}(\chi)$.*

In particular, if $d \neq -1$ is a square-free integer, then $\mathbb{Q}(\chi) = \mathbb{Q}(\sqrt{d})$ for some finite group G and some odd-degree irreducible character $\chi \in \mathrm{Irr}(G)$ precisely when $d \equiv 1 \pmod 4$.

We are able to prove Theorem A1, using the classification of finite simple groups, only because we prove something much stronger for quasi-simple groups. Recall that χ_P (or $\chi|_P$) is the restriction of the character χ to the subgroup P.

Theorem A3. *Suppose that G is a finite quasi-simple group, and $\chi \in \mathrm{Irr}(G)$ has odd degree and conductor $2^a m$, where m is odd and $a \in \mathbb{Z}_{\geq 0}$. If $a \geq 2$, then there exists a 2-element $g \in G$ such that $\chi(g) \notin \mathbb{Q}_{2^{a-1}}$. Furthermore, for all $a \geq 0$, we have $\mathbb{Q}(\chi_P) = \mathbb{Q}_{2^a}$ for $P \in \mathrm{Syl}_2(G)$.*

Theorem A3 shows something perhaps surprising: the field of values of $\mathbb{Q}(\chi_P)$, if G is quasi-simple and $\chi(1)$ is odd, is a full cyclotomic field. (This is not true if $\chi(1)$ is even, as shown by $2.\mathsf{A}_6$.) We will comment more on this later.

Our second set of main results is the p-odd version of Theorems A1, A2 and A3. We characterise $\mathcal{F}_p$ modulo a natural question on the values of characters of quasi-simple groups (Conjecture B3). For many quasi-simple groups we can answer this question (see Theorem 6.1); for others we cannot: surprising as it may seem, the character values of certain quasi-simple groups are far from understood.

Theorem B1. *Let p be any prime and suppose that Conjecture B3 holds. Let G be any finite group and let $\chi \in \mathrm{Irr}_{p'}(G)$ have conductor $p^a m$, where p does not divide m and $a \in \mathbb{Z}_{\geq 0}$. Then p does not divide $[\mathbb{Q}_{p^a} : (\mathbb{Q}(\chi) \cap \mathbb{Q}_{p^a})]$.*

Notice that for $p = 2$, the conclusion of Theorem B1 is exactly Theorem A1. In order to prove the p-odd analog of Theorem A2 – Theorem B2 – we will need a group-theoretic construction which is also of independent interest (Theorem 3.3).

Theorem B2. *Let $\mathbb{F}/\mathbb{Q}$ be an abelian extension of $\mathbb{Q}$ with conductor $n = p^a m$, where p does not divide m and $a \in \mathbb{Z}_{\geq 0}$. Suppose that $[\mathbb{Q}_{p^a} : (\mathbb{F} \cap \mathbb{Q}_{p^a})]$ is not divisible by p. Then there exist a finite group G and a character $\chi \in \mathrm{Irr}_{p'}(G)$ such that $\mathbb{F} = \mathbb{Q}(\chi)$.*

Conjecture B3. *Let G be a finite quasi-simple group and p be an odd prime, and set $\chi \in \mathrm{Irr}_{p'}(G)$. Suppose $f = p^a m$ is the conductor of χ, where p does not divide m and $a \in \mathbb{Z}_{\geq 0}$. Then there exists a p-element $g \in G$ such that $\mathbb{Q}(\chi(g)) \subseteq \mathbb{Q}_{p^a}$ and p does not divide $[\mathbb{Q}_{p^a} : \mathbb{Q}(\chi(g))]$.*

As mentioned already, if Conjecture B3 holds, then Theorems B1 and B2 completely determine the set $\mathcal{F}_p$ of fields of values of the p'-degree irreducible characters in finite groups for every odd prime p.

Some remarks are in order here. First, the conclusion of Conjecture B3 does not hold if p divides $\chi(1)$: for example, $\mathrm{SL}_6(2)$ for $p = 3$. More importantly, we do not know if the statement of Conjecture

B3 holds true for every finite group; on the other hand, we have verified it for many quasi-simple groups, as we have said, in Theorem 6.1. In fact, we have accumulated enough evidence for the following conjecture, which would offer further new insights into the general problem of how the p'-degree characters of a finite group G restrict to a Sylow p-subgroup P of G. This conjecture begins the last and shortest part of this paper.

Conjecture C. *Suppose that G is a finite group, p is a prime and $\chi \in \mathrm{Irr}_{p'}(G)$. Suppose that χ has conductor $p^a m$, where p does not divide m and $a \in \mathbb{Z}_{\geq 0}$. Let $P \in \mathrm{Syl}_p(G)$. Then the degree of the extension $\mathbb{Q}_{p^a}/\mathbb{Q}(\chi_P)$ is not divisible by p.*

Note that Conjecture C implies, among other results, that if $\chi \in \mathrm{Irr}(G)$ has odd degree and $P \in \mathrm{Syl}_2(G)$, then χ is 2-rational (i.e., has odd conductor) exactly when χ_P is rational-valued. This does not seem to have been noticed before.

2. Solving the equation $\mathbb{Q}(\chi) = F$

Before going into the main results of this paper, we prove in this section that given any abelian extension $F/\mathbb{Q}$, where $F \subseteq \mathbb{C}$, there exist a finite group G and $\chi \in \mathrm{Irr}(G)$ such that $F = \mathbb{Q}(\chi)$. We also answer the question of what are exactly the fields of values of groups of odd order (therefore generalising a classical result of W. Burnside), and we determine the field of values of odd-degree irreducible characters of solvable groups. We also do some preliminaries which are necessary for the rest of the paper.

Our notation for characters follows [Is2] and [N2]. If $F/\mathbb{Q}$ is an abelian extension of $\mathbb{Q}$, then the conductor $c(F)$ of F is the smallest integer $n \geq 1$ such that $F \subseteq \mathbb{Q}_n$, where in this paper $\mathbb{Q}_n$ denotes the n-th cyclotomic field. In particular, $c(F)$ is odd or divisible by 4. Recall that the conductor $c(\psi)$ of a character ψ of a group G is $c(\mathbb{Q}(\psi))$. If $\mathbb{Q}(\psi) \subseteq \mathbb{Q}_m$ for some integer $m \geq 1$, then $c(\psi)$ divides m, by elementary Galois theory. In particular, $c(\psi)$ divides the exponent of G. If p is a prime, a character ψ is *p-rational* if p does not divide $c(\psi)$. If $K \subseteq \mathbb{C}$, we denote by $K(\psi)$ the smallest field containing K and the values of ψ. A few times, if α and β are characters, we write $K(\alpha, \beta)$ to denote $K(\alpha)(\beta)$. If $n \geq 1$ is an integer and p is a prime, then n_p is the largest power of p dividing n. We remind the reader that $\mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q})$, where $\mathbb{Q}^{\mathrm{ab}}$ is the field in $\mathbb{C}$ generated by all roots of unity, acts on $\mathrm{Irr}(G)$ for every finite group, as well as $\mathrm{Aut}(G)$, and that both actions commute (see [N2, Chapters 2 and 3], for instance).

Lemma 2.1. *Let G be a finite group, and let N be a normal subgroup of G. Let $\chi \in \mathrm{Irr}(G)$, let $\theta \in \mathrm{Irr}(N)$ be an irreducible constituent of χ_N, let T be the stabiliser of θ in G and let $\psi \in \mathrm{Irr}(T|\theta)$ be the Clifford correspondent of χ over θ.*

(i) *We have $\mathbb{Q}(\chi) \subseteq \mathbb{Q}(\psi)$, and therefore $c(\chi)$ divides $c(\psi)$. Also, $\mathbb{Q}(\chi_N) \subseteq \mathbb{Q}(\theta)$ and $\mathbb{Q}(\theta, \chi) = \mathbb{Q}(\psi)$.*
(ii) *Let $\sigma \in \mathrm{Gal}(\mathbb{Q}(\psi)/\mathbb{Q}(\chi))$. If $o(\sigma)$ and $|\mathbf{N}_G(T)/T|$ are coprime, then σ is trivial.*

Proof. Since $\psi^G = \chi$, by the induction formula we notice that $\mathbb{Q}(\chi) \subseteq \mathbb{Q}(\psi)$. Thus $\mathbb{Q}(\chi) \subseteq \mathbb{Q}_{c(\psi)}$, and therefore $c(\chi)$ divides $c(\psi)$. Since ψ_N is a multiple of θ, notice that $\mathbb{Q}(\theta) \subseteq \mathbb{Q}(\psi)$. By Clifford's theorem, χ_N is a sum of G-conjugates of θ, and since $\mathbb{Q}(\theta) = \mathbb{Q}(\theta^g)$ for $g \in G$, we have $\mathbb{Q}(\chi_N) \subseteq \mathbb{Q}(\theta)$. For the final part of (i), notice that if $\sigma \in \mathrm{Gal}(\mathbb{Q}(\psi)/\mathbb{Q}(\theta, \chi))$, then $\theta^\sigma = \theta$, $\chi^\sigma = \chi$ and therefore $\psi^\sigma = \psi$ by the uniqueness in the Clifford correspondence.

For (ii), we have $\chi = \chi^\sigma$. Hence $\theta^\sigma = \theta^g$ for some element $g \in G$, using Clifford's theorem. Notice then that $g \in \mathbf{N}_G(T)$. As we said, recall that the action of G on $\mathrm{Irr}(N)$ and the Galois action commute. Let $q = o(\sigma)$. Now $\theta = \theta^{\sigma^q} = \theta^{g^q}$, so $g^q \in T$. Since $|\mathbf{N}_G(T)/T|$ and q are coprime, it follows that $g \in T$, so $\theta^\sigma = \theta^g = \theta$. Then $\psi^\sigma = \psi$, by the uniqueness in the Clifford correspondence, and we deduce that σ is trivial. □

Theorem 2.2. *Let $m \geq 1$ be an integer, and let $\mathbb{Q} \subseteq F \subseteq \mathbb{Q}_m$ be any subfield. Then there exists a solvable finite group G of order $m[\mathbb{Q}_m : F]$ having $\chi \in \mathrm{Irr}(G)$, of degree $[\mathbb{Q}_m : F]$, such that $\mathbb{Q}(\chi) = F$.*

Proof. Let ξ be a primitive mth root of unity. Let $C = \langle \xi \rangle$, a cyclic group of order m. Let $H = \mathrm{Gal}(\mathbb{Q}_m/F)$. We have that H is naturally isomorphic to a subgroup of $\mathrm{Aut}(C)$. Now let $G = CH$ be the semidirect product, and let $\lambda \in \mathrm{Irr}(C)$ be of order m. Notice that the stabiliser of λ in H is trivial. Therefore $\lambda^G = \chi \in \mathrm{Irr}(G)$ by the Clifford correspondence. By Lemma 2.1(i), we have $\mathbb{Q}(\chi) \subseteq \mathbb{Q}_m$. We claim that $\mathbb{Q}(\chi) = F$. In order to prove this, it is enough to show that $\sigma \in \mathrm{Gal}(\mathbb{Q}_m/\mathbb{Q})$ fixes χ if and only if $\sigma \in H$. Of course, if $\sigma \in H$, we have that σ fixes χ, since $\sigma \in G$. Conversely, if σ fixes χ, then we have that λ and λ^σ lie under χ. By Clifford's theorem, we have $\lambda^\sigma = \lambda^\tau$ for some $\tau \in H$. Then $\sigma = \tau \in H$, and the proof of the theorem is complete. □

(We thank B. Sambale for pointing out to us that a version of Theorem 2.2 appeared in [FG].)

In Theorem 2.2 we cannot replace 'solvable' with 'nilpotent'. This easily follows from the following:

Theorem 2.3. *Suppose that p is odd and G is a p-group. Let $\chi \in \mathrm{Irr}(G)$. Then $\mathbb{Q}(\chi) = \mathbb{Q}_{p^b}$ for some $b \geq 0$. Thus $\mathbb{Q}(\chi) = \mathbb{Q}_{c(\chi)}$.*

Proof. Let $a \geq 1$, and let $\mathbb{Q} \subseteq F \subseteq \mathbb{Q}_{p^a}$ be a subfield. We notice that $F = \mathbb{Q}_{p^b}$ for some $b \geq 1$ if and only if $\mathbb{Q}_p \subseteq F$. Indeed, we have that $\mathbb{Q}_{p^a}/\mathbb{Q}_p$ is a cyclic extension of degree p^{a-1}, which contains the subfields $\mathbb{Q}_p, \mathbb{Q}_{p^2}, \ldots, \mathbb{Q}_{p^a}$. Hence there are no subfields between $\mathbb{Q}_p$ and $\mathbb{Q}_{p^a}$ other than the fields of the form $\mathbb{Q}_{p^b}$ for $1 \leq b \leq a$.

In order to prove the theorem, we may assume that χ is faithful. If G is trivial, the theorem is clear. Let $Z = \mathbf{Z}(G)$ and let $z \in Z$ be of order p. Then $\chi|_{\langle z\rangle} = \chi(1)\lambda$ for some $\lambda \in \mathrm{Irr}(\langle z\rangle)$, and hence $\lambda(z) \in \mathbb{Q}(\chi)$. Thus $\mathbb{Q}_p \subseteq \mathbb{Q}(\chi)$, and we use the claim in the previous paragraph. □

Notice that the conclusion of Theorem 2.3 does not hold for 2-groups, and that D_{16} is a counterexample. The question of whether, given an irreducible character χ of a finite group G, there is always some $g \in G$ such that $\mathbb{Q}(\chi) = \mathbb{Q}(\chi(g))$, is interesting. Although this does not always happen, we have not found any example in which $\chi(1)$ is odd or χ is 2-rational. A different but related question that is sometimes asked is if any algebraic integer in $\mathbb{Q}_n$ is the value of an irreducible character of a finite group, and again this is true: let a and b be positive integers, and let G be the wreath product of C_a with C_b, where C_a is the cyclic group of order a. Then G has a faithful irreducible character of degree b whose values on the base group of the wreath product are all possible sums of b roots of unity, all of which have order dividing a.

Our next objective is to solve the following question: Which are exactly the fields of values of the irreducible characters of groups of odd order? It is an old theorem of Burnside that these cannot be real unless the character is trivial, but there is more. In order to answer this, we will need two general elementary lemmas that we use in the rest of the paper, and, at the end of the section, some nontrivial character theory of solvable groups.

Lemma 2.4. *Let G be a finite group and p be a prime, and set $P \in \mathrm{Syl}_p(G)$. Suppose that $\psi = \alpha\beta$, where α is a p-rational character of G of p'-degree and β is a linear character of G of order a power of p. Then $\mathbb{Q}(\psi_P) = \mathbb{Q}(\beta)$, $\mathbb{Q}(\psi) = \mathbb{Q}(\alpha, \beta)$ and $c(\psi) = c(\alpha)c(\beta)$.*

Proof. Set $x \in P$. Then $0 \neq \alpha(x) \in \mathbb{Q}$, using the facts that α has p'-degree, x is a p-element and α is p-rational (see [N2, Corollary 4.20].) Thus $\mathbb{Q}(\psi_P) = \mathbb{Q}(\beta_P)$. Since the order of β is a power of p, notice that $\mathbb{Q}(\beta) = \mathbb{Q}(\beta_P)$. We conclude that $\mathbb{Q}(\beta) \subseteq \mathbb{Q}(\psi_P) \subseteq \mathbb{Q}(\psi)$, and therefore $\mathbb{Q}(\psi) = \mathbb{Q}(\alpha, \beta)$. Now, since $c(\alpha)$ and $c(\beta)$ are coprime, we have that the conductor of the field $\mathbb{Q}(\alpha, \beta)$ is $c(\alpha)c(\beta)$, by elementary Galois theory. □

Lemma 2.5. *Let G be a finite group and suppose that $P \triangleleft G$, where $P \in \mathrm{Syl}_p(G)$. Set $\chi \in \mathrm{Irr}_{p'}(G)$ and let $\lambda \in \mathrm{Irr}(P)$ be a linear irreducible constituent of χ_P. Let $T = G_\lambda$ be the stabiliser of λ in G, let $\hat{\lambda} \in \mathrm{Irr}(T)$ be the unique extension of λ which has p-power order and let $\alpha \in \mathrm{Irr}(T/P)$ be such that $(\hat{\lambda}\alpha)^G = \chi$.*

(i) *We have that $\mathbb{Q}(\chi) \subseteq \mathbb{Q}_{o(\lambda)}(\alpha)$ and $\mathbb{Q}(\lambda)/\mathbb{Q}(\chi_P)$ has p'-degree. In particular, $c(\chi_P) = o(\lambda)$ unless $\lambda^p = 1$.*

(ii) *Let f be the conductor of χ. If $o(\lambda) > p$, then $f_p = o(\lambda)$. If $\lambda^p = 1$, then $f_p \leq p$.*
(iii) *If $p = 2$, then $\mathbb{Q}(\chi) = \mathbb{Q}_{o(\lambda)}(\alpha)$, $c(\chi) = c(\lambda)c(\alpha)$ and $\mathbb{Q}_{o(\lambda)} = \mathbb{Q}(\chi_P)$.*

Proof. Write $o(\lambda) = p^b$, with $b \geq 0$. We have that such $\hat{\lambda}$ exists and $o(\hat{\lambda}) = p^b$, by [N2, Corollary 6.4]. First notice that the Clifford correspondent of χ over λ can be written as $\hat{\lambda}\alpha$ by the Gallagher correspondence [Is2, Corollary 6.17]. Write $\psi = \hat{\lambda}\alpha$. By Lemmas 2.1 and 2.4, we have $\mathbb{Q}(\chi) \subseteq \mathbb{Q}(\psi) = \mathbb{Q}_{p^b}(\alpha)$. Now write $\chi_P = e\sum_{g\in G}\lambda^g$, and recall that $\mathbb{Q}(\chi_P) \subseteq \mathbb{Q}(\lambda)$ by Lemma 2.1(i). Now, if $\sigma \in \mathrm{Gal}(\mathbb{Q}(\lambda)/\mathbb{Q}(\chi_P))$ has p-power order, then λ^σ is an irreducible constituent of χ_P, and therefore $\lambda^\sigma = \lambda^g$ for some p'-element g. Since $o(\lambda)$ has p-power, we conclude that $\lambda^g = \lambda$ and σ is the identity. If $p = 2$, then $\mathbb{Q}_{2^b}/\mathbb{Q}$ has degree a power of 2, and we conclude that $\mathbb{Q}_{o(\lambda)} = \mathbb{Q}(\chi_P)$ (which is part of (iii)).

Suppose now that p^c is the conductor of χ_P. Then $\mathbb{Q}(\chi_P) \subseteq \mathbb{Q}_{p^c} \subseteq \mathbb{Q}_{p^b}$. Then $\mathbb{Q}_{p^b}/\mathbb{Q}_{p^c}$ has degree not divisible by p, and the proof of (i) easily follows.

Next we prove (ii). Write $f_p = p^a$, for some $a \geq 0$. Since $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}_{|T/P|}$, we have $\mathbb{Q}(\chi) \subseteq \mathbb{Q}_{p^b|T/P|}$, and therefore f divides $p^b|T/P|$. Hence $p^a \leq p^b$. Since $\mathbb{Q}(\chi_P) \subseteq \mathbb{Q}(\chi)$, we have that $c(\chi_P)$ divides f. Hence if $o(\lambda) > p$, we have $p^a = p^b$ by (i). The rest easily follows.

Finally, assume that $p = 2$. We know by (i) and (ii) that $\mathbb{Q}_{o(\lambda)} = \mathbb{Q}(\chi_P) \subseteq \mathbb{Q}(\chi) \subseteq \mathbb{Q}_{o(\lambda)}(\alpha)$. Thus if $\sigma \in \mathrm{Gal}(\mathbb{Q}_{o(\lambda)}(\alpha)/\mathbb{Q}(\chi)$, then it fixes χ and therefore χ_P. Hence σ fixes λ and $\hat{\lambda}$. By the uniqueness in the Clifford correspondence, σ also fixes α, so σ is the identity. For the last part, $\mathbb{Q}_{o(\lambda)}(\alpha) = \mathbb{Q}(\hat{\lambda}, \alpha)$, and we apply Lemma 2.4. □

We record the following useful fact:

Lemma 2.6. *Suppose that E/K is a finite field extension, and F and L are subfields of E such that $E = \langle F, L\rangle$ and $F \cap L = K$. Assume that F/K is Galois.*

(i) *If $K \subseteq J \subseteq L$ is a subfield and $M = \langle F, J\rangle$, then $M \cap L = J$.*
(ii) *If L/K is Galois and $F \subseteq M \subseteq E$ is any subfield, then $M = \langle F, M \cap L\rangle$.*

Proof. (i) Let $J' = M \cap L$. Then $J \subseteq J'$, and $J' \cap F = K$. By natural irrationalities [We, Corollary 3.4.5], $[M : J] = [F : K]$. Now $M = \langle F, J\rangle \subseteq \langle F, J'\rangle \subseteq M$. Thus $\langle F, J'\rangle = M$, and again by natural irrationalities, $[M : J'] = [F : J' \cap F] = [F : K] = [M : J]$. Since $J \subseteq J'$, the result follows.

(ii) Let $J = M \cap L$ and $M' = \langle F, J\rangle \subseteq M$. By (i) we have $M' \cap L = J$. Now $E = \langle M', L\rangle$ and L/J is Galois, so $[E : M'] = [L : J]$ by natural irrationalities. But we also have $E = \langle M, L\rangle$, which similarly implies $[E : M] = [L : J]$. Thus $[E : M] = [E : M']$. Since $M' \subseteq M$, we have $M = M'$. □

Now we are ready to describe the fields of values of irreducible characters of groups of odd order and the fields of values of the irreducible odd-degree characters of solvable groups. The next three results will not be used in the rest of the paper.

In the next theorem, we use *p-special* characters. We refer the reader to [Is3] for their main properties. We will use the fact that in a solvable group G, restriction defines an injection from the set $\mathcal{X}_p(G)$ of p-special characters of G into $\mathrm{Irr}(P)$, where P is a Sylow p-subgroup of G, and therefore that $\mathbb{Q}(\chi) = \mathbb{Q}(\chi_P)$. (Using the uniqueness of the restriction map, we easily prove that the group $\mathrm{Gal}(\mathbb{Q}(\chi)/\mathbb{Q}(\chi_P))$ is trivial, and hence the result.) In particular, $c(\chi) = c(\chi_P)$. Also, a quasi-primitive character χ of a solvable group is fully factorable – that is, it uniquely factors as a product $\prod_{p\in\mathbb{P}}\chi_p$, where $\mathbb{P}$ is the set of all prime numbers and χ_p is p-special (see [Is3, Theorem 2.17] and [Is2, Berger's Theorem 11.33]). In this case, $\mathbb{Q}(\chi) = \langle\mathbb{Q}(\chi_p) \mid p \in \mathbb{P}\rangle$ (by [Is3, Lemma 2.19]).

Theorem 2.7. *Let $F/\mathbb{Q}$ be an abelian extension and assume that the conductor n of F is odd. Then there exist a group of odd order G and $\chi \in \mathrm{Irr}(G)$ such that $\mathbb{Q}(\chi) = F$ if and only if the extension $\mathbb{Q}_n/F$ has odd degree.*

Proof. If $n = c(F)$ is odd and $\mathbb{Q}_n/F$ has odd degree, then Theorem 2.2 produces a solvable group G of odd order, with a character $\chi \in \mathrm{Irr}(G)$ such that $\mathbb{Q}(\chi) = F$.

Conversely, suppose that $\chi \in \mathrm{Irr}(G)$, where G has odd order. We argue by induction on $|G|$ that $\mathbb{Q}_{c(\chi)}/\mathbb{Q}(\chi)$ has odd degree. Suppose that $\psi^G = \chi$, where $\psi \in \mathrm{Irr}(T)$ is some Clifford correspondent and T is the stabiliser of some normal irreducible constituent. Notice that $[\mathbb{Q}(\psi) : \mathbb{Q}(\chi)]$ is odd by Lemma 2.1(ii). If $T < G$, then by induction, $\mathbb{Q}_{c(\psi)}/\mathbb{Q}(\psi)$ has odd degree, and we conclude that $\mathbb{Q}_{c(\psi)}/\mathbb{Q}(\chi)$ has odd degree. Thus $\mathbb{Q}_{c(\chi)}/\mathbb{Q}(\chi)$ has odd degree using Lemma 2.1(i). Hence, we may assume that χ is quasi-primitive, and therefore χ is fully factorable. Then, using Theorem 2.3, we have

$$\mathbb{Q}(\chi) = \langle \mathbb{Q}(\chi_p) \mid p \in \mathbb{P} \rangle = \langle \mathbb{Q}((\chi_p)|_P) \mid p \in \mathbb{P} \rangle = \langle \mathbb{Q}_{c(\chi_p)} \mid p \in \mathbb{P} \rangle = \mathbb{Q}_{c(\chi)},$$

by elementary Galois theory, and the result follows. □

Using Theorem 2.7 (and the main result of [Is1]), we can fully characterise the extensions $\mathbb{Q}(\chi)/\mathbb{Q}$ whenever $\chi \in \mathrm{Irr}_{2'}(G)$ and G is solvable:

Theorem 2.8. *Let $F/\mathbb{Q}$ be an abelian extension and suppose that $c(F) = n$. Then there exist a finite solvable group G and a character $\chi \in \mathrm{Irr}(G)$ of odd degree such that $\mathbb{Q}(\chi) = F$ if and only if $\mathbb{Q}_n/F$ has odd degree.*

Proof. If $\mathbb{Q}_n/F$ has odd degree, then Theorem 2.2 produces a solvable group with the desired conclusion. Suppose now that G is solvable, $\chi \in \mathrm{Irr}_{2'}(G)$ and $\mathbb{Q}(\chi) = F$. Write $n = 2^a m$, where m is odd and $a \geq 0$. We want to show that $\mathbb{Q}_n/F$ has odd degree. By the main result of [Is1], if $P \in \mathrm{Syl}_2(G)$, then there is a natural correspondence ${}^* : \mathrm{Irr}_{2'}(G) \longrightarrow \mathrm{Irr}_{2'}(\mathbf{N}_G(P))$ that commutes with Galois action (as can be checked). Thus $\mathbb{Q}(\chi) = \mathbb{Q}(\chi^*) = F$, and we may assume that $P \triangleleft G$. By Lemma 2.5(iii), we have $\mathbb{Q}(\chi) = \mathbb{Q}_{2^b}(\alpha)$, where α is an irreducible character of a group of odd order, $b \geq 0$ and $2^b = o(\lambda)$, where $\lambda \in \mathrm{Irr}(P)$ lies below χ. Also, $c(\chi) = c(\lambda)c(\alpha) = 2^a m$, and thus $c(\alpha) = m$. Also, $a = 0$ if $o(\lambda) = 2$ and $a = b$ if $a \geq 2$. In any case, $\mathbb{Q}_{2^a} = \mathbb{Q}_{2^b}$. Notice that $\mathbb{Q}_{2^b}(\alpha) \cap \mathbb{Q}_m = \mathbb{Q}(\alpha)$, by Lemma 2.6. We have that $\mathbb{Q}_n/F$ and $\mathbb{Q}_m/\mathbb{Q}_{c(\alpha)}$ have the same degree by natural irrationalities, and the proof of the theorem is complete by Theorem 2.7. □

Corollary 2.9. *Let G be a finite solvable group, set $\chi \in \mathrm{Irr}_{2'}(G)$ and let $d \neq \pm 1$ be a square-free integer. Assume that $\mathbb{Q}(\chi) = \mathbb{Q}(\sqrt{d})$. Then $d = -p$, and $p \equiv 3 \pmod 4$ is a prime.*

Proof. Write n for the conductor of the field $\mathbb{Q}(\sqrt{d})$. It is well known that $n = |d|$ if $d \equiv 1 \pmod 4$, and $n = 4|d|$ otherwise. By Theorem 2.8, we have that $\varphi(n)/2$ is odd, where φ is the Euler function. Hence we deduce that $n = |d|$ and $d \equiv 1 \pmod 4$, and hence n is odd. As n is square free, we can write $n = p_1 \cdots p_k$, where $2 < p_1 < p_2 < \cdots < p_k$ are prime. Since $4 \nmid \varphi(n)$, we must have $k = 1$, and $n = p \equiv 3 \pmod 4$ is a prime. Thus $d = -p$. □

Using quadratic Gauss sums, it is easy to prove that if p is a prime $p \equiv 3 \pmod 4$, then the semidirect product of C_p with $C_{\frac{p-1}{2}}$ is a group of odd order with an irreducible character χ of (odd) degree $\frac{p-1}{2}$ whose field of values is $\mathbb{Q}(\sqrt{-p})$.

3. Proofs of Theorems A2 and B2

We begin with a simple observation.

Lemma 3.1. *Let G be a finite group, set $\chi \in \mathrm{Irr}(G)$ and let $\mathbb{F} := \mathbb{Q}(\chi)$. Let A be a subgroup of $\mathrm{Gal}(\mathbb{F}/\mathbb{Q})$ and let $\rho := \sum_{\alpha \in A} \chi^\alpha$. Then $\mathbb{Q}(\rho) = \mathbb{F}^A$ is the fixed field by A.*

Proof. Recall that $\mathbb{F}/\mathbb{Q}$ is a finite abelian Galois extension. Clearly, $\mathbb{Q}(\rho) \subseteq \mathbb{Q}(\chi) = \mathbb{F}$ and $\rho^\gamma = \sum_{\alpha \in A} \chi^{\alpha\gamma} = \sum_{\alpha \in A} \chi^\alpha = \rho$ for all $\gamma \in A$, and so $\mathbb{Q}(\rho) \subseteq \mathbb{F}^A$. Conversely, suppose that $\rho^\beta = \rho$ for some $\beta \in \mathrm{Gal}(\mathbb{F}/\mathbb{Q})$. Then

$$\sum_{\alpha \in A} \chi^{\alpha\beta} = \rho^\beta = \rho = \sum_{\alpha \in A} \chi^\alpha.$$

Since each χ^α is an irreducible character, it follows that $\chi^\beta = \chi^\alpha$ for some $\alpha \in A$, and so $\chi^{\beta\alpha^{-1}} = \chi$ and χ is $\beta\alpha^{-1}$-fixed. As $\mathbb{Q}(\chi) = \mathbb{F}$, we see that $\beta\alpha^{-1}$ acts trivially on $\mathbb{F}$, whence $\beta = \alpha \in A$. Thus the Galois automorphisms of $\mathbb{F} \supseteq \mathbb{Q}(\rho)$ are precisely the elements in A, and we conclude that $\mathbb{Q}(\rho) = \mathbb{F}^A$. □

The next two theorems provide the key group-theoretic constructions to realise various abelian extensions of $\mathbb{Q}$.

Theorem 3.2. *Let p be any prime, $N \in \mathbb{Z}_{\geq 1}$ be coprime to p, $\zeta \in \mathbb{C}$ be a primitive Nth root of unity and $\mathbb{F}$ be any subfield of $\mathbb{Q}(\zeta)$. Then there exist a finite group G and an irreducible character χ of G of p'-degree with $\mathbb{Q}(\chi) = \mathbb{F}$.*

Proof. Let $A \leq \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ be such that $\mathbb{F} = \mathbb{Q}(\zeta)^A$ by Galois correspondence, and set $n = |A| = [\mathbb{Q}(\zeta) : \mathbb{F}]$. Write

$$A = \left\{\sigma_{k_i} : \zeta \mapsto \zeta^{k_i} \mid k_i \in (\mathbb{Z}/N\mathbb{Z})^\times,\ 1 \leq i \leq n\right\}.$$

As $p \nmid N$, we can find a smallest $m \in \mathbb{Z}_{\geq 1}$ such that $N | (p^m - 1)$. Now let $q := p^m$ and $G := \mathrm{GL}_n(q)$. Then we can identify the Langlands dual group G^* with G. Let $\varepsilon \in \mathbb{F}_q^\times$ be of order N. Consider the semisimple element

$$s := \mathrm{diag}(\varepsilon^{k_1}, \varepsilon^{k_2}, \ldots, \varepsilon^{k_n}) \in G^* \tag{3.1}$$

and $\chi = \chi_s$ the semisimple character of G labelled by s, of degree $|G : \mathbf{C}_G(s)|_{p'}$ (compare [C, §8.4]). We may assume that $k_1 = 1$ (so that σ_{k_1} is the trivial automorphism). Since $|s| = |\varepsilon| = N$, the proof of [NT1, Lemma 9.1] shows that

$$\mathbb{Q}(\chi) \subseteq \mathbb{Q}(\zeta). \tag{3.2}$$

Furthermore, for any element $\sigma_t : \zeta \mapsto \zeta^t$ in $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$, the same proof shows that $\chi^{\sigma_t} = \chi_{s^t}$, the semisimple character of G labelled by s^t. In particular, if χ is σ_t-fixed, then s^t is conjugate to s in G^*. In this case, the eigenvalue ε^t of s^t (acting on $\mathbb{F}_q^n$) is also an eigenvalue of s, whence $\varepsilon^t = \varepsilon^{k_i}$ for some $1 \leq i \leq n$ by formula (3.1), and so

$$\sigma_t(\zeta) = \zeta^t = \zeta^{k_i} = \sigma_{k_i}(\zeta)$$

(that is, $\sigma_t = \sigma_{k_i} \in A$). Conversely, as A is a subgroup, for any $\sigma_t \in A$ the set $\{k_1, k_2, \ldots, k_n\}$ of n pairwise distinct elements in $(\mathbb{Z}/N\mathbb{Z})^\times$ is stable under multiplication by t. Hence definition (3.1) of s ensures that s^t is conjugate to s in G^*, whence $\chi^{\sigma_t} = \chi_{s^t} = \chi$ and χ is σ_t-fixed.

We have shown that the Galois automorphisms of $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ that stabilise χ are precisely the elements of A. By Galois correspondence, this implies that $\mathbb{Q}(\chi) = \mathbb{Q}(\zeta)^A = \mathbb{F}$, as desired. □

Theorem 3.3. *Let $\mathbb{F}$ be a finite abelian extension of $\mathbb{Q}$ and suppose that $\mathbb{F} = \mathbb{Q}(\alpha)$ for some irreducible character α of a finite group H. Then for any subfield $\mathbb{E}$ of $\mathbb{F}$ with $\mathbb{F}/\mathbb{E}$ a cyclic extension of degree d, there exist a finite group G and an irreducible character χ of G of degree $d\alpha(1)^d$ with $\mathbb{Q}(\chi) = \mathbb{E}$.*

Proof. View $\mathbb{E}$ as the fixed field $\mathbb{F}^A$ for a subgroup $A = \langle a \rangle \leq \mathrm{Gal}(\mathbb{F}/\mathbb{Q})$ of order d. Now we take G to be the wreath product $G = H \wr A = H^d \rtimes A$, where

$$H^d = \{(x_1, x_2, \ldots, x_d) \mid x_i \in H\}$$

is a direct product of $d = |A|$ copies of H. Furthermore, conjugation by any $b \in A$ cyclically permutes the d entries $x_1, \ldots, x_d$ of any element $x = (x_1, x_2, \ldots, x_d) \in H^d$, sending x to $(x_d, x_1, x_2, \ldots, x_{d-1})$. Consider the irreducible character

$$\theta = \alpha^a \times \alpha^{a^2} \times \cdots \times \alpha^{a^d}$$

of H^d, so that

$$\theta((x_1, x_2, \ldots, x_d)) = \prod_{i=1}^{d} \alpha^{a^i}(x_i). \tag{3.3}$$

The arguments in the proof of Lemma 3.1 show that the d irreducible characters α^{a^i}, $1 \leq i \leq d$, are pairwise distinct. The described action of A on H^d now implies that the stabiliser $I_G(\theta) = H^d$. (Indeed, any $1 \neq a^j \in A$ sends θ to an outer tensor product, with the first factor now being $\alpha^{a^{j+1}} \neq \alpha^a$, whence $\theta^{a^j} \neq \theta$.)

By Clifford's theorem, $\chi := \theta^G$ is irreducible, of degree $d\alpha(1)^d$. Note that χ vanishes outside of H^d. Next, any A-conjugate θ^b with $b \in A$ takes values in $\mathbb{Q}(\alpha) = \mathbb{F}$, whence $\mathbb{Q}(\chi) \subseteq \mathbb{F}$. Moreover, the described A-action on H^d and equation (3.3) show that for any element $x = (x_1, \ldots, x_d) \in H^d$,

$$\theta(x^a) = \theta((x_d, x_1, x_2, \ldots, x_{d-1})) = \alpha^a(x_d)\alpha^{a^2}(x_1)\alpha^{a^3}(x_2)\cdots\alpha^{a^d}(x_{d-1}) = (\theta(x))^a,$$

whence $\theta(x^{a^i}) = (\theta(x))^{a^i}$ for all $1 \leq i \leq d$. Thus $\chi(x) = \sum_{i=1}^d \theta(x^{a^i}) = \sum_{i=1}^d (\theta(x))^{a^i}$ is a-fixed, and so $\mathbb{Q}(\chi) \subseteq \mathbb{F}^A = \mathbb{E}$.

Now taking $y = (z, 1, 1, \ldots, 1) \in H^d$ for any $z \in H$, we have $\chi(y) = \alpha(1)^{d-1}\rho(z)$, with $\rho := \sum_{i=1}^d \alpha^{a^i}$. In particular, $\mathbb{Q}(\chi) \supseteq \mathbb{Q}(\rho)$. By Lemma 3.1, $\mathbb{Q}(\rho) = \mathbb{F}^A = \mathbb{E}$. Consequently, $\mathbb{Q}(\chi) = \mathbb{E}$. □

We note that an inductive argument allows one to remove the cyclic assumption in Theorem 3.3. Now we are ready to prove Theorems A2 and B2.

Proofs of Theorems A2 and B2 Define $E := \mathbb{Q}_{p^a m}$ and $F := \mathbb{Q}_{p^a}$ (with $p = 2$ in Theorem A2), and let $M \subseteq E$ be any subfield such that $p \nmid [F : M \cap F]$ – equivalently, M contains the unique subfield $\mathbb{E}_{p^{a-1}}$ of F that has degree p^{a-1} over $\mathbb{Q}$. Then the subfield $\tilde{M} := \langle M, \mathbb{Q}_p \rangle$ of E contains $\langle \mathbb{E}_{p^{a-1}}, \mathbb{Q}_p \rangle = F$.

First we show how to attain $\tilde{M}$ as the value field of some p'-degree character. Note that $E := \langle F, L \rangle$ for $L := \mathbb{Q}_m$, and $F \cap L = \mathbb{Q}$ because $p \nmid m$. By Lemma 2.6(ii), $\tilde{M} = \langle F, J \rangle = J(\zeta)$, where $J := \tilde{M} \cap L$ and $\zeta = \exp(2\pi i/p^a)$. Applying Theorem 3.2, we can find a finite group H and an irreducible character $\theta \in \mathrm{Irr}(H)$ of p'-degree such that $\mathbb{Q}(\theta) = J$. Now we consider $\tilde{H} = C_{p^a} \times H$ and the irreducible character $\tilde{\theta} = \lambda \times \theta$ of $\tilde{H}$, where $\lambda \in \mathrm{Irr}(C_{p^a})$ is faithful. Then $\tilde{\theta}(1) = \theta(1)$ is coprime to p, and $\mathbb{Q}(\tilde{\theta}) = J(\zeta) = \tilde{M}$.

Now, if $p = 2$, then $\mathbb{Q}_2 = \mathbb{Q}$ and $\tilde{M} = M$, and so we have completed the proof of Theorem A2. Assume $p > 2$. Then $F \cap \tilde{M} \supseteq \mathbb{E}_{p^a}$ (where $\mathbb{E}_{p^a}$ is the only extension of $\mathbb{Q}_{p^{a+1}}$ of degree p^a over the rationals), and so $F/(F \cap \tilde{M})$ is a cyclic Galois extension, of degree $d|(p-1)$. As $\tilde{M} = \langle M, F \rangle$, by [We, Theorem 3.4.3] we have that $\tilde{M}/M$ is a cyclic Galois extension of the same degree d. Applying Theorem 3.3, we obtain a finite group $G = \tilde{H} \wr C_d$ and an irreducible character $\chi \in \mathrm{Irr}(G)$ of degree $d\theta(1)^d$ with $\mathbb{Q}(\chi) = M$. □

4. Proofs of Theorems A1 and B1

As we have seen in the previous sections, it is not completely trivial to work with conductors of fields of values. Although our results are on conductors, it is convenient to express them, and to work, using certain Galois automorphisms which are fundamental when studying values of characters. We shall see that these are the automorphisms that control the prime powers dividing the conductor of a character. As usual, let us fix a prime p for the rest of the section. If $e \geq 1$ is an integer, then we let $\sigma_e \in \mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q})$ be the automorphism that fixes roots of unity of order not divisible by p and sends any p-power root of unity ξ to ξ^{1+p^e}. Hence, a p-power root of unity ξ is fixed by σ_e if and only if its order $o(\xi)$ divides p^e. Thus $\mathbb{Q}_{p^e}$ is contained in the fixed field of σ_e. If p is odd, in this paper we will denote by $\mathbb{E}_{p^e}$ the unique subfield $\mathbb{E}$ with $[\mathbb{E} : \mathbb{Q}] = p^e$ in the cyclotomic field $\mathbb{Q}_{p^{e+1}}$, whenever $e \geq 1$.

In this section we prove Theorem A1 (assuming a weaker version of Theorem A3 – Theorem 5.1 – whose proof is deferred until Section 5), and Theorem B1. We begin with the following elementary result:

Lemma 4.1. *Let p be a prime and let $e \geq 1$ be an integer. If $p = 2$, assume that $e \geq 2$.*

(i) *If $f \geq e$, then the restriction τ_f of σ_e to $\mathbb{Q}_{p^f}$ has order p^{f-e} and generates $\mathrm{Gal}(\mathbb{Q}_{p^f}/\mathbb{Q}_{p^e})$. In particular, if $n = p^f m \geq 1$ is an integer, with m not divisible by p, then the restriction of σ_e to $\mathbb{Q}_n$ is the identity if $f \leq e$, and has order p^{f-e} and fixed field $\mathbb{Q}_{p^e m}$ if $f \geq e$.*

(ii) *Let $\chi \in \mathrm{Irr}(G)$, where G is a finite group. If χ is σ_e-invariant, then χ is σ_{e+1}-invariant.*

(iii) *Set $\chi \in \mathrm{Irr}(G)$, where G is a finite group, and let c be the conductor of χ. Let p be a prime and write $c = p^a m$, where m is not divisible by p and $a \geq 1$. If $p > 2$, then a is the smallest positive integer e such that χ is σ_e-invariant. If $p = 2$, then a is the smallest integer $e \geq 2$ such that χ is σ_e-invariant.*

Proof. If $m \in \mathbb{Z}$ is congruent to 1 mod p^e but not to 1 mod p^{e+1}, using the binomial theorem we easily have that m^p is congruent to 1 mod p^{e+1} but not to 1 mod p^{e+2}. Therefore, for every $s \geq 1$, we have that m^{p^s} is congruent to 1 mod p^{e+s} but not to 1 mod p^{e+s+1}. Hence, if $f \geq e$ we have that the restriction τ_f of σ_e to $\mathbb{Q}_{p^f}$ has order p^{f-e}. In particular, τ_f is a generator of $\mathrm{Gal}(\mathbb{Q}_{p^f}/\mathbb{Q}_{p^e})$. This proves the first part of (i). If n is any integer, then write $n = p^f m$, where m is not divisible by p and $f \geq 0$. Let τ now be the restriction of σ_e to $\mathbb{Q}_n$. We have $\tau \in \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}_m)$. If $f < e$, then τ is the identity. Otherwise, τ has order p^{f-e}. This easily concludes the proof of (i).

We prove (ii). Suppose that $\chi \in \mathrm{Irr}(G)$ is σ_e-invariant, and set $d \geq e$. We want to show that χ is σ_d-invariant. We may assume that $\mathbb{Q}(\chi) \subseteq \mathbb{Q}_n$, where $p^f := n_p \geq p^e$. Notice that the restriction γ of σ_d to $\mathbb{Q}_{p^f}$ fixes the p^e-roots of unity, and therefore $\gamma \in \langle \tau_f \rangle$, where τ_f is as in the previous paragraph. Let γ_0 be the restriction of σ_d to $\mathbb{Q}_{p^f m}$, and let τ_0 be the restriction of σ_e to $\mathbb{Q}_{p^f m}$. Using the notation in the previous paragraph, we have $\gamma_0 \in \langle \tau_0 \rangle$, since γ is a power of τ_f and both fix p'-roots of unity. Now, since χ is τ_0-invariant, it is also γ_0-invariant. This proves (ii).

To prove (iii), notice that σ_a fixes $\mathbb{Q}_{p^a}$ and $\mathbb{Q}_m$, and therefore χ is σ_a-fixed. Assume that χ is σ_e-fixed for some $1 \leq e < a$, and furthermore, $e \geq 2$ if $p = 2$. By (i), we have that the fixed field of the restriction of σ_e to $\mathbb{Q}_c$ is exactly $\mathbb{Q}_{p^e m}$. Hence $\mathbb{Q}(\chi) \subseteq \mathbb{Q}_{p^e m}$, which contradicts the definition of the conductor c. □

Notice therefore that we can reformulate Theorems A1 and A3 and Conjecture B3 in terms of the Galois action of the automorphisms σ_e, using Lemma 4.1.

Lemma 4.2. *Let G be a finite group and N be a normal subgroup of G. Suppose that G/N has order not divisible by p. Set $\chi \in \mathrm{Irr}(G)$ and let $\theta \in \mathrm{Irr}(N)$ be an irreducible constituent of χ_N.*

(i) *Suppose that $e \geq 1$. Then χ is σ_e-fixed if and only if θ is σ_e-fixed.*

(ii) *Suppose that p^a is the p-part of the conductor of χ and that p^b is the p-part of the conductor of θ. If $a, b \geq 1$ or $p = 2$, then $a = b$.*

Proof. Let τ be the restriction of σ_e to $\mathbb{Q}_{|G|}$. Then τ has order a power of p, by Lemma 4.1(i). We have that χ (or θ) is σ_e-invariant if and only if it is τ-invariant.

If θ is τ-invariant, then χ is τ-invariant, by [NT4, Lemma 5.1]. If χ is τ-invariant, then θ is τ-invariant by Lemma 2.1. This proves (i).

If $p = 2$, we claim that θ is 2-rational if and only if χ is 2-rational. Indeed, suppose that χ is 2-rational. Write $|G| = 2^f m$, where m is odd, and set $\sigma \in \mathrm{Gal}(\mathbb{Q}_{|G|}/\mathbb{Q}_m)$. Then σ has 2-power order and therefore $\theta^\sigma = \theta$ by Lemma 2.1. If θ is 2-rational, then χ is 2-rational by [ILNT, Lemma 2.1]. Hence, if $p = 2$, we may assume that $a, b \geq 2$. Now (ii) follows easily from (i) and Lemma 4.1(iii). □

We remark that in Lemma 4.2(ii), we need $a, b \geq 1$, even if the characters have degree not divisible by p. For instance, if $a = 0$, then b can be 1, as shown by S_3 with $p = 3$, and $N = \mathsf{A}_3$. If $b = 0$, a can be 1, as shown by `SmallGroup`(24, 4) [GAP], again with $p = 3$.

Lemma 4.3. *Suppose that G is a finite group and $N \lhd G$. Let $\lambda, \theta \in \mathrm{Irr}(N)$ be G-invariant, and assume that $\lambda\theta$ is irreducible and extends to G. If θ extends to G, then λ extends to G.*

Proof. This is [ILNT, Lemma 2.2]. □

Lemma 4.4. *Let p be a prime. Suppose that G is a finite group and $N \lhd G$. Let $\lambda, \theta \in \mathrm{Irr}(N)$ be G-invariant, and assume that λ is linear and $\lambda\theta$ extends to G. Suppose that $\chi \in \mathrm{Irr}(G)$ has p'-degree and lies over $\theta \in \mathrm{Irr}(N)$. Let $\tau \in \mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q})$ fix p'-roots of unity.*

(i) *If $\mu = \lambda_{p'}$, then $\mu\theta$ extends to a character $\psi \in \mathrm{Irr}(G)$. Also, we can write $\chi = \psi\xi$, where $\xi \in \mathrm{Irr}(G|\mu^{-1})$.*
(ii) *If G/N is perfect and θ is τ-invariant, then ψ is τ-invariant.*

Proof. Part (i) is [ILNT, Lemma 2.3(i)].

(ii) By hypothesis, θ is τ-invariant, and since $\mu = \lambda_{p'}$ is also τ-invariant, we see that $\varphi = \mu\theta$ is τ-invariant. We are assuming that G/N is perfect, so by Gallagher's theorem [Is2, Corollary 6.17] we deduce that ψ is the unique extension of φ to G. The Galois group $\mathrm{Gal}(\mathbb{Q}(\psi)/\mathbb{Q}(\varphi))$ thus fixes ψ, so the Galois group is trivial, and thus $\mathbb{Q}(\psi) = \mathbb{Q}(\varphi)$. We conclude that ψ is τ-fixed, as required. □

The next result is standard.

Theorem 4.5. *Set $N \lhd G$, where G is a finite group, and let $\theta \in \mathrm{Irr}(N)$ be G-invariant. Then there is a finite group H and a surjective homomorphism $\pi : H \longrightarrow G$ such that $Z = \ker(\pi) \subseteq \mathbf{Z}(H)$. Furthermore, if $K = \pi^{-1}(N)$ and $\widehat{\theta} \in \mathrm{Irr}(K/Z)$ corresponds to θ via the induced isomorphism $K/Z \longrightarrow N$, then $\widehat{\theta}$ is H-invariant and there is a linear H-invariant character $\lambda \in \mathrm{Irr}(K)$ such that $\lambda\widehat{\theta}$ extends to H.*

Proof. This is the content, for instance, of [N2, Theorem 5.6]. □

The following is a suitable modification of [ILNT, Theorem 2.6] for our present situation:

Theorem 4.6. *Let p be a prime and G a finite group, set $N \lhd G$ and let $\theta \in \mathrm{Irr}_{p'}(N)$ be G-invariant and σ_e-fixed. Suppose that G/N is a nonabelian simple group, and let $\chi \in \mathrm{Irr}(G|\theta)$ have p'-degree. Suppose that χ is not σ_e-fixed.*

(a) *If p is odd and Conjecture B3 holds, then there exists a p-element $x \in G$ such that $\mathbb{E}_{p^e} \subseteq \mathbb{Q}(\chi(x))$.*
(b) *Assume that $p = 2$, $e \geq 2$, $P \in \mathrm{Syl}_2(G)$ and $\mathbb{Q}_{2^e} \subseteq \mathbb{Q}(\chi_P)$. Then $\mathbb{Q}(\chi_P) = \mathbb{Q}_{2^a}$ for some $a \geq e+1$.*

Proof. (i) By Theorem 4.5, there is a finite group H with a central subgroup Z such that $H/Z = G$ (where we identify G with H/Z). Furthermore, if $K/Z = N$, then there is a linear H-invariant character $\lambda \in \mathrm{Irr}(K)$ such that $\lambda\theta$ extends to H, and θ is H-invariant. Notice that now we view θ as an irreducible character of K with Z in its kernel. Also, $\chi \in \mathrm{Irr}(H)$ contains Z in its kernel. By Lemma 4.4, if $\mu = \lambda_{p'}$, we know that $\mu\theta$ extends to a σ_e-invariant character $\psi \in \mathrm{Irr}(H)$. Furthermore, we can write $\chi = \psi\xi$ for some character $\xi \in \mathrm{Irr}(H|\mu^{-1})$. Notice that ξ and ψ have p'-degree, since $\chi(1)$ is p'. Also, ξ is not σ_e-invariant, since ψ is σ_e-invariant and χ is not.

Write $L = \ker(\mu^{-1})$, so K/L is a central p'-subgroup of H/L, because μ^{-1} is invariant in H and has p'-order. Let W/L be the final term of the derived series of H/L, so W/L is perfect. Now $KW = H$, because H/K is a nonabelian simple group, and since $W/(K \cap W) \cong H/K$ is simple and $(K \cap W)/L$ is central in W/L, we see that W/L is quasi-simple.

Now ξ_W is irreducible, because $KW = H$ and K/L is central in W/L. Also, $|H : W| = |K : (K \cap W)|$, which divides $|K : L|$, so $|H : W|$ is p'. It follows that ξ_W is not σ_e-invariant, because otherwise ξ would be σ_e-invariant by Lemma 4.2, which is not the case.

(ii) Suppose first that p is odd and that Conjecture B3 holds. By Conjecture B3 applied to the character ξ_W of W/L, we deduce that there exists an element $w \in W$ such that w has p-power order modulo L, and $\mathbb{E}_{p^e} \subseteq \mathbb{Q}(\xi(w))$. Also, observe that we can assume that w has p-power order p^f. Since $\mathbb{E}_{p^e} \subseteq \mathbb{Q}(\xi(w))$, we have $f \geq e+1$. Now $\chi(w) = \psi(w)\xi(w)$, and $\psi(w) \in \mathbb{Q}_{p^e}$ because w has p-power order and ψ is σ_e-invariant. Furthermore, $\psi(w) \neq 0$ by [N2, Lemma 4.19(ii)], because w is a p-element and $\psi(1)$ is p'.

Since $\mathbb{Q}(\chi(w)) \subseteq \mathbb{Q}_{p^f}$, we can write $[\mathbb{Q}(\chi(w)) : \mathbb{Q}] = p^a t$, where t divides $p-1$ and $a \leq f$. Suppose that p^e divides $[\mathbb{Q}(\chi(w)) : \mathbb{Q}]$. Then $\mathbb{E}_{p^e} \subseteq \mathbb{Q}(\chi(w))$, because $\mathbb{E}_{p^e}$ is the only extension of $\mathbb{Q}$

inside $\mathbb{Q}_{p^f}$ that has degree p^e (using the fact that $\mathbb{Q}_{p^f}/\mathbb{Q}$ is cyclic). Hence we may assume that p^e does not divide $[\mathbb{Q}(\chi(w)) : \mathbb{Q}]$, and thus $a < e$. Then $[\mathbb{Q}(\chi(w)) : \mathbb{Q}]$ divides $p^{e-1}(p-1)$, and therefore $\mathbb{Q}(\chi(w)) \subseteq \mathbb{Q}_{p^e}$, because $\mathbb{Q}_{p^e}$ is the unique extension of its degree inside $\mathbb{Q}_{p^f}$ (again using the fact that $\mathbb{Q}_{p^f}/\mathbb{Q}$) is cyclic). Then $\xi(w) = \chi(w)/\psi(w) \in \mathbb{Q}_{p^e}$, but this is a contradiction, since $\mathbb{E}_{p^e} \subseteq \mathbb{Q}(\xi(w))$.

(iii) Assume now that $p = 2$ and $e \geq 2$. Since ξ_W is not σ_e-invariant, by Theorem 5.1 we can find a 2-element $w \in W$ such that $\xi(w) \notin \mathbb{L} := \mathbb{Q}_{2^e}$. In particular, the order of w is 2^f for some $f > e$. Next, $\chi(w) = \psi(w)\xi(w)$, and $\psi(w) \in \mathbb{L}$ because w has 2-power order and ψ is σ_e-invariant (using Lemma 4.1). Furthermore, $\psi(w) \neq 0$ by [N2, Lemma 4.19(ii)], because w is a 2-element and $2 \nmid \psi(1)$. It follows that $\chi(w) \notin \mathbb{L}$.

We may assume that $w \in P$. Since $\mathbb{L} \subseteq \mathbb{Q}(\chi_P)$ by hypothesis, we have

$$\mathbb{Q}(\chi_P) = \mathbb{L}(\chi_P) \supseteq \mathbb{L}(\chi(w)).$$

Defining $b := \exp(P)$, we certainly have $b \geq f > e$. Now $\mathbb{Q}(\chi_P)$ contains $\mathbb{L}$ properly and is contained in $\mathbb{Q}_{2^b}$. As $e \geq 2$, we also note that $\mathbb{Q}_{2^b}/\mathbb{Q}_{2^e}$ is a cyclic extension of degree 2^{b-e}, with all intermediate fields being $\mathbb{Q}_{2^c}$ with $e \leq c \leq b$. It follows that $\mathbb{Q}(\chi_P) = \mathbb{Q}_{2^a}$ for some $a > e$, as desired. □

The following contains Theorems A1 and B1 (by applying Lemma 4.1). Again, we use some of the ideas in [ILNT].

Theorem 4.7. *Let p be a prime and G a finite group, set $\chi \in \mathrm{Irr}_{p'}(G)$ and let $e \in \mathbb{Z}_{\geq 1}$.*

(i) *Assume that p is odd and that Conjecture B3 holds for all quasi-simple groups S such that $S/\mathbf{Z}(S)$ is involved in G. Then either χ is σ_e-invariant or $\mathbb{E}_{p^e} \subseteq \mathbb{Q}(\chi)$.*

(ii) *Suppose that $p = 2$. Then either χ is σ_e-invariant or $\mathbb{Q}_{2^{e+1}} \subseteq \mathbb{Q}(\chi)$.*

Proof. If p is odd, let $\mathbb{K} = \mathbb{E}_{p^e}$, and if $p = 2$, let $\mathbb{K} = \mathbb{Q}_{2^{e+1}}$. In both cases, we have $|\mathbb{K} : \mathbb{Q}| = p^e$. We assume that χ is not σ_e-invariant and we prove that $\mathbb{K} \subseteq \mathbb{Q}(\chi)$. If p is odd, then we argue by induction on $|G|$. If $p = 2$, then we argue by induction on $|G| + e$. Write $\tau = \sigma_e$.

First we claim that if $p = 2$, then we may assume that $e \geq 2$ and that $\mathbb{Q}_{2^e} \subseteq \mathbb{Q}(\chi)$. Indeed, if $e = 1$ or $e = 2$, since χ is not σ_e-invariant, then χ is not 2-rational. Therefore $\mathbb{Q}(\chi) \supseteq \mathbb{Q}(i) = \mathbb{Q}_{2^2}$ by [ILNT, Theorem C], and the claim is proved. If $e \geq 3$, then χ is not σ_{e-1}-invariant by Lemma 4.1, and therefore $\mathbb{Q}(\chi) \supseteq \mathbb{Q}_{2^e}$ by induction. This proves the claim.

Let N be a normal subgroup of G. Let θ be an irreducible constituent of χ_N and let T be the stabiliser of θ in G. Also, let $\psi \in \mathrm{Irr}(T)$ be the Clifford correspondent of χ over θ, so $\psi^G = \chi$. Since $\mathbb{Q}(\chi) \subseteq \mathbb{Q}(\psi)$ (by Lemma 2.1(i)), we know that ψ is not τ-fixed. Notice that $|G : T|$ is not divisible by p, because χ has p'-degree. We claim that $[\mathbb{Q}(\psi) : \mathbb{Q}(\chi)]$ is not divisible by p. Otherwise, let $\sigma \in \mathrm{Gal}(\mathbb{Q}(\psi)/\mathbb{Q}(\chi))$ have order p. Then $\chi^\sigma = \chi$. Since $\mathbf{N}_G(T)/T$ has order not divisible by p, we have $\sigma = 1$ by Lemma 2.1(ii). This is a contradiction, and so $[\mathbb{Q}(\psi) : \mathbb{Q}(\chi)]$ is not divisible by p, as claimed.

Assume that $T < G$. In this case, $\mathbb{K} \subseteq \mathbb{Q}(\psi)$ by the inductive hypothesis. Since $[\mathbb{Q}(\psi) : \mathbb{Q}(\chi)]$ is not divisible by p, we deduce that $\mathbb{K} \subseteq \mathbb{Q}(\chi)$, as wanted.

Thus, we may assume that if N is any normal subgroup of G, then $\chi_N = e\theta$. In particular, $\mathbb{Q}(\theta) \subseteq \mathbb{Q}(\chi)$. Also, if $N < G$, we may assume that θ is τ-invariant, by the inductive hypothesis.

Suppose that $N = \mathbf{O}^p(G) < G$. Since χ has p'-degree, we see that θ has p'-degree. By [Is2, Theorem 6.28], there is a unique extension $\hat{\theta} \in \mathrm{Irr}(G)$ of θ to G with determinantal order not divisible by p. By uniqueness, notice that $\hat{\theta}$ is τ-invariant, because θ is. By Gallagher [Is2, Corollary 6.17], it follows that $\chi = \lambda\hat{\theta}$, where $\lambda \in \mathrm{Irr}(G/N)$ is linear (because G/N is a p-group and $\chi(1)$ is not divisible by p).

We want to show that $\mathbb{K} \subseteq \mathbb{Q}(\chi)$. So it is enough to show that if $\sigma \in \mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q})$ fixes $\mathbb{Q}(\chi)$, then it fixes $\mathbb{K}$. But if σ fixes χ, then it fixes θ. Therefore it fixes $\hat{\theta}$, because $\hat{\theta}$ is uniquely determined by θ. By the uniqueness in the Gallagher correspondence, it follows that σ fixes λ. Hence $\mathbb{Q}(\lambda) \subseteq \mathbb{Q}(\chi)$. Now, since χ is not σ_e-invariant, it follows that λ is not σ_e-invariant. Therefore the order of λ is at least p^{e+1}. Thus $\mathbb{Q}_{p^{e+1}} \subseteq \mathbb{Q}(\lambda)$. Then $\mathbb{K} \subseteq \mathbb{Q}_{p^{e+1}} \subseteq \mathbb{Q}(\lambda) \subseteq \mathbb{Q}(\chi)$, as desired.

If G/N has p' order, where N is proper in G, then since θ is σ_e-invariant, we can apply Lemma 4.2 to deduce that χ is σ_e-invariant, contrary to hypothesis.

Thus, by taking a maximal normal subgroup N of G, we may assume that G/N is a nonabelian simple group. Now we apply Theorem 4.6 to conclude that $\mathbb{K} \subseteq \mathbb{Q}(\chi)$. □

We conclude this section by noting that [NT4, Conjecture A] implies that the conclusion of Theorem B1 holds in the case where P/P' is elementary abelian for $P \in \mathrm{Syl}_p(G)$.

5. Proof of Theorem A3: Quasi-simple groups

Throughout this section, σ_e is defined with respect to $p = 2$. In this section we prove Theorem A3. The bulk of the proof is devoted to the following weaker version:

Theorem 5.1. *Set $e \geq 2$ and let G be a finite quasi-simple group. If $\xi \in \mathrm{Irr}_{2'}(G)$ is not σ_e-invariant, then there is a 2-element $g \in G$ such that $\xi(g) \notin \mathbb{Q}_{2^e}$.*

5.1. Further reductions

First we prove some preliminary results, some of them extracted from [ILNT].

Lemma 5.2. *The following statements hold:*

(i) *It suffices to prove Theorem 5.1 in the case where $\mathbf{Z}(G)$ is of odd order and $\exp(P/P') > 2^e$ for $P \in \mathrm{Syl}_2(G)$.*
(ii) *Furthermore, Theorem 5.1 holds in the case where $G/\mathbf{Z}(G) \cong {}^2F_4(2)'$.*

Proof. (i) Modding out by $\mathrm{Ker}(\xi)$, we may assume that χ is faithful. Since $\xi(1)$ is odd, we then have that $|\mathbf{Z}(G)|$ is odd. Furthermore, since ξ is not σ_e-invariant, $\exp(P/P') > 2^e$ by [M, Theorem 1].

(ii) Since ${}^2F_4(2)'$ has trivial Schur multiplier, we have $G \cong {}^2F_4(2)'$. Now the statement can be checked using [Atlas]. □

Proposition 5.3 ([ILNT], Proposition 4.3)**.** *Let G be a finite simple group and set $P \in \mathrm{Syl}_2(G)$. Then $\exp(P/P') \leq 2$ for $P \in \mathrm{Syl}_2(G)$ if one of the following conditions holds:*

(i) *$G = \mathsf{A}_n$ for some $n \geq 5$.*
(ii) *G is one of the 26 sporadic simple groups.*
(iii) *G is a simple group of Lie type in characteristic 2 and $G \not\cong {}^2F_4(2)'$.*
(iv) *q is an odd prime power. Furthermore, $G = \mathrm{PSp}_{2m}(q)$ with $m \geq 1$, $P\Omega_n^{\pm}(q)$ with $n \geq 7$, $\mathrm{PSL}_{2^m}(q)$ or $\mathrm{PSU}_{2^m}(q)$ with $m \geq 2$, $G_2(q)$, ${}^2G_2(q)$ with $q = 3^{2a+1}$, ${}^3D_4(q)$, $F_4(q)$, $E_8(q)$ or the (simple) group $E_7(q)$.*
(v) *$\epsilon = \pm 1$, q is any prime power such that $4|(q+\epsilon)$ and $G = \mathrm{PSL}_n^{\epsilon}(q)$ with $n \geq 3$, or G is the (simple) group $E_6^{\epsilon}(q)$.*

Corollary 5.4. *It suffices to prove Theorem 5.1 in the case where q is an odd prime power, $q \equiv \epsilon(\bmod\ 4)$ for some $\epsilon = \pm 1$ and either $G = \mathrm{SL}_n^{\epsilon}(q)$ with $n \geq 3$ not a 2-power or $G = E_6^{\epsilon}(q)_{\mathrm{sc}}$.*

Proof. Let $S = G/\mathbf{Z}(G)$, so that S is simple. By Lemma 5.2, we may assume that $|\mathbf{Z}(G)|$ is odd, $S \not\cong {}^2F_4(2)'$ and $\exp(P/P') > 2^e$ for $P \in \mathrm{Syl}_2(G)$. Hence, $\exp(Q/Q') > 2^e$ for $Q \in \mathrm{Syl}_2(S)$. This implies by Proposition 5.3 that there is some $q \equiv \epsilon(\bmod 4)$ such that either $S \cong \mathrm{PSL}_n^{\epsilon}(q)$ with $n \geq 3$ not a 2-power or $S \cong E_6^{\epsilon}(q)$ (the simple group). Inspecting the Schur multiplier of S in those cases, we see that G is a quotient of $\mathrm{SL}_n^{\epsilon}(q)$ or $E_6^{\epsilon}(q)_{\mathrm{sc}}$. Inflating χ if necessary, we may thus assume that $G = \mathrm{SL}_n^{\epsilon}(q)$ or $E_6^{\epsilon}(q)_{\mathrm{sc}}$. □

5.2. *Special linear and unitary groups*

In this subsection we prove Theorem 5.1 for $G = \mathrm{SL}_n^\epsilon(q)$. Set $n \in \mathbb{Z}_{\geq 1}$ and consider the 2-adic decomposition

$$n = 2^{m_1} + 2^{m_2} + \cdots + 2^{m_r}, \tag{5.1}$$

with $m_1 > m_2 > \cdots > m_r \geq 0$. In what follows, we will refer to the summands 2^{m_i} in equation (5.1) as 2*-adic parts* of n. A decomposition $n = n_1 + n_2 + \cdots + n_k$ of n will be called a *proper decomposition* of n if

$$k \geq 1,\ n_i \in \mathbb{Z},\ n_1 > n_2 > \cdots > n_k \geq 1$$

and every 2-adic part of n is a 2-adic part of some summand n_i, $1 \leq i \leq k$. By [GKNT, Lemma 2.2], the latter condition is equivalent to requiring that $n!/\prod_{i=1}^k n_i!$ be odd.

For a fixed $\epsilon \in \{\pm 1\}$, let $\mu_{q-\epsilon} = \langle \zeta \rangle$ be the cyclic subgroup of order $q - \epsilon$ of $\mathbb{F}_{q^2}^\times$ and define $\alpha := \zeta^{(q-\epsilon)_{2'}}$ so that $\langle \alpha \rangle = \mathbf{O}_2(\mu_{q-\epsilon})$. Fix a $(q-\epsilon)$th primitive root of unity $\tilde{\zeta} \in \mathbb{C}$, and define $\tilde{\alpha} := \tilde{\zeta}^{(q-\epsilon)_{2'}}$, a $(q-\epsilon)_2$th root of unity in $\mathbb{C}$. For $s \in \mu_{q-\epsilon}$, let $[s] \in \mathbb{Z}/(q-\epsilon)\mathbb{Z}$ be such that $s = \zeta^{[s]}$. We will consider the map

$$F : x \in \overline{\mathbb{F}}_q^\times \mapsto x^{q\epsilon}.$$

We will also use the Dipper–James labelling for irreducible characters of $\mathrm{GL}_n(q)$, as in [GKNT, (2.2)], and its analogue for a subset of $\mathrm{Irr}(\mathrm{GU}_n(q))$ as explained in [GKNT, Lemma 5.2].

To handle groups of type A we will need the following two statements.

Lemma 5.5. *Let q be an odd prime power, $\epsilon = \pm 1$, $e \geq 2$, set $n \in \mathbb{Z}_{\geq 3}$ not a 2-power and define $G := \mathrm{SL}_n^\epsilon(q) \lhd \mathrm{GL}_n^\epsilon(q) =: \tilde{G}$. Let $\chi \in \mathrm{Irr}(G)$ be of odd degree. Then the following statements hold:*

(i) *χ extends to $\tilde{\chi} \in \mathrm{Irr}(\tilde{G})$.*

(ii) *There exist a proper decomposition $n = n_1 + n_2 + \cdots + n_k$ of n, k pairwise distinct elements $\boldsymbol{s}_i \in \mu_{q-\epsilon}$, $1 \leq i \leq k$, and k partitions $\lambda_i \vdash n_i$, $1 \leq i \leq k$, such that*

$$\tilde{\chi} = S(\boldsymbol{s}_1, \lambda_1) \circ S(\boldsymbol{s}_2, \lambda_2) \circ \cdots \circ S(\boldsymbol{s}_k, \lambda_k).$$

(iii) *Suppose χ is not σ_e-invariant. Then $k \geq 2$ in* (ii)*, $2^{e+1} | (q-\epsilon)$, and there exist $1 \leq i < j \leq k$ such that $(q-\epsilon)_2/2^e$ does not divide $[\boldsymbol{s}_i] - [\boldsymbol{s}_j]$.*

Proof. Statement (i) follows from [ST, Lemma 10.2], and (ii) is proved in [GKNT, Theorem 2.5] for $\epsilon = 1$ and [GKNT, Lemma 5.2] for $\epsilon = -1$.

For (iii), note that for a suitable choice of $\tilde{\zeta}$, $S(\zeta^a, (n))$ is the linear character of $\tilde{G}$ sending $g \in \tilde{G}$ with $\det(g) = \zeta^b$ to $\tilde{\zeta}^{ab}$. Now suppose that χ is not σ_e-invariant but the conclusion of (iii) does not hold. Define $2^a := (q-\epsilon)_2$ and $b := \min(a, e)$. Multiplying $\tilde{\chi}$ by $S((\boldsymbol{s}_1^{-1}, (n))$, we may assume that 2^{a-b} divides $[\boldsymbol{s}_i]$ for all i. Recall that $S(1, \lambda_i)$ is a unipotent character of $\mathrm{GL}_{n_i}^\epsilon(q)$ and so takes only integer values. Since

$$S(\boldsymbol{s}_i, \lambda_i) = S(\boldsymbol{s}_i, (n_i)) S(1, \lambda_i), \tag{5.2}$$

(see, for example, [GT, Lemma 2.9] for the case where $\epsilon = 1$ and the displayed formula just before [GKNT, Lemma 5.1] in general), the condition on $[\boldsymbol{s}_i]$ now implies that $S(\boldsymbol{s}_i, \lambda_i)$ takes values in $\mathbb{Q}(\tilde{\zeta}^{(q-\epsilon)_2/2^b})$, and so it is σ_e-invariant (as $b \leq e$). Note that $\tilde{\chi} = \pm R_L^{\tilde{G}}(\psi)$, where

$$\psi = S(\boldsymbol{s}_1, \lambda_1) \otimes S(\boldsymbol{s}_2, \lambda_2) \otimes \cdots \otimes S(\boldsymbol{s}_k, \lambda_k); \tag{5.3}$$

that is, $\tilde{\chi}$ is Lusztig induced from the Levi subgroup

$$L = \mathrm{GL}_{n_1}^\epsilon(q) \times \mathrm{GL}_{n_2}^\epsilon(q) \times \cdots \times \mathrm{GL}_{n_k}^\epsilon(q). \tag{5.4}$$

For future use, we also note that $\mathbf{N}_{\tilde{G}}(L) = L$. Arguing as in the proof of [GKNT, Theorem 5.3], we see that $\tilde{\chi}$ and χ are σ_e-invariant – a contradiction. □

The next statement is extracted from [GLBST, Lemma 7.5] and its proof.

Lemma 5.6. *Let $\tilde{G} = \mathrm{GL}_n^{\epsilon}(q)$ with $n \geq 1$, $\epsilon = \pm 1$, and let q be any odd prime power. Also fix the generator α of $\mathbf{O}_2(\mu_{q-\epsilon})$ as before. Then the following statements hold:*

(i) *If $n = 2^m$ for some $m \in \mathbb{Z}_{\geq 1}$, then there exists a regular 2-element $g_n(\alpha) \in \tilde{G}$ of determinant α, whose eigenvalues on $\overline{\mathbb{F}}_q^n$ form an F-orbit*

$$\{\theta, \theta^{q\epsilon}, \ldots, \theta^{(q\epsilon)^{n-1}}\}$$

of some generator θ of $\mathbf{O}_2(\mathbb{F}_{q^n}^{\times})$. In particular, all eigenvalues of $g_n(\alpha)$ lie in $\mathbb{F}_{q^{2^m}} \setminus \mathbb{F}_{q^{2^{m-1}}}$.

(ii) *For every 2-element δ of $\mu_{q-\epsilon}$, there exists a regular 2-element $h_n(\delta) \in \tilde{G}$ of determinant δ with all eigenvalues on $\overline{\mathbb{F}}_q^n$ belonging to $\mathbb{F}_{q^{2^{m_1}}}$, if n is written in the form of equation (5.1).*

Theorem 5.7. *Let $n \in \mathbb{Z}_{\geq 3}$ be not a 2-power, $e \geq 2$, $\epsilon = \pm 1$, and let q be an odd prime power such that $(q-\epsilon)_2 = 2^a \geq 4$. Then Theorem 5.1 holds for $G = \mathrm{SL}_n^{\epsilon}(q)$.*

Proof. Let $\chi \in \mathrm{Irr}(G)$ be of odd degree and not σ_e-invariant. We define $\tilde{G} := \mathrm{GL}_n^{\epsilon}(q)$ and apply Lemma 5.5 to get the character $\tilde{\chi}$ as described in that lemma, and $a \geq e+1$. We will write $\tilde{\chi} = \pm R_L^{\tilde{G}}(\psi)$ with ψ given in equation (5.3). Also define $V := \mathbb{F}_q^n$ (or $\mathbb{F}_{q^2}^n$), denote the natural module for $\tilde{G}$ and define $\tilde{V} := V \otimes \overline{\mathbb{F}}_q$. Since $n = n_1 + \cdots + n_k$ is a proper decomposition, the Levi subgroup L from equation (5.4) acts semisimply with pairwise nonisomorphic simple submodules on V and on $\tilde{V}$. Also let I_m denote the identity $m \times m$-matrix over $\mathbb{F}_{q^2}$, and define

$$g_{2^m}(\alpha^{-1}) := (g_{2^m}(\alpha))^{-1},$$

with $g_{2^m}(\alpha)$ as defined in Lemma 5.6.

(i) Case 1. There exist $i_0 < j_0$ such that $2^{a-e-1} \nmid ([\boldsymbol{s}_{i_0}] - [\boldsymbol{s}_{j_0}])$.

Case 1a. Suppose in addition that the smallest 2-adic part 2^{m_r} of n – compare equation (5.1) – is not a 2-adic part of either n_{i_0} or n_{j_0}.

Then we consider the following two elements in $\tilde{G}$ using Lemma 5.6:

$$\begin{aligned} g &= \big(g_{2^{m_1}}(\alpha), \ldots, g_{2^{m_{i_0}}}(\alpha), \ldots, g_{2^{m_{j_0-1}}}(\alpha), g_{2^{m_{j_0}}}(\alpha^{-1}), g_{2^{m_{j_0+1}}}(\alpha), \ldots, g_{2^{m_{r-1}}}(\alpha), h_{2^{m_r}}(\delta)\big),\\ g' &= \big(g_{2^{m_1}}(\alpha), \ldots, g_{2^{m_{i_0-1}}}(\alpha), g_{2^{m_{i_0}}}(\alpha^{-1}), g_{2^{m_{i_0+1}}}(\alpha), \ldots, g_{2^{m_{j_0}}}(\alpha), \ldots, g_{2^{m_{r-1}}}(\alpha), h_{2^{m_r}}(\delta)\big), \end{aligned}$$

each containing only one block $g_{2^{m_i}}(\alpha^{-1})$ with $1 \leq i \leq r-1$, and with $\delta \in \mu_{q-\epsilon}$ chosen so that $g, g' \in \mathrm{SL}_n^{\epsilon}(q)$. We will show that

$$\exp\left(\frac{2\pi i}{2^{e+1}}\right) \in \mathbb{Q}(\chi(g)) \cup \mathbb{Q}(\chi(g')). \tag{5.5}$$

As shown in Case 1a of the proof of [ILNT, Theorem 4.7], each of g and g' is contained in a unique $\tilde{G}$-conjugate of the Levi subgroup L given in equation (5.4), and so without loss we may assume $g, g' \in L$; furthermore,

$$\mathbf{C}_{\tilde{G}}(g) = \mathbf{C}_L(g). \tag{5.6}$$

According to [DM, Proposition 9.6],

$$\mathsf{St}_{\tilde{G}} \cdot \tilde{\chi} = \pm \mathsf{St}_{\tilde{G}} \cdot R_L^{\tilde{G}}(\psi) = \pm(\mathsf{St}_L \cdot \psi)^{\tilde{G}}, \tag{5.7}$$

where $\mathsf{St}_{\tilde{G}}$ (resp., St_L) denotes the Steinberg character of $\tilde{G}$ (resp., of L). Applying this formula to g and using the fact that L is the unique $\tilde{G}$-conjugate of L that contains g, we have

$$\mathsf{St}_{\tilde{G}}(g)\chi(g) = \pm\mathsf{St}_L(g)\psi(g),$$

and similarly for g'. On the other hand, as g is semisimple, we have

$$\mathsf{St}_{\tilde{G}}(g) = \pm|\mathbf{C}_{\tilde{G}}(g)|_p, \quad \mathsf{St}_L(g) = \pm|\mathbf{C}_L(g)|_p$$

(see [DM, Corollary 9.3]), and similarly for g'. It follows that

$$\chi(g) = \kappa\psi(g), \ \chi(g') = \kappa'\psi(g') \tag{5.8}$$

for some $\kappa, \kappa' \in \mathbb{Q}^\times$.

Now we evaluate ψ on g and g', using equation (5.3). Since $2 \nmid \chi(1)$, the degrees of ψ and of $S(\boldsymbol{s}_i, \boldsymbol{\lambda}_i)$ are all odd, whence $S(\boldsymbol{s}_i, \boldsymbol{\lambda}_i)$ evaluated at the $\mathrm{GL}^\epsilon_{n_i}(q)$-component of g is nonzero by [ILNT, Lemma 2.4]. Recalling the constructions of g and g' and applying equation (5.2) to $S(\boldsymbol{s}_{i_0}, \boldsymbol{\lambda}_{i_0})$ and $S(\boldsymbol{s}_{j_0}, \boldsymbol{\lambda}_{j_0})$, we now have

$$\frac{\psi(g)}{\psi(g')} = \tilde{\alpha}^{2([\boldsymbol{s}_{i_0}]-[\boldsymbol{s}_{j_0}])}. \tag{5.9}$$

As $|\tilde{\alpha}| = 2^a$ and $2^{a-e-1} \nmid ([\boldsymbol{s}_{i_0}] - [\boldsymbol{s}_{j_0}])$, we see that $\psi(g)/\psi(g')$ is a root of unity of order $2^f \geq 2^{e+1}$. On the other hand, as the unipotent characters $S(1, \boldsymbol{\lambda}_i)$ take only integer values, equation (5.2) implies that $\psi(g)$ is a $\mathbb{Z}$-multiple of a 2-power root of unity. It follows from equation (5.9) that this root of unity for at least one of g, g' must have order $\geq 2^{e+1}$ – say for g. We conclude by equation (5.8) that $\chi(g)$ is a $\mathbb{Q}$-multiple of a 2-power root of unity of order $\geq 2^{e+1}$, and $\chi(g) \neq 0$ by [ILNT, Lemma 2.4]. Thus $\exp(2\pi i/2^{e+1}) \in \mathbb{Q}(\chi(g))$, establishing formula (5.5).

Case 1b. Suppose we are in Case 1, but the smallest 2-adic part 2^{m_r} of n is a 2-adic part of, say, n_{j_0}. Then we consider the following two elements in $\tilde{G}$ using Lemma 5.6:

$$\begin{aligned} g &= \big(g_{2^{m_1}}(\alpha), g_{2^{m_2}}(\alpha), \ldots, g_{2^{m_{r-1}}}(\alpha), h_{2^{m_r}}(\delta)\big), \\ g' &= \big(g_{2^{m_1}}(\alpha), \ldots, g_{2^{m_{i_0-1}}}(\alpha), g_{2^{m_{i_0}}}(\alpha^{-1}), g_{2^{m_{i_0+1}}}(\alpha), \ldots, g_{2^{m_{r-1}}}(\alpha), h_{2^{m_r}}(\delta\alpha^2)\big), \end{aligned}$$

with $\delta \in \mu_{q-\epsilon}$ chosen so that $g, g' \in \mathrm{SL}^\epsilon_n(q)$. Now the same arguments as in Case 1a show that each of g and g' is contained in a unique $\tilde{G}$-conjugate of L, say $g, g' \in L$, and moreover, equations (5.8) and (5.9) hold. Hence we conclude as before that formula (5.5) holds, as desired.

(ii) Case 2. For all $1 \leq i, j \leq k$, 2^{a-e-1} divides $[\boldsymbol{s}_i] - [\boldsymbol{s}_j]$.

Multiplying $\tilde{\chi}$ by $S(\boldsymbol{s}_1^{-1}, (n))$, we may assume that 2^{a-e-1} divides $[\boldsymbol{s}_i]$ for all $1 \leq i \leq k$. By Lemma 5.5(iii), there exist some $i_0 < j_0$ such that $2^{a-e} \nmid ([\boldsymbol{s}_{i_0}] - [\boldsymbol{s}_{j_0}])$. Keeping in mind that $n = n_1 + \cdots + n_k$ is a proper decomposition, we partition

$$\{m_1, \ldots, m_r\} = \{m'_1, \ldots, m'_s\} \cup \{m''_1, \ldots, m''_t\},$$

with $s + t = r$, $m'_1 > \ldots > m'_s$, $m''_1 > \ldots > m'_t$, such that

- each 2-adic part of any n_i with $2^{a-e} \nmid [\boldsymbol{s}_i]$ is among $2^{m'_1}, \ldots, 2^{m'_s}$, and vice versa, each $2^{m'_{i'}}$ is a 2-adic part of some n_i with $2^{a-e} \nmid [\boldsymbol{s}_i]$; and
- each 2-adic part of any n_j with $2^{a-e} \mid [\boldsymbol{s}_j]$ is among $2^{m''_1}, \ldots, 2^{m''_t}$, and vice versa, each $2^{m''_{i'}}$ is a 2-adic part of some n_j with $2^{a-e} \mid [\boldsymbol{s}_j]$.

Now write $L = L_1 \times L_2$, where

$$L_1 = \prod_{i:2^{a-e}\nmid[\boldsymbol{s}_i]} \mathrm{GL}^\epsilon_{n_i}(q), \ L_2 = \prod_{j:2^{a-e}\mid[\boldsymbol{s}_j]} \mathrm{GL}^\epsilon_{n_j}(q).$$

We claim that to prove the theorem in this case, it suffices to find a 2-element $g \in G$ such that whenever a conjugate g^x of g is contained in L,

$$\text{the projection of } g^x \text{ onto } L_1 \text{ has determinant } \equiv \alpha (\operatorname{mod} \alpha^2). \tag{5.10}$$

Indeed, suppose $h_1 h_2 = g^x \in L$, with h_i the projection of g^x onto L_i for $i = 1, 2$. As g is a 2-element, the determinant of the projection of h_1 onto the direct factor $\mathrm{GL}^{\epsilon}_{n_i}(q)$ of L_1 is α^{a_i} for some $a_i \in \mathbb{Z}$, and similarly the determinant of the projection of h_2 onto the direct factor $\mathrm{GL}^{\epsilon}_{n_j}(q)$ of L_2 is α^{b_j} for some $b_j \in \mathbb{Z}$. Recalling equation (5.2) and the fact that unipotent characters $S(1, \lambda_i)$ take only integer values, we see that there is an integer $\kappa(x) \in \mathbb{Z}$ such that

$$\psi(g^x) = \kappa(x)\tilde{\alpha}^{m(x)},$$

with

$$m(x) := \left(\sum_{i:2^{a-e} \nmid [\boldsymbol{s}_i]} [\boldsymbol{s}_i] a_i + \sum_{j:2^{a-e} | [\boldsymbol{s}_j]} [\boldsymbol{s}_j] b_j \right) \equiv 2^{a-e-1} \sum_{i:2^{a-e} \nmid [\boldsymbol{s}_i]} a_i \equiv 2^{a-e-1} (\operatorname{mod} 2^{a-e}),$$

since by expression (5.10) we have

$$\alpha^{\sum_{i:2^{a-e} \nmid [\boldsymbol{s}_i]} a_i} = \det(h_1) \equiv \alpha (\operatorname{mod} \alpha^2).$$

But $|\tilde{\alpha}| = 2^a$, so we have $\psi(g^x) = \kappa'(x)\tilde{\beta}$, where

$$\tilde{\beta} := \exp(2\pi i / 2^{e+1})$$

and $\kappa'(x) \in \mathbb{Q}(\tilde{\beta}^2) = \mathbb{Q}_{2^e}$. It now follows from equation (5.7) that

$$\chi(g) = \kappa' \tilde{\beta}$$

for some $\kappa' \in \mathbb{Q}_{2^e}$. Since $\kappa \neq 0$ by [ILNT, Lemma 2.4], we conclude that $\chi(g) \notin \mathbb{Q}_{2^e}$, as desired.

We will now follow Case 2 of the proof of [ILNT, Theorem 4.7] to construct a 2-element $g = g_1 g_2 \in G \cap L$, with $g_1 \in L_1$ and $g_2 \in L_2$, that satisfies formula (5.10).

Case 2a. We are in Case 2, but s and t are both odd.

Setting

$$\begin{aligned} g_1 &= \big(g_{2^{m'_1}}(\alpha), g_{2^{m'_2}}(\alpha^{-1}), g_{2^{m'_3}}(\alpha), g_{2^{m'_4}}(\alpha^{-1}), \ldots, g_{2^{m'_{s-2}}}(\alpha), g_{2^{m'_{s-1}}}(\alpha^{-1}), g_{2^{m'_s}}(\alpha)\big), \\ g_2 &= \big(g_{2^{m''_1}}(\alpha^{-1}), g_{2^{m''_2}}(\alpha), g_{2^{m''_3}}(\alpha^{-1}), g_{2^{m''_4}}(\alpha), \ldots, g_{2^{m''_{t-2}}}(\alpha^{-1}), g_{2^{m''_{t-1}}}(\alpha), g_{2^{m''_t}}(\alpha^{-1})\big), \end{aligned}$$

and arguing as in Case 1a, we see that L is the unique $\tilde{G}$-conjugate of L that contains g. Clearly, $\det(g_1) = \alpha$, and so we are done.

Case 2b. We are in Case 2, but $s + t$ is odd.

Multiplying $\tilde{\chi}$ by $S(\alpha^{2^{a-e-1}}, (n))$ if necessary, we may assume that $2 \nmid s$ and $2|t$. We set

$$\begin{aligned} g_1 &= \big(g_{2^{m'_1}}(\alpha), g_{2^{m'_2}}(\alpha^{-1}), g_{2^{m'_3}}(\alpha), g_{2^{m'_4}}(\alpha^{-1}), \ldots, g_{2^{m'_{s-2}}}(\alpha), g_{2^{m'_{s-1}}}(\alpha^{-1}), g_{2^{m'_s}}(\alpha)\big), \\ g_2 &= \big(g_{2^{m''_1}}(\alpha^{-1}), g_{2^{m''_2}}(\alpha), g_{2^{m''_3}}(\alpha^{-1}), g_{2^{m''_4}}(\alpha), \ldots, g_{2^{m''_{t-3}}}(\alpha^{-1}), g_{2^{m''_{t-2}}}(\alpha), g_{2^{m''_{t-1}}}(\alpha^{-1}), g_2^*\big), \end{aligned}$$

where

$$g_2^* = \begin{cases} I_{2^{m''_t}}, & m'_s > m''_t, \\ \big(g_{2^{m''_t - 1}}(\alpha), g_{2^{m''_t - 1}}(\alpha^{-1})\big), & m'_s < m''_t. \end{cases}$$

If $m'_s > m''_t$ or if $m''_t > m'_s$ but $m''_t \neq m'_i + 1$ for all i, then arguing as in Case 1a we see that L is the unique $\tilde{G}$-conjugate of L that contains g. As $\det(g_1) = \alpha$, we are done in this case.

Suppose that $m''_t = m'_j + 1$ for some j and $g \in L^x$ for some $x \in \tilde{G}$. Again, we argue as in Case 1a and see that each 2-adic part 2^{m_i} with $m_i \neq m''_t, m'_j$ is 'filled up' uniquely by the F-orbit of g-eigenvalues within $g_{2^{m_i}}(\alpha^{\pm 1})$ (that is, this F-orbit of g-eigenvalues is the only one of length 2^{m_i}). This leaves three F-orbits of g-eigenvalues, of length $2^{m'_j}$ each, and afforded by two blocks $g_{2^{m'_j}}(\alpha)$ and one block $g_{2^{m'_j}}(\alpha^{-1})$, to fill up the two remaining 2-adic parts $2^{m''_t} = 2 \cdot 2^{m'_j}$ and $2^{m'_j}$. Clearly, all possible ways of filling up the remaining 2-adic part $2^{m'_j}$ for L^x_1 have determinant α or α^{-1}, and so formula (5.10) is satisfied.

Case 2c. We are in Case 2, but s and t are even.

Multiplying $\tilde{\chi}$ by $S(\alpha^{2^{a-e-1}}, (n))$ if necessary, we may assume that $m'_s > m''_t$. We set

$$\begin{aligned} g_1 &= \big(g_{2^{m'_1}}(\alpha), g_{2^{m'_2}}(\alpha^{-1}), g_{2^{m'_3}}(\alpha), g_{2^{m'_4}}(\alpha^{-1}), \ldots, g_{2^{m'_{s-3}}}(\alpha), g_{2^{m'_{s-2}}}(\alpha^{-1}), g_{2^{m'_{s-1}}}(\alpha^{-1}), g_1^\sharp\big),\\ g_2 &= \big(g_{2^{m''_1}}(\alpha^{-1}), g_{2^{m''_2}}(\alpha), g_{2^{m''_3}}(\alpha^{-1}), g_{2^{m''_4}}(\alpha), \ldots, g_{2^{m''_{t-3}}}(\alpha^{-1}), g_{2^{m''_{t-2}}}(\alpha), g_{2^{m''_{t-1}}}(\alpha^{-1}), g_2^*\big),\end{aligned}$$

where $\big(g_1^\sharp || g_2^*\big)$ is chosen to be

$$\begin{array}{ll} \big(\big(g_{2^{m'_s-1}}(\alpha^{-1}), g_{2^{m'_s-1}}(\alpha^3)\big) || I_{2^{m''_t}}\big), & m'_s > m''_t + 1,\\ \big(\mathrm{diag}(1, \alpha^2) || I_1\big); & m'_s = m''_t + 1 = 1,\\ \big(\big(g_{2^{m''_t-1}}(\alpha), g_{2^{m''_t-1}}(\alpha), g_{2^{m''_t-1}}(\alpha), g_{2^{m''_t-1}}(\alpha^{-1})\big) || \big(g_{2^{m''_t-1}}(\alpha), g_{2^{m''_t-1}}(\alpha^{-1})\big)\big), & m'_s = m''_t + 1 \geq 2. \end{array}$$

Suppose $g \in L^x$ for some $x \in \tilde{G}$. Again we argue as in Case 1a and see that each 2-adic part $2^{m_i} > 2^{m'_s}$ is filled up uniquely by the F-orbit of g-eigenvalues of $g_{2^{m_i}}(\alpha^{\pm 1})$.

Consider the case where $m'_s > m''_t + 1$. The smallest 2-adic part $2^{m''_t}$ can only be filled up by the block $I_{2^{m''_t}}$, because all other eigenvalues of g have F-orbit of length $> 2^{m''_t}$. If, moreover, $m'_s - 1$ is not equal to any m''_i, then the two blocks $g_{2^{m'_s-1}}(\alpha^{-1})$ and $g_{2^{m'_s-1}}(\alpha^3)$ can only fill up the 2-adic part $2^{m'_s}$. Thus L is the unique $\tilde{G}$-conjugate of L that contains g, and $\det(g_1) = \alpha$ as desired. Suppose $m'_s - 1 = m''_i$. Then each 2-adic part $2^{m''_j}$ with $i < j < t$ must be filled up by the unique block $g_{2^{m''_j}}(\alpha^{\pm 1})$ in g_2. Next, the 2-adic part $2^{m''_i}$ can be filled up by an F-orbit of length $2^{m''_i}$ coming from the three remaining blocks $g_{2^{m'_s-1}}(\alpha^{-1})$, $g_{2^{m'_s-1}}(\alpha^3)$ and $g_{2^{m''_i}}(\alpha^{\pm 1})$. Any choice of such filling gives the same determinant modulo α^2. The two remaining F-orbits then fill up the remaining 2-adic part $2^{m'_s}$ of L^x_1, thus giving the same determinant modulo α^2 for the projection on g onto L^x_1, as required in formula (5.10).

Suppose $m'_s = m''_t + 1$. In this case, all 2-adic parts but $2^{m'_s} = 2 \cdot 2^{m''_t}$ and $2^{m''_t}$ are already filled up uniquely by suitable blocks of g. If $m''_t = 0$, then the 2-adic part $2^{m''_t}$ can be filled up by a g-eigenvalue 1 or α^2. If $m''_t \geq 1$, then the 2-adic part $2^{m''_t}$ can be filled up by two F-orbits of g-eigenvalues of length $2^{m''_t-1}$, afforded by blocks $g_{2^{m''_t-1}}(\alpha)$ or $g_{2^{m''_t-1}}(\alpha^{-1})$. Evidently, any choice of such filling gives the same determinant modulo α^2. The remaining F-orbits then fill up the remaining 2-adic part $2^{m'_s}$ of L^x_1 and thus give the same determinant modulo α^2 for the projection on g onto L^x_1, as required in formula (5.10).

This completes the proof of Theorem 5.1 for $G = \mathrm{SL}^\epsilon_n(q)$. □

For future reference, we will need the following consequence of the foregoing analysis:

Proposition 5.8. *Let $G = \mathrm{GL}^\epsilon_n(q)$ with $2 \nmid q$ and $\epsilon = \pm$. Suppose*

$$\chi = S(\boldsymbol{s}_1, \boldsymbol{\lambda}_1) \circ S(\boldsymbol{s}_2, \boldsymbol{\lambda}_2) \circ \cdots \circ S(\boldsymbol{s}_k, \boldsymbol{\lambda}_k)$$

is an odd-degree irreducible character of G as in Lemma 5.5(ii), and let 2^c be the smallest 2-part of $[\boldsymbol{s}_i]$, $1 \leq i \leq k$. If $P \in \mathrm{Syl}_2(G)$ and $2^a := (q - \epsilon)_2$, then $\mathbb{Q}(\chi_P) = \mathbb{Q}_{2^{a-c}}$.

Proof. (i) Recall that unipotent characters $S(1, \boldsymbol{\lambda}_i)$ and linear characters $S(\pm 1, (n_i))$ are rational-valued. More generally, if 2^{t_i} denotes the 2-part of $[\boldsymbol{s}_i]$, then the linear character $S(\boldsymbol{s}_i, (n_i))$ can take values at

2-elements only in $\mathbb{Q}_{2^{a-t_i}}$. Hence, using equation (5.2) and the arguments in the proof of Lemma 5.5, we see that

$$\mathbb{Q}(\chi_P) \subseteq \mathbb{Q}_{2^{a-c}}. \tag{5.11}$$

In particular, if $c \geq a-1$, then $\chi|_P$ is rational and we are done. In what follows we may therefore assume that $a \geq 2$ and $c \leq a-2$. Furthermore, if $k=1$, then $c=t_1$ and again we are done by using equation (5.2) and the preceding arguments. Thus we may assume that $k \geq 2$; in particular, n is not a 2-power (since $n = n_1 + \cdots + n_k$ is a proper decomposition).

(ii) Let $0 \leq b \leq a$ be the largest integer subject to the condition that 2^b divides $[\boldsymbol{s}_i] - [\boldsymbol{s}_j]$ for all $1 \leq i < j \leq k$. Note that $b \geq c$. (Assume that $b \leq c-1$. By the definition of b and c, we have $[\boldsymbol{s}_i]_2 = 2^c$ for some i and $2^c \nmid ([\boldsymbol{s}_i] - [\boldsymbol{s}_j])$ for some $j \neq i$, whence $2^c \nmid [\boldsymbol{s}_j]$ – a contradiction.) Next we fix an index l with $[\boldsymbol{s}_l]_2 = 2^c$ and write

$$\chi = S(\boldsymbol{s}_l, (n))\chi', \tag{5.12}$$

where $\chi' = S(\boldsymbol{s}_1/\boldsymbol{s}_l, \boldsymbol{\lambda}_1) \circ S(\boldsymbol{s}_2/\boldsymbol{s}_l, \boldsymbol{\lambda}_2) \circ \cdots \circ S(\boldsymbol{s}_k/\boldsymbol{s}_l, \boldsymbol{\lambda}_k)$. Then χ and χ' have the same restriction, call it φ, to $[G,G] = \mathrm{SL}_n^{\epsilon}(q)$. The arguments in the proof of Lemma 5.5 can then apply to show that φ is $\sigma_{b'}$-invariant for all $b' \geq a-b$ and

$$\mathbb{Q}(\chi'_P) \subseteq \mathbb{Q}_{2^{a-b}}, \ \mathbb{Q}(\chi_Q) \subseteq \mathbb{Q}_{2^{a-b}}, \tag{5.13}$$

where $Q = P \cap [G,G] \in \mathrm{Syl}_2([G,G])$. We also note that

$$S(\boldsymbol{s}_1, (n))(u) \text{ is a primitive } 2^{a-c}\text{-root of unity if } u \in P \text{ has } \det(u) = \zeta^{(q-\epsilon)_{2'}}. \tag{5.14}$$

Consider the case where $b \geq a-1$. By formula (5.13), $\chi'(u) \in \mathbb{Q}$, and it is nonzero as $2 \nmid \chi(1)$. Hence equation (5.12) and formula (5.14) show that $\mathbb{Q}(\chi(u)) \supseteq \mathbb{Q}_{2^{a-c}}$, whence we have equality in formula (5.11), as required.

(iii) From now on we may assume that $b \leq a-2$. Note that $\varphi = \chi_{[G,G]}$ is irreducible, since $\boldsymbol{s}_i$, $1 \leq i \leq k$, are pairwise distinct and $n = n_1 + \cdots + n_k$ is a proper decomposition. Moreover,

$$\varphi \text{ is not } \sigma_{a-b-1}\text{-invariant}. \tag{5.15}$$

Assume the contrary. As φ extends to G, we have that χ and $\sigma_{a-b-1}(\chi)$ can differ only by a linear character of G. Using the unique representation of χ as in Lemma 5.5(ii) (see, for example, [GKNT, Lemma 5.2] for the uniqueness in the case where $\epsilon = -$) and the action of Galois automorphisms of $\mathbb{Q}_{q-\epsilon}$ on these representations (see, for example, the last displayed formula in the proof of [GKNT, Theorem 5.3]), we have

$$(\boldsymbol{s}'_1)^{2^{a-b-1}} = (\boldsymbol{s}'_2)^{2^{a-b-1}} = \cdots = (\boldsymbol{s}'_k)^{2^{a-b-1}},$$

where $\boldsymbol{s}'_i$ is the 2-part of $\boldsymbol{s}_i$, and in fact $(\boldsymbol{s}_i/\boldsymbol{s}_j)^{2^{a-b-1}} = 1$ for all i, j. This implies that 2^{b+1} divides $[\boldsymbol{s}_i] - [\boldsymbol{s}_j]$ for all i, j, contradicting the choice of b.

In particular, φ is not σ_1-invariant, and so it is not 2-rational. By [ILNT, Theorem E], $i \in \mathbb{Q}(\varphi_Q) \subseteq \mathbb{Q}(\chi_P)$. Recalling formula (5.11) and the cyclic extension $\mathbb{Q}_{2^{a-c}}/\mathbb{Q}(i)$, it suffices now to show that

$$\mathbb{Q}(\chi_P) \not\subseteq \mathbb{Q}_{2^{a-c-1}}. \tag{5.16}$$

(iv) If $b > c$, then formulas (5.13) and (5.14) show that $\chi(u) \notin \mathbb{Q}_{2^{a-c-1}}$, and so formula (5.16) holds. Finally, we consider the case where $b = c$. If $c = a-2$, then $i \in \mathbb{Q}(\chi_P)$ as noted already, implying formula (5.16). If $c \leq a-3$, then as φ is not σ_{a-c-1}-invariant, by formula (5.15), we have $\mathbb{Q}(\varphi_Q) \not\subseteq \mathbb{Q}_{2^{a-c-1}}$ by Theorem 5.1, and so formula (5.16) holds again, completing the proof. □

5.3. *Groups of type E_6 and $^2E_6(q)$*

The rest of the section is devoted to proving Theorem 5.1 for $G = E_6^\epsilon(q)_{\mathrm{sc}}$. First we recall the following result from [ILNT]:

Proposition 5.9 ([ILNT], Proposition 4.9)**.** *Let $G = \mathcal{G}^F = E_6^\epsilon(q)_{\mathrm{sc}}$, and suppose that $q \equiv \epsilon (\mathrm{mod}\, 8)$. Write $(q-\epsilon)_2 = 2^a$. Then there exists an element $t \in G$ with the following properties:*

(i) *t is a 2-element;*
(ii) *$\mathbf{C}_G(t)$ is a maximal torus $(q^4-1)\times(q^2-1)$;*
(iii) *t centralises a unique involution v that has centraliser of type D_5T_1 in $\mathcal{G}$;*
(iv) *if $L = \mathbf{C}_G(v)$ and $D = L' \cong D_5^\epsilon(q)$, then the coset $tD \in L/D$ has order 2^a and generates $\mathbf{O}_2(L/D)$;*
(v) *$t^G \cap L = t^L$.*

Proof of Theorem 5.1 By Corollary 5.4 and Theorem 5.7, it suffices to prove Theorem 5.1 in the case where $G = \mathcal{G}^F = E_6^\epsilon(q)_{\mathrm{sc}}$, with $\epsilon = \pm 1$ and $4|(q-\epsilon)$. Here $\mathcal{G}$ is a simple, simply connected algebraic group of type E_6 in characteristic $p|q$ and $F : \mathcal{G} \to \mathcal{G}$ is a suitable Steinberg endomorphism. Using [Lu] one can see that G has exactly $8(q-\epsilon)$ irreducible characters of odd degree, eight of which are unipotent and listed in [C, §13.9]. As shown in the proof of [M, Theorem 3.4], any unipotent character of odd degree of G lies in the principal series and is 2-rational. So we may assume that χ is one of $8(q-\epsilon-1)$ nonunipotent characters of odd degree and χ belongs to the rational series $\mathcal{E}(G,(s))$, labelled by a 2-central semisimple element $s \in G^*$. Here, $G^* = \mathcal{G}^{*F^*}$ and $(\mathcal{G}^*, F^*)$ is dual to $(\mathcal{G}, F)$.

As mentioned in the proof of [M, Theorem 3.4], $\mathbf{C}_{\mathcal{G}^*}(s)$ is connected. In fact, as one can see using [LSS, Table 5.1], there are $q-\epsilon-1$ classes of such elements $s \in G^*$, with $\mathbf{C}_{\mathcal{G}^*}(s) = \mathcal{L}^*$, an F^*-stable Levi subgroup of type D_5T_1, dual to an F-stable Levi subgroup $\mathcal{L}$ of $\mathcal{G}$. Next, as mentioned in the proof of [NT3, Lemma 4.13], $L := \mathcal{L}^F$ and $\mathcal{L}^{*F^*}$ each have exactly eight unipotent characters of odd degree, and furthermore their degrees are pairwise distinct. The latter immediately implies that these unipotent characters are rational-valued (indeed, any Galois automorphism of $\overline{\mathbb{Q}}$ acts on the set of unipotent characters and hence fixes each of these eight characters).

Since $\mathbf{C}_{\mathcal{G}^*}(s) = \mathcal{L}^*$, Lusztig's classification of irreducible characters of G in the rational series $\mathcal{E}(G,(s))$ [DM, §13] yields

$$\chi = \pm R_L^G(\psi\lambda), \tag{5.17}$$

where $\psi \in \mathrm{Irr}(L)$ is unipotent of odd degree and $\lambda \in \mathrm{Irr}(L)$ has degree 1. (Indeed, as $s \in \mathbf{Z}(L^*)$, by [DM, Proposition 13.30], there is a linear character $\lambda = \hat{s}$ of L such that multiplication by λ gives a bijection between $\mathcal{E}(L,(1))$ and $\mathcal{E}(L,(s))$. Next, by [DM, Theorem 13.25], there are some signs ε_G and ε_L such that the map

$$\varepsilon_G\varepsilon_L R_L^G : \mathcal{E}(L,(s)) \to \mathcal{E}(G,(s))$$

is a bijective isometry which sends true characters to true characters.) The formula for the Lusztig induction functor R_L^G (see [DM, p. 90]) shows that it commutes with Galois actions on characters; see also [GM, Corollary 3.3.14]. With the assumption that χ is not σ_e-invariant and the aforementioned rationality of ψ, this implies that λ is not σ_e-invariant. Since $L/D \cong C_{q-\epsilon}$ for $D := L'$ as in Proposition 5.9(iv), it follows that λ is a character of L/D of order divisible by 2^{e+1}, and $(q-\epsilon)_2 = 2^a \geq 2^{e+1}$.

We now consider the regular 2-element $t \in L$ constructed in Proposition 5.9. For any $t' \in t^G \cap L$, $\mathbf{C}_{\mathcal{G}}(t')$ is a maximal torus (of rank 6). At the same time, $\mathbf{C}_{\mathcal{L}}(t')$ contains a maximal torus of rank 6. It follows that $\mathbf{C}_{\mathcal{L}}(t') = \mathbf{C}_{\mathcal{G}}(t')$, and so $\mathbf{C}_G(t') \leq L$ for all $t' \in t^G \cap L$. Thus we can apply [ILNT, Lemma 4.8] to t and obtain from equations (5.7) and (5.17) that

$$\chi(t) = \pm \mathsf{St}_G(t)\chi(t) = \pm(\mathsf{St}_G \cdot R_L^G(\psi\lambda))(t) = \pm(\mathsf{St}_L\psi\lambda)^G(t) = \pm\psi(t)\lambda(t) \tag{5.18}$$

(noting that the Steinberg character takes values ±1 at regular semisimple elements). Recall from Proposition 5.9(iv) that the coset tD generates $\mathbf{O}_2(L/D)$. Since λ has order divisible by 2^{e+1}, it follows that $\lambda(t)$ is a primitive root of unity ξ of order $2^b \geq 2^{e+1}$. Now equation (5.18) yields $\chi(t) = \pm\psi(t)\xi$, and $\psi(t)$ is an odd integer by [ILNT, Lemma 2.4]. Hence $\mathbb{Q}_{2^{e+1}} \subseteq \mathbb{Q}(\chi(t))$, as required. □

5.4. *Completion of the proof of Theorem A3*

Note that Theorem A3 obviously holds when $a = 0$. Since $\mathbb{Q}_m = \mathbb{Q}_{2m}$ when m is odd, it remains to prove Theorem A3 when $a \geq 2$; in particular, χ is not 2-rational. By Lemma 4.1(iii), a is the smallest integer $e \geq 2$ such that χ is σ_e-invariant. The first statement of Theorem A3 now follows from [ILNT, Theorem E] when $a = 2$, and it is just Theorem 5.1 when $a \geq 3$. For the second statement, define $b := \exp(P)$, so that $\mathbb{L} := \mathbb{Q}(\chi_P) \subseteq \mathbb{Q}_{2^b}$. It follows from [ILNT, Theorem E] that $i \in \mathbb{L}$, and so $\mathbb{Q}_{2^2} \subseteq \mathbb{L} \subseteq \mathbb{Q}_{2^b}$ and $b \geq 2$. However, $\mathbb{Q}_{2^b}/\mathbb{Q}_{2^2}$ is a cyclic extension of degree 2^{b-2}, and all intermediate subfields are $\mathbb{Q}_{2^c}$ with $2 \leq c \leq b$. It follows that $\mathbb{L} = \mathbb{Q}_{2^d}$ for some $2 \leq d \leq b$. Applying Theorem 5.1, we have $d \geq a$. On the other hand, $d \leq a$ by the definition of $c(\chi) = 2^a m$, and hence $d = a$, as stated. □

6. Evidence in support of Conjecture B3

Theorem 6.1. *Let $p > 2$ be a prime and G a finite quasisimple group. Then Conjecture B3 holds for G, unless possibly when $S := G/\mathbf{Z}(G)$ is a finite simple group of Lie type in characteristic $\neq p$.*

Proof. (i) First we consider the ‘generic’ case, where G is a quotient of $\mathcal{G}^F$ for some simple, simply connected algebraic group $\mathcal{G}$ over a field of characteristic p and $F : \mathcal{G} \to \mathcal{G}$ a Steinberg endomorphism, and let $\mathbb{K} := \mathbb{Q}(\zeta_{|G|_{p'}})$, where $\zeta_n := \exp(2\pi i/n)$ for any $n \in \mathbb{Z}_{\geq 1}$. Set $\chi \in \mathrm{Irr}(G)$. Now if $p = 5$ and $\mathcal{G}$ is of type E_8, then $\mathbb{Q}(\chi) \subseteq \mathbb{K}(\zeta_p)$ by [TZ, Proposition 10.12]. In all other cases, $\mathbb{Q}(\chi) \subseteq \mathbb{K}(\sqrt{p}) \subseteq \mathbb{K}(\zeta_p)$ by [TZ, Theorem 1.3]. It follows that χ has conductor $c(\chi) = p^a m$ with $p \nmid m$ and $0 \leq a \leq 1$. In this case, if $g \in G$ is a p-element, then $\chi(g) \in \mathbb{Q}_{p^a}$ and certainly $[\mathbb{Q}_{p^a} : \mathbb{Q}]$ divides $p - 1$, and so we are done.

(ii) Next we consider the case where $S = \mathsf{A}_n$ with $n \geq 8$. Without any loss we may assume that $\mathbf{Z}(G) = C_2$, and G is a normal subgroup of index 2 in $H = 2\mathsf{S}_n$, a double cover of S_n; in particular, $\mathbf{Z}(H) = \mathbf{Z}(G) = \langle z \rangle$. Define $\mathbb{K} := \mathbb{Q}(\zeta_{|G|_{p'}})$, and consider any p-element $g \in G$ and p'-element $s \in H$ that commutes with g. With s projecting onto $\bar{s} \in \mathsf{S}_n$, define $C := \mathbf{C}_H(s)$, $\bar{C} := \mathbf{C}_{H/\mathbf{Z}(H)}(\bar{s})$, and let D be the full inverse image of $\bar{C}$ in H. Clearly, $xsx^{-1} = s$ or sz, and so $[D : C] \leq 2$. It is well known that any complex character of S_n is rational and so has a field of values contained in $\mathbb{K}$. By [TZ, Corollary 2.12], the latter implies that every p-element in S_n is *strongly rational* – that is, rational in the centraliser of any p'-element of S_n that commutes with it. Hence, for any integer $\ell \in \mathbb{Z}$ coprime to p, there exists an element $y \in D$ such that $ygy^{-1} \in g^\ell \mathbf{Z}(H)$. But since $|g|$ is odd and $\mathbf{Z}(H) = C_2$, it follows that $ygy^{-1} = g^\ell$ – that is, g is rational in D. Since $[D : C] \leq 2$, it follows that the generators of $\langle g \rangle$ break into at most two C-conjugacy classes. We have shown that g is strongly half-rational in the sense of [TZ, Definition 2.4]. Hence, by [TZ, Lemma 2.8(ii)], $\mathbb{Q}(\chi) \subseteq \mathbb{K}(\sqrt{p})$ for every $\chi \in \mathrm{Irr}(H)$.

Consider any $\psi \in \mathrm{Irr}(G)$, and assume first that ψ is faithful. By a classical result of Schur [HH, Theorem 8.6], there is a strict partition λ of n such that ψ is an irreducible constituent of a faithful irreducible character $\langle \lambda \rangle$ of H labelled by λ. Moreover, if λ is odd, then $\psi = \langle \lambda \rangle_G$, whence $\mathbb{Q}(\psi) \subseteq \mathbb{K}(\sqrt{p})$ as already shown. Suppose λ is even. Then, again by Schur’s result [HH, Theorem 8.7(iv)], for any $x \in G$ we have $\psi(x) = (\langle \lambda \rangle(x) \pm \xi)/2$, where either $\xi = 0$ or x projects onto an element of cycle type $\lambda = (\lambda_1, \ldots, \lambda_l)$ in S_n and

$$\xi = \sqrt{(-1)^{(n-l)/2}\lambda_1 \ldots \lambda_l}.$$

Since $\xi \in \mathbb{K}(\sqrt{p})$, we conclude that $\mathbb{Q}(\psi) \subseteq \mathbb{K}(\sqrt{p})$. In the case where ψ is not faithful, the same conclusion holds by [JK, Theorem 2.5.13].

We have shown that $\mathbb{Q}(\psi) \subseteq \mathbb{K}(\sqrt{p})$ for all $\psi \in \mathrm{Irr}(G)$, and the statement now follows as at the end of (i).

(iii) All the remaining cases – where S is either a sporadic simple group, A_n with $5 \leq n \leq 7$ or a simple group of Lie type with exceptional Schur multiplier – can be checked directly using [GAP]. □

7. Results on Conjecture C

In this last section, we prove some results on Conjecture C. In order to check our statement, a more comprehensive understanding of the values of p'-degree characters on p-elements is needed.

We start with some elementary lemmas.

Lemma 7.1. *Let G be a finite group and p a prime, and set $P \in \mathrm{Syl}_p(G)$. Set $\chi \in \mathrm{Irr}(G)$ and let $f = p^a m$ be the conductor of χ, where $a \geq 0$ and p does not divide m. Then the conductor of $\mathbb{Q}(\chi_P)$ divides p^a. In particular, $\mathbb{Q}(\chi_P) \subseteq \mathbb{Q}_{p^a}$.*

Proof. If p^b is the exponent of P, we have $\mathbb{Q}(\chi_P) \subseteq \mathbb{Q}_{p^b}$. In particular, the conductor of $\mathbb{Q}(\chi_P)$ is p^c for some $c \leq b$. Now $\mathbb{Q}(\chi_P) \subseteq \mathbb{Q}(\chi) \subseteq \mathbb{Q}_{p^a m}$, and therefore $\mathbb{Q}(\chi_P) \subseteq \mathbb{Q}_{p^c} \cap \mathbb{Q}_{p^a m} = \mathbb{Q}_{\mathrm{gcd}(p^c, p^a m)} = \mathbb{Q}_{\mathrm{min}(p^c, p^a)}$. By the definition of the conductor, we have $p^c \leq \min(p^c, p^a)$, and therefore $p^c \leq p^a$, as required. □

Next we show an elementary reformulation of Conjecture C for p odd, which also shows its equivalence with the conclusion of Conjecture B3. Again, recall that if p is odd and $a \geq 1$, then $\mathbb{E}_{p^{a-1}}$ is the unique subfield of $\mathbb{Q}_{p^a}$ of degree p^{a-1} over $\mathbb{Q}$.

Lemma 7.2. *Suppose that p is odd. Let $\chi \in \mathrm{Irr}(G)$ have conductor $p^a m$, where p does not divide m, $a \geq 2$, and set $P \in \mathrm{Syl}_p(G)$. Then the following are equivalent:*

(i) *There exists $x \in P$ such that $\mathbb{E}_{p^{a-1}} \subseteq \mathbb{Q}(\chi(x))$.*
(ii) *p does not divide $[\mathbb{Q}_{p^a} : \mathbb{Q}(\chi_P)]$.*
(iii) *χ_P is not τ-invariant, where $\tau \in \mathrm{Gal}(\mathbb{Q}_{p^a}/\mathbb{Q})$ is any Galois automorphism of order p.*

Proof. We have that the extension $\mathbb{Q}_{p^a}/\mathbb{Q}$ is cyclic and that $\mathbb{E}_{p^{a-1}}$ is contained in every subfield K of $\mathbb{Q}_{p^a}$ such that $[\mathbb{Q}_{p^a} : K]$ is not divisible by p, by elementary Galois theory. Let $\tau \in \mathrm{Gal}(\mathbb{Q}_{p^a}/\mathbb{Q})$ be of order p, and let $F = \mathbb{Q}_{p^{a-1}}$ be the fixed field of τ, which is the unique subfield K such that $[\mathbb{Q}_{p^a} : K] = p$. Hence F contains every subfield $K \subseteq \mathbb{Q}_{p^a}$ such that $[\mathbb{Q}_{p^a} : K]$ is divisible by p. By Lemma 7.1, we have $\mathbb{Q}(\chi(x)) \subseteq \mathbb{Q}(\chi_P) \subseteq \mathbb{Q}_{p^a}$ for every $x \in P$.

Now, if there exists $x \in P$ such that $\mathbb{E}_{p^{a-1}} \subseteq \mathbb{Q}(\chi(x)) \subseteq \mathbb{Q}(\chi_P)$, then p does not divide $[\mathbb{Q}_{p^a} : \mathbb{Q}(\chi_P)]$. Hence (i) implies (ii). Assume (ii). If $\mathbb{E}_{p^{a-1}}$ is not contained in $\mathbb{Q}(\chi(x))$, where $x \in P$, then p divides the index of the cyclic extension $\mathbb{Q}_{p^a}/\mathbb{Q}(\chi(x))$, and therefore $\mathbb{Q}(\chi(x)) \subseteq F$. If this happens for all $x \in P$, we have $\mathbb{Q}(\chi_P) \subseteq F$ and therefore p divides $[\mathbb{Q}_{p^a} : \mathbb{Q}(\chi_P)]$. Finally, p divides $[\mathbb{Q}_{p^a} : \mathbb{Q}(\chi_P)]$ if and only if $\mathbb{Q}(\chi_P) \subseteq \mathbb{Q}_{p^{a-1}}$ if and only if χ_P is τ-invariant. This shows that (ii) and (iii) are equivalent. □

Next we prove Conjecture C in the case where G has a normal Sylow p-subgroup.

Theorem 7.3. *Let G be a finite group, and set $P \in \mathrm{Syl}_p(G)$. Set $\chi \in \mathrm{Irr}_{p'}(G)$ and assume $P \triangleleft G$. Suppose that the conductor of χ is $p^a m$, where $a \geq 1$ and p does not divide m. Then $\mathbb{Q}_{p^a}/\mathbb{Q}(\chi_P)$ has degree not divisible by p.*

Proof. By Lemma 7.1, we have $\mathbb{Q}(\chi_P) \subseteq \mathbb{Q}_{p^a}$. We may assume that $a \geq 2$. Let $\lambda \in \mathrm{Irr}(P)$ be a linear irreducible constituent of χ_P. By Lemma 2.5(ii), we have $o(\lambda) = p^a$. Now apply Lemma 2.5(i). □

Using Gajendragadkar–Isaacs theory, it is easy to prove Conjecture C for primitive characters of p-solvable groups.

Theorem 7.4. *Suppose that χ is a primitive character of a p-solvable group, of degree not divisible by p. If p^a is the p-part of the conductor of χ, and $P \in \mathrm{Syl}_p(G)$, then $\mathbb{Q}(\chi_P) = \mathbb{Q}_{p^a}$. In particular, Conjecture C holds for χ.*

Proof. Suppose that $\chi = \alpha\beta$, where α is a p'-special character of G and β is p-special and linear. We know that α is p-rational by [Is3, Corollary 2.13]. By Lemma 2.4, we have $c(\chi) = c(\alpha)c(\beta)$ and $c(\beta) = c(\chi)_p = p^a$. Also, $\mathbb{Q}(\chi_P) = \mathbb{Q}(\beta_P) = \mathbb{Q}_{p^a}$. □

The following might be useful in the future:

Theorem 7.5. *If G is a counterexample for Conjecture C minimising $|G|$, then $\mathbf{O}_p(G) = 1$ and G/G' has order not divisible by p.*

Proof. Set $\chi \in \mathrm{Irr}(G)$ of p'-degree and suppose that the p-part of the conductor of χ is p^a. Set $P \in \mathrm{Syl}_p(G)$. Assume that $\mathbb{Q}_{p^a}/\mathbb{Q}(\chi_P)$ has degree divisible by p but Conjecture C holds for every finite group of order smaller than G. We have $a \geq 2$. We also may assume that $\ker(\chi) = 1$ by minimality.

Let $N = \mathbf{O}^p(G)$ and assume that $N < G$. We will now deduce a contradiction. Write $\chi_N = \theta \in \mathrm{Irr}(N)$ and $\chi = \hat{\theta}\lambda$, where $\hat{\theta}$ is the canonical extension of θ and $\lambda \in \mathrm{Irr}(G/N)$ is linear. In particular, $c(\theta) = c(\hat{\theta})$. (See [N2, Corollaries 6.2 and 6.4].) Suppose that θ is p-rational. Then $\hat{\theta}$ is p-rational, and then $\mathbb{Q}(\chi_P) = \mathbb{Q}(\lambda)$ by Lemma 2.4. Since $p^a = c(\chi)_p = c(\lambda)$ by Lemma 2.4, we get a contradiction. We assume that θ is not p-rational.

If $e \geq 1$, notice that

$$(\hat{\theta}\lambda)^{\sigma_e} = \hat{\theta}\lambda$$

if and only if $\theta^{\sigma_e} = \theta$ and $\lambda^{\sigma_e} = \lambda$, using the uniqueness in the Gallagher correspondence. This shows that $c(\chi)_p = \max(c(\lambda), c(\theta)_p)$, using Lemma 4.1(iii).

Write $c(\theta)_p = p^d$, where $d \geq 1$, $o(\lambda) = p^b$, and let $Q = P \cap N$. By induction, we have that $\mathbb{Q}_{p^d}/\mathbb{Q}(\chi_Q)$ has degree not divisible by p.

Assume first that $p^b \leq p^d$. Then $c(\chi)_p = p^a$ and $a = d$. Since $\mathbb{Q}_{p^a}/\mathbb{Q}(\chi_Q)$ has degree not divisible by p and $\mathbb{Q}(\chi_Q) \subseteq \mathbb{Q}(\chi_P) \subseteq \mathbb{Q}_{p^a}$, we are done in this case.

Assume now that $p^b > p^d$. Therefore $c(\chi)_p = o(\lambda) = p^b$ and $a = b$. Let $\tau \in \mathrm{Gal}(\mathbb{Q}_{p^b m}/\mathbb{Q}_{p^d m})$ be of order p, where m is the p'-part of the order of $|G|$, fixing $\chi_P = \hat{\theta}_P\lambda_P$. Then τ fixes $\hat{\theta}$ and thus, using the fact that $\hat{\theta}(x) \neq 0$ on every p-element x, we have $\lambda^\tau = \lambda$, which is impossible. This shows that G/G' has order not divisible by p.

Assume that $\mathbf{O}_p(G) > 1$. Notice that $\mathbf{O}_p(G) \leq G'$, by the previous part. Let L be a minimal normal subgroup of G inside $\mathbf{O}_p(G)$. Therefore, L is an elementary abelian p-subgroup. Now, let $\epsilon \in \mathrm{Irr}(P)$ be a linear irreducible constituent of χ_P, and let $\lambda = \epsilon_L$. Notice that $\lambda \neq 1$, because χ is faithful. Thus, if $T = G_\lambda$ is the stabiliser of λ in G, we have $P \leq T$. Also, let $\psi \in \mathrm{Irr}(T|\lambda)$ be the Clifford correspondent of χ over λ. Thus $\psi^G = \chi$ and $\chi_T = \psi + \Delta$, where no irreducible constituent of Δ lies over λ (using the Clifford correspondence). By the induction formula and the fact that the p-elements of T are inside some T-conjugate of P, we easily deduce that $\mathbb{Q}(\chi_P) \subseteq \mathbb{Q}(\psi_P)$. In particular, $p^a \leq p^c$, where c is the conductor of ψ_P. We claim that $\mathbb{Q}_p(\chi_P) = \mathbb{Q}(\psi_P)$, where $\mathbb{Q}_p = \mathbb{Q}(\lambda)$ is the pth cyclotomic field. Since ψ_L is a multiple of λ, we have $\mathbb{Q}_p(\chi_P) \subseteq \mathbb{Q}(\psi_P)$. Set $\sigma \in \mathrm{Gal}(\mathbb{Q}(\psi_P)/\mathbb{Q}_p(\chi_P))$. Notice that we have $\chi_P = \psi_P + \Delta_P$, where no irreducible constituent of Δ_P lies over λ. Now let ρ be an irreducible constituent of ψ_P. Since σ fixes χ_P, it follows that ρ^σ is an irreducible constituent of either ψ_P or Δ_P. Since ρ lies over λ and σ fixes λ, it follows that ρ^σ is an irreducible constituent of ψ_P. Then

$$[\psi_P, \rho] = [\chi_P, \rho] = [(\chi_P)^\sigma, \rho^\sigma] = [\chi_P, \rho^\sigma] = [\psi_P, \rho^\sigma],$$

and we easily deduce that $(\psi_P)^\sigma = \psi_P$. This proves the claim.

By elementary Galois theory, we have that $\mathrm{Gal}(\mathbb{Q}(\psi_P)/\mathbb{Q}(\chi_P))$ is isomorphic to $\mathrm{Gal}(\mathbb{Q}_p/(\mathbb{Q}_p \cap \mathbb{Q}(\chi_P)))$, and therefore has order not divisible by p. Thus $\mathbb{Q}(\psi_P)/\mathbb{Q}(\chi_P)$ has degree not divisible by p.

Now, by [N2, Lemma 5.11], we have that λ extends to some $\nu \in \mathrm{Irr}(T)$. If $T = G$, then $G' \leq \ker(\nu)$, and therefore $\lambda = 1$, which is not possible. We conclude that $T < G$. By minimality, we have that $\mathbb{Q}_{p^c}/\mathbb{Q}(\psi_P)$ has degree not divisible by p. Since $p^a \leq p^c$, $a \geq 2$, and $\mathbb{Q}(\psi_P)/\mathbb{Q}(\chi_P)$ has degree not divisible by p, we deduce that $\mathbb{Q}(\psi_P) \subseteq \mathbb{Q}_{p^a}$. Then $a = c$, and $\mathbb{Q}_{p^a}/\mathbb{Q}(\chi_P)$ has degree not divisible by p. This is a contradiction. □

Theorem A3 immediately shows the following:

Corollary 7.6. *Conjecture C holds in the case where $p = 2$ and G is quasi-simple.*

Another case of Conjecture C that we can handle is the following:

Theorem 7.7. *Suppose that G has p-length 1. Then Conjecture C holds for G. In particular, Conjecture C holds for p-solvable groups with abelian Sylow p-subgroups.*

Proof. Suppose that G has a normal p'-subgroup K and a Sylow p-subgroup P such that $L = KP \triangleleft G$. Suppose that $\chi \in \mathrm{Irr}_{p'}(G)$, and let p^a be the p-part of the conductor of χ. We may assume that $a \geq 2$.

Let $\eta \in \mathrm{Irr}(L)$ be under χ, so that χ_L is a rational multiple of $\sum_{x \in \mathbf{N}_G(P)} \eta^x$. Now η has p'-degree, so $\eta_K = \theta \in \mathrm{Irr}(K)$. Thus $\eta = \hat{\theta}\lambda$ for some $\lambda \in \mathrm{Irr}(P)$ linear, where $\hat{\theta} \in \mathrm{Irr}(L)$ is the canonical extension of θ. (We identify the characters of L/K with the characters of P.) By the first paragraph in the proof of Theorem 7.4, we have that the p-part of the conductor of η is $o(\lambda) = p^b$ (using the facts that $\hat{\theta}$ is p'-special and λ is p-special).

We claim that η is not p-rational. Otherwise, if $p = 2$, χ is p-rational by Lemma 4.2(ii), which is not possible. If p is odd, then $\lambda = 1$ and η is p'-special. Since G/L is a p'-group, χ is p'-special by [Is3, Theorem 2.4(i)], and in this case $a = 0$ (by [Is3, Corollary 2.13]) – a contradiction. This proves the claim. Hence, $b \geq 1$. By Lemma 4.2(ii), we conclude that $a = b$.

We want to study the field of values of the character

$$\Delta = \sum_{x \in \mathbf{N}_G(P)} \lambda^x (\hat{\theta}_P)^x .$$

We claim that

$$\mathbb{Q}(\Delta) = \mathbb{Q}(\sum_{x \in \mathbf{N}_G(P)} \lambda^x).$$

Set $y \in P$. Then $\hat{\theta}(y) = \epsilon_y \theta_y(1)$, where ϵ_y is a sign and $\theta_y \in \mathrm{Irr}(\mathbf{C}_G(y))$ is the $\langle y \rangle$-Glauberman correspondent of θ (by [Is2, Theorems 13.6 and 13.14]). Notice that $(\theta_y)^x = \theta_{y^x}$ and $\epsilon_y = \epsilon_{y^x}$ for $y \in P$ and $x \in \mathbf{N}_G(P)$ (by the uniqueness in [Is2, Theorem 13.6]). Also, $(\hat{\theta}^x) = \widehat{\theta^x}$ for $x \in \mathbf{N}_G(P)$, this time by the uniqueness of canonical extensions.

Thus,

$$\mathbb{Q}(\Delta) = \mathbb{Q}(\sum_{x \in \mathbf{N}_G(P)} \lambda^x(y)\hat{\theta}(y^{x^{-1}}) \mid y \in P) =$$

$$\mathbb{Q}(\epsilon_y \theta_y(1) \sum_{x \in \mathbf{N}_G(P)} \lambda^x(y) \mid y \in P) = \mathbb{Q}(\sum_{x \in \mathbf{N}_G(P)} \lambda^x)),$$

as claimed. Now, if $\psi \in \mathrm{Irr}(\mathbf{N}_G(P))$ lies over λ, we have $\mathbb{Q}(\psi_P) = \mathbb{Q}(\Delta) = \mathbb{Q}(\chi_P)$ and we apply Theorem 7.3. □

Next we make a few remarks concerning the Galois–McKay conjecture. As formulated in [N2, Conjecture 9.8] (or at the end of [N1]), this proposes that if G is a finite group of order n, $P \in \mathrm{Syl}_p(G)$ and $\mathcal{H}$ is the subgroup of $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})$ that sends p'-roots of unity to some arbitrary p-power, then there should exist a bijection

$$^* : \mathrm{Irr}_{p'}(G) \to \mathrm{Irr}_{p'}(\mathbf{N}_G(P))$$

that commutes with the action of $\mathcal{H}$. Now let $\mathbb{F}$ be the fixed field in $\mathbb{Q}_n$ by $\mathcal{H}$. (Notice that if $m = n_{p'}$, then $\mathbb{F}$ is the fixed field in $\mathbb{Q}_m$ of the subgroup generated by the *Frobenius automorphism* $\xi \mapsto \xi^p$, where ξ is any m-root of unity.) Since $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{F}) = \mathcal{H}$, by elementary Galois theory it easily follows that the Galois–McKay conjecture is equivalent to showing that $\mathbb{F}(\chi) = \mathbb{F}(\chi^*)$ for all $\chi \in \mathrm{Irr}_{p'}(G)$. (If $\mathbf{Q}_p$ is the field of p-adic numbers, it can be proved that this is equivalent to showing that $\mathbf{Q}_p(\chi) = \mathbf{Q}_p(\chi^*)$ for all $\chi \in \mathrm{Irr}_{p'}(G)$.)

We find it interesting to study the class of finite groups for which the bijection * in the Galois–McKay conjecture can be strengthened in the following way:

Condition D. *Let G be a finite group and p a prime, and set $P \in \mathrm{Syl}_p(G)$. Then there exists a bijection $^* : \mathrm{Irr}_{p'}(G) \to \mathrm{Irr}_{p'}(\mathbf{N}_G(P))$ such that $\mathbb{Q}(\chi_P) = \mathbb{Q}(\chi^*|_P)$ and $\mathbf{Q}_p(\chi) = \mathbf{Q}_p(\chi^*)$ for all $\chi \in \mathrm{Irr}_{p'}(G)$.*

Suppose that Condition D holds for G and consider any $\chi \in \mathrm{Irr}_{p'}(G)$. Since $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}_m) \leq \mathcal{H}$, we easily deduce that the Galois–McKay conjecture implies that χ is p-rational if and only if χ^* is p-rational. (More than that, it implies that $c(\chi)$ and $c(\chi^*)$ have the same p-part.) In the case where χ is p-rational, notice that χ_P (and $\chi^*|_P$) is rational-valued, so Condition D, for p-rational characters, follows from the Galois–McKay conjecture. Once χ is not p-rational, Condition D is new territory. We remark that the restriction $\chi^*|_P$ is well understood: it is a sum of $\mathbf{N}_G(P)$-conjugate linear characters of P. However, in general, notice that χ_P might contain irreducible characters of P of degree divisible by p, and constituents with different multiplicities. We believe that studying the character χ_P is of interest.

We caution the reader that Condition D does *not* always hold. We thank B. Sambale for communicating to us that $G = \mathrm{PrimitiveGroup}(64, 38)$ (in the notation of [GAP]) for $p = 3$ is an example. (This group is not a counterexample to Conjecture C.) On the other hand, as we will show, Condition D does hold for many interesting classes of finite groups, so it might be worth exploring further.

We show now that Condition D implies Conjecture C.

Theorem 7.8. *Condition D implies Conjecture C.*

Proof. Let G be a finite group of order n and p a prime, set $P \in \mathrm{Syl}_p(G)$ and let $N = \mathbf{N}_G(P)$. Let $\mathcal{G} = \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})$. Let $\mathcal{H}$ be the subgroup of Galois automorphisms that send every p'-root of unity in $\mathbb{Q}_n$ to some fixed but arbitrary p-power. Let $\mathbb{F}$ be the fixed field of $\mathcal{H}$. Assume that there is a bijection

$$^* : \mathrm{Irr}_{p'}(G) \to \mathrm{Irr}_{p'}(N)$$

such that $\mathbb{F}(\chi) = \mathbb{F}(\chi^*)$ – or equivalently, that commutes with the action of $\mathcal{H}$. Since $\sigma_e \in \mathcal{H}$ for every e, we have that the p-parts of the conductors of χ and χ^* are the same, say p^a, where $\chi \in \mathrm{Irr}_{p'}(G)$. Now if $\mathbb{Q}(\chi_P) = \mathbb{Q}(\chi^*|_P)$, then $[\mathbb{Q}_{p^a} : \mathbb{Q}(\chi_P)] = [\mathbb{Q}_{p^a} : \mathbb{Q}(\chi^*|_P)]$. By Theorem 7.3, this latter number is not divisible by p. □

Next we present several classes of finite groups which satisfy Condition D.

Theorem 7.9. *Condition D holds in the following cases:*

(i) *G has a cyclic Sylow p-subgroup P.*
(ii) *G has a self-normalising Sylow p-subgroup P, and either p is odd or G is solvable.*
(iii) *G has a normal p-complement.*
(iv) *G is a sporadic simple group.*
(v) *$p = 2$, $P \in \mathrm{Syl}_2(G)$ is self-normalising and P/P' is elementary abelian.*
(vi) *$p = 2$ and $G = \mathsf{S}_n$ or $G = \mathsf{A}_n$ with $n \geq 5$.*
(vii) *p is any prime and $G = \mathsf{S}_n$.*
(viii) *$p = 2 \nmid q$ and $G = \mathrm{GL}_n(q)$ or $G = \mathrm{GU}_n(q)$.*

Proof. (i) We have that $\mathrm{Irr}_{p'}(G)$ is a union of $\mathrm{Irr}_{p'}(B)$ for p-blocks B of G of maximal defect. Let us fix a block B of maximal defect of G, and let b be the Brauer first main correspondent in $\mathbf{N}_G(P)$. Write $|P| = p^a$. By [N1, Theorem 3.4], there is a bijection $^* : \mathrm{Irr}_{p'}(B) \to \mathrm{Irr}_{p'}(b)$ that commutes with σ for all $\sigma \in \mathcal{H}_B$. (Here $\mathcal{H}$ is the subgroup of Galois automorphisms of $\mathrm{Gal}(\mathbb{Q}_{|G|}/\mathbb{Q})$ that send p'-roots of unity to a fixed but arbitrary p-power, and $\mathcal{H}_B$ the stabiliser in $\mathcal{H}$ of B.) This naturally defines an $\mathcal{H}$-equivariant bijection $^* : \mathrm{Irr}_{p'}(G) \to \mathrm{Irr}_{p'}(\mathbf{N}_G(P))$. We only need to check that $\mathbb{Q}(\chi_P) = \mathbb{Q}(\chi^*|_P)$. Now let us use the notation given in the paragraph preceding [N1, Theorem 3.4]. Suppose first that $|\Delta| = 1$.

Then $a = 1$ and $e = p - 1$. By the formulas in [D1, Corollary 1.9], we have that χ_P is rational-valued for every $\chi \in \mathrm{Irr}(B)$ (and for the same reason, so is $\chi^*|_P$). Hence, (i) is proved. Assume that $|\Delta| > 1$, and divide $\mathrm{Irr}(B)$ into nonexceptional and exceptional characters. The bijection * sends exceptional (resp., nonexceptional) characters of $\mathrm{Irr}(B)$ onto exceptionals (resp., nonexceptionals) of $\mathrm{Irr}(b)$. Now if χ is nonexceptional, then $\mathbb{Q}(\chi_P) = \mathbb{Q}$ (again by [D1, Corollary 1.9]), and there is nothing else to prove. The arguments in [N1, Theorem 3.4] (together with [D3]) show that we may label the exceptional characters in B as $\{\chi_\lambda \mid \lambda \in \Delta\}$, and the exceptional characters in b as $\{\tilde{\chi}_\lambda \mid \lambda \in \Delta\}$ such that $(\chi_\lambda)^* = \tilde{\chi}_\lambda$, and both satisfy the formulas in [D1, Corollary 1.9]. In particular, we have that $\chi_\lambda(x)$ is a rational multiple of $\tilde{\chi}_\lambda(x)$ for every $x \in P$. Therefore $\mathbb{Q}(\chi_P) = \mathbb{Q}(\chi^*|_P)$ for all $\chi \in \mathrm{Irr}(B)$.

(ii) When $\mathbf{N}_G(P) = P$, by [NTV, Corollary B] in the case where p is odd and by [N2, Theorem 9.4] in the case where G is solvable, there is a natural bijection $\chi \mapsto \chi^*$ between $\mathrm{Irr}_{p'}(G)$ and the set of linear characters of P; in fact, χ^* is the unique linear constituent of χ_P. Such a map commutes with the action of *any* Galois automorphism in $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, and hence $\mathbb{Q}(\chi) = \mathbb{Q}(\chi^*)$. Next, suppose that $\gamma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ fixes χ^*. Then χ^* is the (unique) linear constituent of $(\chi^\gamma)_P$, whence $\chi^* = (\chi^\gamma)^*$ and so $\chi = \chi^\gamma$. This implies that

$$\mathbb{Q}(\chi_P) \subseteq \mathbb{Q}(\chi) \subseteq \mathbb{Q}(\chi^*).$$

Now assume that $\gamma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ fixes χ_P. Then $(\chi^*)^\gamma$ is the (unique) linear constituent of χ_P, whence $(\chi^*)^\gamma = \chi^*$. Thus $\mathbb{Q}(\chi^*) \subseteq \mathbb{Q}(\chi_P)$, and so $\mathbb{Q}(\chi_P) = \mathbb{Q}(\chi^*)$, as stated.

(iii) Suppose that G has a normal p-complement K and a Sylow p-subgroup P. By [N2, Theorem 9.2], there exists a canonical bijection $^* : \mathrm{Irr}_{p'}(G) \longrightarrow \mathrm{Irr}_{p'}(\mathbf{N}_G(P))$ such that $\mathbb{Q}(\chi) = \mathbb{Q}(\chi^*)$ for every $\chi \in \mathrm{Irr}_{p'}(G)$. Furthermore, if $\chi_K = \theta$, then $\chi = \hat{\theta}\lambda$, where $\hat{\theta}$ is the canonical extension of θ to G [N2, Corollary 6.4] and $\lambda \in \mathrm{Irr}(G/K)$ is linear. Now $\mathbb{Q}(\theta) = \mathbb{Q}(\hat{\theta})$, and we deduce that $\hat{\theta}$ is p-rational. Therefore $\hat{\theta}(x) \in \mathbb{Q}$ for all $x \in P$. Also $\hat{\theta}(x) \neq 0$, by [N2, Corollary 4.20]. Now $\mathbb{Q}((\hat{\theta}\lambda)|_P) = \mathbb{Q}(\lambda)$. Since $\chi^* = (\theta^* \times \lambda)$, where θ^* is the P-Glauberman correspondent of θ, we deduce that $\mathbb{Q}(\chi^*|_P) = \mathbb{Q}(\lambda)$, as desired.

(iv) Most of the character tables of the Sylow normalisers of the sporadic simple groups are given in [GAP], but not all. The Galois–McKay conjecture was proved for the sporadic groups in [Tu, Theorem 3.1]. As remarked before, Condition D is equivalent to Galois–McKay for p-rational characters. The only case of a Sylow normaliser $\mathbf{N}_G(P)$ of a sporadic group possessing non-p-rational characters and whose Sylow normaliser is not given in [GAP] is Th for $p = 3$. The group $\mathbf{N}_G(P)/P'$, as described in [Wi], is `SmallGroup`(108,40), and we check that Condition D holds in this case using [GAP].

(v) By [ILNT, Theorem D], since P/P' is elementary abelian, all odd-degree irreducible characters of G are 2-rational, and the same holds for $\mathbf{N}_G(P) = P$. Hence, by the main result of [SF], all odd-degree irreducible characters of G are $\mathcal{H}$-invariant, and again the same holds for P. It remains to apply the main result of [MS] guaranteeing the existence of a McKay bijection.

(vi) Since the statement is obvious for $n = 5$, we may assume that $n \geq 6$. Hence $P \in \mathrm{Syl}_2(G)$ is self-normalising (see, for example, [Ko, Theorem 2]. Furthermore, P/P' is elementary abelian by [NT2, Lemma 3.3]. Hence we are done, by using (v).

(vii) Let ς denote the Galois automorphism of $\mathrm{Gal}(\mathbb{Q}_{|G|_{p'}}/\mathbb{Q})$ that sends any p'-root of unity to its p-power. Since the McKay conjecture holds for G [O] and since G is rational, it suffices to show that any $\psi \in \mathrm{Irr}_{p'}(\mathbf{N}_G(P))$ is rational on $P \in \mathrm{Syl}_p(G)$, and moreover is p-rational and ς-invariant. We will do it in steps. First, if $n = p$, then $N_1 := \mathbf{N}_{\mathsf{S}_p}(C_p) \cong C_p \rtimes C_{p-1}$; in particular, every element of C_p is rational in N_1 and any $\psi \in \mathrm{Irr}(N_1)$ is p-rational and ς-invariant, whence the claim follows. Next, in the case where $n = p^k$, we have $N_k := \mathbf{N}_{\mathsf{S}_{p^k}}(P)/P' \cong (N_1)^k$ by [O, Proposition (1.5)] using induction on $k \geq 1$, and so the claim follows from the case $n = p$. Now, if $n = ap^k$ with $1 \leq a < p$ and $k \geq 1$, then

$$P \cong Q^a, \ \mathbf{N}_G(P) \cong N_k \wr \mathsf{S}_a$$

for a suitable $Q \in \mathrm{Syl}_p(\mathsf{S}_{p^k})$. By the previous case (and the representation theory of wreath products [JK, §4.4]), every irreducible constituent of $\psi|_{(N_k)^a}$ is rational on P, and ψ is again p-rational and

ς-invariant. Finally, if $n = \sum_{i=0}^{t} a_i p^i$ is the p-adic decomposition of n, then

$$P = \prod_{i: a_i \neq 0} P_i, \; \mathbf{N}_G(P) = \prod_{i: a_i \neq 0} \mathbf{N}_{\mathsf{S}_{a_i p^i}}(P_i)$$

for suitable $P_i \in \mathrm{Syl}_p(\mathsf{S}_{a_i p^i})$ (and after suitably conjugating P). Hence the claim follows from the preceding case.

(viii) We will use the canonical McKay bijection $\chi \mapsto \chi^\sharp$ between $\mathrm{Irr}_{2'}(G)$ and $\mathrm{Irr}_{2'}(\mathbf{N}_G(P))$ for $P \in \mathrm{Syl}_2(G)$ constructed in [GKNT, Theorem 5.3]. As mentioned in [GKNT, Theorem E], this bijection commutes with Galois automorphisms, and so $\mathbb{Q}(\chi) = \mathbb{Q}(\chi^\sharp)$, hence it remains to show that $\mathbb{Q}(\chi_P) = \mathbb{Q}(\chi^\sharp\,|_P)$ for any $\chi \in \mathrm{Irr}_{2'}(G)$. To unify the notation, we will again write GL^ϵ for GL when $\epsilon = +1$ and for GU when $\epsilon = -1$. Also decompose

$$n = 2^{m_1} + 2^{m_2} + \cdots + 2^{m_r}$$

with $m_1 > m_2 > \cdots > m_r \geq 0$ as in equation (5.1). Then we can choose $P_i \in \mathrm{Syl}_2(G_i)$, where $G_i = \mathrm{GL}^\epsilon_{2^{m_i}}(q)$, and embed $G_1 \times G_2 \times \cdots \times G_r$ in G such that we can identify P with $P_1 \times P_2 \times \cdots \times P_r$ and then have

$$\mathbf{N}_G(P) = \mathbf{N}_{G_1}(P_1) \times \mathbf{N}_{G_2}(P_2) \times \cdots \times \mathbf{N}_{G_r}(P_r) \tag{7.1}$$

(see [GKNT, (5.5)]).

On the global side, we can write

$$\chi = S(s_1, \lambda_1) \circ S(s_2, \lambda_2) \circ \cdots \circ S(s_k, \lambda_k),$$

as in Lemma 5.5(ii). Recall that $s_i \in \mu_{q-\epsilon}$ for $1 \leq i \leq k$; let 2^c denote the smallest 2-part of $[s_i]$, $1 \leq i \leq k$. Then $\mathbb{Q}(\chi_P) = \mathbb{Q}_{2^{a-c}}$ by Proposition 5.8. Rephrasing it, we have $\mathbb{Q}(\chi_P) = \mathbb{Q}_{2^d}$, where 2^d is the largest 2-part of the orders of s_i, $1 \leq i \leq k$. In terms of the α-map in the proof of [GKNT, Theorem 5.3], we note that 2^d is the largest 2-part of the orders of $\hat{s}_i \in \mu_{q-\epsilon}$, $1 \leq i \leq r$, if

$$\alpha(\chi) = (\hat{s}_1, \nu_1, \hat{s}_2, \nu_2, \ldots, \hat{s}_r, \nu_r).$$

On the local side, in accordance with equation (7.1), we consider $\theta = \theta_1 \otimes \theta_2 \otimes \cdots \otimes \theta_r$, where $\theta_i \in \mathrm{Irr}_{2'}(\mathbf{N}_{G_i}(P_i))$. Note by [GKNT, (5.3)] that

$$\mathbf{N}_{G_i}(P_i) = Z_i \times P_i, \tag{7.2}$$

where Z_i is a central $2'$-group. Now the β-map in the proof of [GKNT, Theorem 5.3] is constructed such that

$$\beta(\theta) = (\hat{t}_1, \mu_1, \hat{t}_2, \mu_2, \ldots, \hat{t}_r, \mu_r)$$

if $\beta(\theta_i) = (\hat{t}_i, \mu_i)$ and $\hat{t}_i \in \mu_{q-\epsilon}$. We also note that $\mathbb{Q}((\theta_i)_{P_i}) = \mathbb{Q}_{2^{d_i}}$, where 2^{d_i} is the 2-part of the order of $\hat{t}_i$. (Indeed, this is the case if $q \equiv -\epsilon(\bmod 4)$, since the map β commutes with Galois automorphisms by [GKNT, Lemma 5.1]. Assume now that $4|(q-\epsilon)$. Analyzing the proof of [GKNT, Lemma 5.1] in this case, we see that $\mathbb{Q}((\theta_i)_{P_i}) = \mathbb{Q}(\gamma)$ for some linear character γ of $\mathbf{O}_2(\mu_{q-\epsilon})$, whose order is precisely 2^{d_i}.) It now follows from equations (7.1) and (7.2) that

$$\mathbb{Q}(\theta_P) = \mathbb{Q}_{2^{\max_{1 \leq i \leq r} d_i}},$$

and $2^{\max_{1 \leq i \leq r} d_i}$ is certainly the largest 2-part of the orders of $\hat{t}_i$, $1 \leq i \leq r$.

Since $\chi^\sharp = \beta^{-1}\alpha(\chi)$ by [GKNT, Theorem E], we conclude that $\mathbb{Q}(\chi_P) = \mathbb{Q}(\chi^\sharp|_P)$, as desired. □

We also mention that E. Giannelli [Gi] has proved that Condition D (and a blockwise version of it) holds for A_n for any odd prime p.

In the next result, we will show that Condition D holds for certain finite groups of Lie type in defining characteristic. Let $\mathcal{G}$ be a simple, simply connected algebraic group over an algebraically closed field of characteristic p, and let $F : \mathcal{G} \to \mathcal{G}$ be a Steinberg endomorphism. Consider the regular embedding of $(\mathcal{G}, F)$ in $(\tilde{\mathcal{G}}, F)$, as discussed in [R, §4.1]. Then $\mathcal{G}^F$ embeds in $\tilde{\mathcal{G}}^F$. Note that the latter groups include the general linear group $\mathrm{GL}_n(q)$, the general unitary group $\mathrm{GU}_n(q)$, the conformal symplectic group $\mathrm{CSp}_{2n}(q)$ when $2 \nmid q$ and $\mathrm{Sp}_{2n}(q)$ when $2|q$, the conformal spin groups $\mathrm{CSpin}^{\epsilon}_n(q)$ when $2 \nmid q$ and furthermore $\epsilon \neq +$ when $2|n$, the orthogonal groups $\Omega^{\pm}_{2n}(q)$ when $2|q$ and $G_2(q)$, ${}^2F_4(q)$ with $q = 2^{2a+1}$, $F_4(q)$ and $E_8(q)$.

Proposition 7.10. *In the introduced notation, Condition D holds for* $(\tilde{\mathcal{G}}^F, p)$.

Proof. If $\tilde{\mathcal{G}}^F = G_2(3)$, $F_4(2)$ or ${}^2F_4(2)$, this claim can be checked using [GAP]. Henceforth, we may assume that $\tilde{\mathcal{G}}^F \neq G_2(3), F_4(2), {}^2F_4(2)$. Under this extra assumption, [R, Theorem 5.2] yields an $\mathcal{H}$-equivariant McKay bijection $\chi \mapsto \chi^*$ for $(\tilde{\mathcal{G}}^F, p)$ in all the cases already listed. Hence, as we discussed before Theorem 7.8, to verify Condition D it suffices to prove that all $\chi \in \mathrm{Irr}_{p'}(\tilde{\mathcal{G}}^F)$ are p-rational. This follows from [TZ, Theorem 1.9(i)(i)] if p is a good prime and q is a square, where $q = q(F)$ denotes the common absolute value of eigenvalues of F on the character group of an F-stable maximally split maximal torus of $\mathcal{G}$. If $q = 2$ and $\mathcal{G}$ is of type A_n, BC_n or D_n, then $\tilde{\mathcal{G}}^F = \mathrm{GL}^{\pm}_{n+1}(q)$, $\mathrm{Sp}_{2n}(q)$, $\Omega^{\pm}_{2n}(q)$ or ${}^3D_4(q)$, and we can apply [TZ, Theorem 1.9(i)(ii)] – or we can argue directly when $\tilde{\mathcal{G}}^F \in \{B_2(2) \cong \mathsf{S}_6, {}^2B_2(2) \cong C_5 \rtimes C_4\}$.

Thus we may assume furthermore that $q > 2$ if $\mathcal{G}$ is classical and $p = 2$. Now let $(\tilde{\mathcal{G}}^*, F^*)$ be dual to $(\tilde{\mathcal{G}}, F)$. Since $\tilde{\mathcal{G}}$ has connected centre, every semisimple element $s \in (\tilde{\mathcal{G}}^*)^{F^*}$ has connected centraliser. Then by [M, Theorem 6.8], the only p'-degree unipotent character of $\mathbf{C}_{(\tilde{\mathcal{G}}^*)^{F^*}}(s)$ is the principal character. The Lusztig classification of irreducible characters of $\tilde{\mathcal{G}}^F$ implies that the p'-degree characters $\chi \in \mathrm{Irr}_{p'}(\tilde{\mathcal{G}}^F)$ are precisely the semisimple characters, one for each semisimple class in $(\tilde{\mathcal{G}}^*)^{F^*}$. The claim now follows, since it is well known that semisimple characters are p-rational (see, for example, [C, Theorem 7.2.8 and Proposition 8.4.6] and use the fact that the Green functions are integer-valued [C, p. 237]). □

Added in proof. Conjecture C for p-solvable groups has now been proved by M. Isaacs and the first author (work in progress). It looks plausible that Condition D, with $\mathbb{Q}$ replaced by $\mathbb{Q}_p$, might hold true for arbitrary finite groups.

Acknowledgements. The work on this paper started when the first author visited the Department of Mathematics, Rutgers University, in spring 2019. It was continued while both authors visited the Mathematisches Forschungsinstitut Oberwolfach in February 2020 and the second author visited the Isaac Newton Institute for Mathematical Sciences in March 2020. It is a pleasure to thank the Rutgers Mathematics Department, the Mathematisches Forschungsinstitut Oberwolfach and the Isaac Newton Institute for hospitality and support.

The authors thank Eugenio Giannelli, Martin Liebeck and Gunter Malle for useful discussions, and Thomas Breuer for helping them with some calculations. Special thanks are due to Gunter Malle for a thorough reading of the manuscript and helpful comments.

The authors thank the referee for careful reading and many comments that helped improve the exposition of the paper.

Conflict of Interest: None.

Financial support. The research of the first author is supported by the Ministerio de Ciencia e Innovación PID2019-103854GB-I00 and FEDER funds. The second author gratefully acknowledges the support of the NSF (grant DMS-1840702), the Joshua Barlaz Chair in Mathematics, and the Charles Simonyi Endowment at the Institute for Advanced Study (Princeton).

References

[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).

[C] R. Carter, *Finite Groups of Lie type: Conjugacy Classes and Complex Characters* (Wiley, Chichester, 1985).

[D1] E. C. Dade, 'Blocks with cyclic defect groups', *Ann. of Math.* **84** (1966), 20–48.

[D3] E. C. Dade, 'Counting characters in blocks with cyclic defect groups, I', *J. Algebra* **186** (1996), 934–969.

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

[FG] B. Fein and B. Gordon, 'Fields generated by characters of finite groups', *J. Lond. Math. Soc.* 4 (1972), 735–740.

[GAP] The GAP Group, 'GAP – groups, algorithms, and programming', version 4.10.0 (2018). URL: http://www.gap-system.org.

[Gi] E. Giannelli, 'The Sylow restriction refinement of the McKay conjecture for symmetric and alternating groups', Algebra Number Theory, 2021 (to appear).

[GKNT] E. Giannelli, A. S. Kleshchev, G. Navarro and P. H. Tiep, 'Restriction of odd degree characters and natural correspondences', *Int. Math. Res. Not. IMRN* **2017** (20), 6089–6118.

[GLBST] R. M. Guralnick, M. W. Liebeck, E. O'Brien, A. Shalev and P. H . Tiep, 'Surjective word maps and Burnside's $p^a q^b$ theorem', *Invent. Math.* **213** (2018), 589–695.

[GM] M. Geck and G. Malle, *The Character Theory of Finite Groups of Lie Type: A Guided Tour*, Cambridge Studies in Advanced Mathematics (Cambridge University Press, 2020).

[GT] R. M. Guralnick and P. H. Tiep, 'Low-dimensional representations of special linear groups in cross characteristic', *Proc. Lond. Math. Soc.* **78** (1999), 116–138.

[HH] P. N. Hoffman and J. F. Humphreys, *Projective Representations of the Symmetric Group* (Clarendon Press, Oxford, 1992).

[ILNT] I. M. Isaacs, M. Liebeck, G. Navarro and P. H . Tiep, 'Fields of values of odd degree irreducible characters', *Adv. Math.* **354** (2019), 106757.

[Is1] I. M Isaacs, 'Characters of solvable and symplectic groups', *Amer. J. Math.* **85** (1973), 594–635.

[Is2] I. M. Isaacs, *Character Theory of Finite Groups* (American Mathematical Society, Providence, RI, 2008).

[Is3] I. M. Isaacs, *Characters of Solvable Groups* (American Mathematical Society, Providence, RI, 2018).

[JK] G. James and A. Kerber, *The Representation Theory of the Symmetric Group*, Encyclopedia of Mathematics and Its Applications, **16** (Addison-Wesley, Reading, MA, 1981).

[Ko] A. S. Kondrat'ev, 'Normalizers of the Sylow 2-subgroups in finite simple groups', *Math. Notes* **78** (2005), 338–346.

[LSS] M. W. Liebeck, J. Saxl and G. Seitz, 'Subgroups of maximal rank in finite exceptional groups of Lie type', *Proc. Lond. Math. Soc.* **65** (1992), 297–325.

[Lu] F. Lübeck, 'Character degrees and their multiplicities for some groups of Lie type of rank < 9', URL: http://www.math.rwth-aachen.de/~Frank.Luebeck/chev/DegMult/index.html.

[M] G. Malle, 'Height 0 characters of finite groups of Lie type', *Represent. Theory* **11** (2007), 192–220.

[MS] G. Malle and B. Späth, 'Characters of odd degree', *Ann. of Math.* **184** (2016), 869–908.

[N1] G. Navarro, 'The McKay conjecture and Galois automorphisms', *Ann. of Math.* **160** (2004), 1129–1140.

[N2] G. Navarro, *Character Theory and the McKay Conjecture* (Cambridge University Press, Cambridge, 2018).

[NT1] G. Navarro and P. H. Tiep, 'Rational irreducible characters and rational conjugacy classes in finite groups', *Trans. Amer. Math. Soc.* **360** (2008), 2443–2465.

[NT2] G. Navarro and P. H. Tiep, 'Real groups and Sylow 2-subgroups', *Adv. Math.* **299** (2016), 331–360.

[NT3] G. Navarro and P. H. Tiep, 'Irreducible representations of odd degree', *Math. Ann.* **365** (2016), 1155–1185.

[NT4] G. Navarro and P. H. Tiep, 'Sylow subgroups, exponents, *and character tables', Trans. Amer. Math. Soc.* **372** (2019), 4263–4291.

[NTV] G. Navarro, P. H. Tiep and C. Vallejo, 'McKay natural correspondences on characters', *Algebra Number Theory* **8** (2014), 1839–1856.

[O] J. B. Olsson, 'McKay numbers and heights of characters', *Math. Scand.* **38** (1976), 25–42.

[R] L. Ruhstorfer, 'The Navarro refinement of the McKay conjecture for finite groups of Lie type in defining characteristic', Preprint, 2020, arXiv:1703.09006.

[SF] A. A. Schaeffer-Fry, 'Actions of Galois automorphisms on Harish-Chandra series and Navarro's self-normalizing Sylow 2-subgroup conjecture', *Trans. Amer. Math. Soc.* **372** (2019), 457–483.

[ST] A. A. Schaeffer-Fry and J. Taylor, 'On self-normalising Sylow 2-subgroups in type *A*', *J. Lie Theory* **28** (2018), 139–168.

[Tu] A. Turull, 'Strengthening the McKay conjecture to include local fields and local Schur indices', *J. Algebra* **319** (2008), 4853–4868.

[TZ] P. H. Tiep and A. E. Zalesskii, 'Unipotent elements of finite groups of Lie type and realization fields of their complex representations', *J. Algebra* **271** (2004), 327–390.

[We] S. H. Weintraub, *Galois Theory*, Universitext (Springer, New York 2009).

[Wi] R. A. Wilson, 'The McKay conjecture is true for the sporadic simple groups', *J. Algebra* **207** (1998), 294–305.