FIELDS OF VALUES OF ODD-DEGREE IRREDUCIBLE CHARACTERS

I. M. ISAACS, M. W. LIEBECK, GABRIEL NAVARRO, AND PHAM HUU TIEP

Abstract. In this paper we clarify the quadratic irrationalities that can be admitted by an odd-degree complex irreducible character χ of an arbitrary finite group. Write $\mathbb{Q}(\chi)$ to denote the field generated over the rational numbers by the values of χ, and let $d > 1$ be a square-free integer. We prove that if $\mathbb{Q}(\chi) = \mathbb{Q}(\sqrt{d})$ then $d \equiv 1 \pmod 4$ and if $\mathbb{Q}(\chi) = \mathbb{Q}(\sqrt{-d})$, then $d \equiv 3 \pmod 4$. This follows from the main result of this paper: either $i \in \mathbb{Q}(\chi)$ or $\mathbb{Q}(\chi) \subseteq \mathbb{Q}(\exp(2\pi i/m))$ for some odd integer $m \geq 1$.

1. Introduction

Browsing through character tables of finite groups, one never encounters an odd-degree irreducible character with field of values $\mathbb{Q}(\sqrt{2})$ or $\mathbb{Q}(\sqrt{-2})$. Of course, $\mathbb{Q}(\sqrt{-3})$ occurs as the field of values of a linear character of order 3, but no example of $\mathbb{Q}(\sqrt{3})$ is found. Also, although the alternating group A_5 has odd-degree irreducible characters whose field of values is $\mathbb{Q}(\sqrt{5})$, it seems that $\mathbb{Q}(\sqrt{-5})$ shows up as the field of values only for certain even-degree irreducible characters. A pattern is emerging, and one naively thinks that such a simple-to-state fact should have an easy proof.

Recall that if $\chi \in \mathrm{Irr}(G)$ is an irreducible complex character of a finite group G, then $\mathbb{Q}(\chi)$ denotes the field of values of χ, that is, the field generated over $\mathbb{Q}$ by the values of χ.

Theorem A. *Let G be a finite group, and let $\chi \in \mathrm{Irr}(G)$, where $\chi(1)$ is odd. Also, let $d > 1$ be a square-free integer.*

(a) *If $\mathbb{Q}(\chi) = \mathbb{Q}(\sqrt{d})$ then $d \equiv 1 \pmod 4$.*
(b) *If $\mathbb{Q}(\chi) = \mathbb{Q}(\sqrt{-d})$ then $d \equiv 3 \pmod 4$.*

Of course, since d is square-free, we cannot have $d \equiv 0 \pmod 4$, but note that it is a consequence of Theorem A that if $d \equiv 2 \pmod 4$, then $\mathbb{Q}(\chi)$ cannot be either $\mathbb{Q}(\sqrt{d})$ or $\mathbb{Q}(\sqrt{-d})$.

2010 *Mathematics Subject Classification.* Primary 20C15, 20C33.

Key words and phrases. Character values, rationality.

The research of the third author is supported by the Prometeo/Generalitat Valenciana, Proyecto MTM2016-76196-P and FEDER funds. The fourth author gratefully acknowledges the support of the NSF (grant DMS-1840702), and the Joshua Barlaz Chair in Mathematics. The authors are also grateful to R. M. Guralnick, F. Lübeck, and R. Lyons for helpful discussions.

The authors are grateful to the referees for several comments that helped greatly improve the exposition of the paper, in particular the proof of Theorem B.

Note that both (a) and (b) of Theorem A can occur. Consider, for example, $G = \mathrm{PSL}_2(p)$, where p is an odd prime. If $p \equiv 1 \pmod 4$, there exists $\chi \in \mathrm{Irr}(G)$ with $\chi(1) = (p+1)/2$, and $\mathbb{Q}(\chi) = \mathbb{Q}(\sqrt{p})$. If $p \equiv 3 \pmod 4$, however, there exists $\chi \in \mathrm{Irr}(G)$ with $\chi(1) = (p-1)/2$ and $\mathbb{Q}(\chi) = \mathbb{Q}(\sqrt{-p})$.

The key to our proof of Theorem A is to consider separately the cases where the character χ is or is not 2-rational. (Recall that a character χ is said to be 2-*rational* if $\mathbb{Q}(\chi)$ is contained in some cyclotomic field $\mathbb{Q}_m = \mathbb{Q}(\exp(2\pi i/m))$, where m is odd and $i = \sqrt{-1}$.)

Let $d > 1$ be an odd integer. For notational convenience, we write $\epsilon_d = \pm 1$, where $\epsilon_d \equiv d (\mathrm{mod}\, 4)$. (Equivalently, $\epsilon_d = (-1)^{(d-1)/2}$.) Using this notation, we can offer a more complete version of Theorem A.

Theorem B. *Let $\gamma = \sqrt{\epsilon d}$, where $\epsilon = \pm 1$ and $d > 1$ is a square-free integer, and let χ be a character of some finite group G.*

(a) *If χ is 2-rational and $\gamma \in \mathbb{Q}(\chi)$, then d is odd, and $\epsilon = \epsilon_d$.*
(b) *If χ is not 2-rational and it is irreducible of odd degree, then $i \in \mathbb{Q}(\chi)$ and $\mathbb{Q}(\chi) \neq \mathbb{Q}(\gamma)$.*

To see why Theorem A is a consequence of Theorem B, observe that in Theorem A, we are assuming that $\mathbb{Q}(\chi) = \mathbb{Q}(\gamma)$, where $\gamma = \sqrt{\epsilon d}$ for some sign ϵ and square-free integer $d > 1$. Theorem B(b) guarantees that χ is 2-rational, and by Theorem B(a) we see that d is odd and $\epsilon = \epsilon_d$, as required for Theorem A.

Theorem B is an easy consequence of the following main result of this paper, whose proof relies on the simple group classification.

Theorem C. *Suppose that G is a finite group, and $\chi \in \mathrm{Irr}(G)$ has odd degree. If χ is not 2-rational, then $i \in \mathbb{Q}(\chi)$.*

We will need the following result, which follows from results of [NT3] and [M], and whose proof also relies on the simple group classification.

Theorem D. *Let G be a finite group with a Sylow 2-subgroup P. Then $\exp(P/P') \le 2$ if and only if all odd-degree irreducible characters of G are 2-rational.*

Finally, we will also need to establish the following result on quasi-simple groups. Recall that G is said to be *quasi-simple* if G is perfect and $G/\mathbf{Z}(G)$ is a simple group.

Theorem E. *Suppose that G is a quasi-simple finite group. Assume that $\chi \in \mathrm{Irr}(G)$ has odd degree and is not 2-rational. Then there exists a 2-element $g \in G$ such that $i \in \mathbb{Q}(\chi(g))$.*

Note that in Theorem E, we show not only that $i \in \mathbb{Q}(\chi)$, which establishes Theorem C for quasi-simple groups, but also, we prove more: that $i \in \mathbb{Q}(\chi(g))$ for some 2-element g of G. This suggests the possibility that Theorem C could be strengthened to show for an arbitrary finite group G that if $\chi \in \mathrm{Irr}(G)$ has odd degree and is not 2-rational, then $i \in \mathbb{Q}(\chi(g))$ for some 2-element $g \in G$. It is not clear, however, even for solvable groups, if this enhanced version of Theorem C is true, but not surprisingly, the original statement of Theorem C can be proved for solvable groups without appealing to the simple group classification. In fact, the enhanced version of this theorem holds for groups G having a normal Sylow 2-subgroup. (See Section 5 below.)

The (as yet unproved) Galois–McKay conjecture [N1] offers a connection between the fields of values of odd-degree characters of a finite group G and those of its 2-Sylow normalizer. As we will discuss in Section 5, some cases of Theorem B are explained by this conjecture, but not all.

2. Proofs assuming Theorem E

We follow the notation in [I2] for characters. If G is a finite group, then $\mathrm{Irr}(G)$ is the set of its irreducible complex characters. If N is a subgroup of G and $\theta \in \mathrm{Irr}(N)$, then $\mathrm{Irr}(G|\theta)$ is the set of the irreducible constituents of the induced character θ^G. By Frobenius reciprocity, this is the set of the irreducible characters χ of G such that the restriction χ_N contains θ as an irreducible constituent, and in this case, we say that χ "lies over" θ. If $n > 0$ is an integer and p is a prime, we uniquely factor $n = n_p n_{p'}$, where n_p is the largest power of p dividing n. If g is an element of finite order of a group G, then we can uniquely write $g = g_p g_{p'}$, where $g_p, g_{p'} \in \langle g \rangle$ have orders a p-power and not divisible by p, respectively. In particular, this applies if G is the group of linear characters of some group.

Lemma 2.1. *Let G be a finite group, and let N be a normal subgroup of G. Suppose that G/N has odd order. Let $\theta \in \mathrm{Irr}(N)$ be 2-rational. Then every character $\chi \in \mathrm{Irr}(G|\theta)$ is 2-rational.*

Proof. We proceed by induction on $|G|$. Let T be the stabilizer of θ in G, and let $\eta \in \mathrm{Irr}(T|\theta)$ be the Clifford correspondent of χ with respect to θ, so $\eta^G = \chi$. If $T < G$, then η is 2-rational by the inductive hypothesis. Since $\mathbb{Q}(\chi) \subseteq \mathbb{Q}(\eta)$, we deduce that χ is 2-rational, as required. We can assume, therefore, that $T = G$, so θ is invariant in G.

Now suppose that $N \subseteq H < G$. If ψ is an irreducible constituent of χ_H, then ψ lies over θ, so by the inductive hypothesis, ψ is 2-rational. For all elements $x \in H$, therefore, $\chi(x)$ has the form $\sum_\psi \psi(x)$ and thus $\chi(x)$ is 2-rational.

It remains to show that $\chi(x)$ is 2-rational if x lies in no proper subgroup of G containing N. We can assume, therefore, that $G = N\langle x \rangle$, so G/N is cyclic, and since θ is invariant in G, Corollary 11.22 of [I2] guarantees that θ extends to G. By Corollary 6.17 of [I2], the group of linear characters of G/N acts transitively by multiplication on $\mathrm{Irr}(G|\theta)$.

Let $n = |G|$, and $m = |G|_{2'}$, and let $\mathcal{G} = \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}_m)$. Then $\mathcal{G}$ is a 2-group, and we let $\sigma \in \mathcal{G}$. Since $\theta^\sigma = \theta$, both χ and χ^σ lie in $\mathrm{Irr}(G|\theta)$, and thus $\chi^\sigma = \chi\lambda$ for some linear character λ of G/N.

Since $|G/N|$ is odd, λ^m is principal. Then λ has values in $\mathbb{Q}_m$, so $\lambda^\sigma = \lambda$, and we have $\chi^{\sigma^m} = \chi\lambda^m = \chi$. Also, since σ has 2-power order, we have $\sigma \in \langle \sigma^m \rangle$, and thus σ fixes χ. Then $\mathcal{G}$ fixes χ, so χ has values in $\mathbb{Q}_m$, as required. □

Lemma 2.2. *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. Let $\chi \in \mathrm{Irr}(G)$ be an extension of θ. By the Gallagher correspondence (Theorem 6.16 of [I2]), the map $\beta \mapsto \beta\chi$ defines a bijection $\mathrm{Irr}(G|\lambda) \mapsto \mathrm{Irr}(G|\lambda\theta)$. Suppose that $\psi \in \mathrm{Irr}(G)$ extends $\lambda\theta$, and let $\beta \in \mathrm{Irr}(G|\lambda)$ be such that $\beta\chi = \psi$. Then $\beta(1)\theta(1) = \beta(1)\chi(1) = \psi(1) = \lambda(1)\theta(1)$, and we conclude that $\beta(1) = \lambda(1)$. Since β lies over λ, we conclude that $\beta_N = \lambda$. □

Lemma 2.3. *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 $\theta \in \mathrm{Irr}(N)$.*

(a) *If $\mu = \lambda_{p'}$, then $\mu\theta$ extends to a character $\psi \in \mathrm{Irr}(G)$. Also, we can write $\chi = \psi\xi$, where $\xi \in \mathrm{Irr}(G|\mu^{-1})$.*

(b) *If G/N is perfect and θ is p-rational, then ψ is p-rational.*

Proof. (a) Let P/N be a Sylow p-subgroup of G/N. Since χ has p'-degree, some irreducible constituent τ of χ_P has p'-degree. Then $\tau(1)$ and $|P : N|$ are relatively prime, so τ_N is irreducible by Corollary 11.29 of [I2]. Then $\tau_N = \theta$, and thus θ extends to P. Also, $\lambda\theta$ extends to G by hypothesis, so $\lambda\theta$ extends to P, and we conclude by Lemma 2.2 that λ extends to P. It follows that λ_p extends to P because λ_p is a power of λ.

If Q/N is a Sylow q-subgroup of G/N, where $q \neq p$, Corollary 6.28 of [I2] guarantees that λ_p extends to Q, and it follows by Corollary 11.31 of [I2] that λ_p extends to G. Now $\lambda\theta = \lambda_p\lambda_{p'}\theta$ extends to G, and since λ_p also extends to G, we deduce from Lemma 2.2 that $\lambda_{p'}\theta = \mu\theta$ extends to some character $\psi \in \mathrm{Irr}(G)$.

Now write $\varphi = \mu\theta$ so $\psi_N = \varphi$ and $\theta = \mu^{-1}\varphi$. Then $\chi \in \mathrm{Irr}(G|\mu^{-1}\varphi)$, and so by Theorem 6.16 of [I2], there exists a character $\xi \in \mathrm{Irr}(G|\mu^{-1})$ such that $\chi = \xi\psi$, and this completes the proof of (a).

(b) By hypothesis, θ is p-rational, and since $\mu = \lambda_{p'}$ is also p-rational, we see that φ is p-rational. We are assuming that G/N is perfect, so by Gallagher's theorem (Corollary 6.17 of [I2]) 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 p-rational, as required. □

We will use the following well-known facts. We write $\mathbf{R}$ for the ring of algebraic integers in $\mathbb{C}$.

Lemma 2.4. *Let χ be a character of a finite group G, and let p be a prime contained in a maximal ideal M of $\mathbf{R}$. Given $g \in G$, we have $\chi(g) \equiv \chi(g_{p'}) \pmod M$. In particular, if g is a p-element, then $\chi(g) \equiv \chi(1) \pmod M$, and so if $\chi(g) = 0$, then $\chi(1)$ is divisible by p.*

Proof. See, for instance, Lemma 4.19(b) of [N2]. □

Next is a standard result from the theory of projective representations.

Theorem 2.5. *Let $N \lhd G$, 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 $\pi : H \to G$ 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 $K/Z \to N$, 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 Theorem 5.6 of [N2]. □

The following result, which assumes Theorem E, will be essential in our proof of Theorem C. In Lemma 2.1 we assumed that G/N has odd order, but now we assume that G/N is simple.

Theorem 2.6. *Suppose that $N \triangleleft G$ and let $\theta \in \mathrm{Irr}(N)$ be G-invariant and 2-rational, with $\theta(1)$ odd. Suppose that G/N is a non-abelian simple group, and let $\chi \in \mathrm{Irr}(G|\theta)$ have odd degree. If χ is not 2-rational, then there exists a 2-element $x \in G$ such that $i \in \mathbb{Q}(\chi(x))$.*

Proof. By Theorem 2.5, 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 2.3, if $\mu = \lambda_{2'}$, we know that $\mu\theta$ extends to a 2-rational 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 odd-degree, since $\chi(1)$ is odd. Also, ξ is not 2-rational, since ψ is 2-rational and χ is not.

Write $L = \ker(\mu^{-1})$, so K/L is a central odd-order subgroup of H/L because μ^{-1} is invariant in H and has odd 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 odd. It follows that ξ_W is not 2-rational because otherwise, ξ would be 2-rational by Lemma 2.1, and this is not the case.

By Theorem E applied to the character ξ_W of W/L, we deduce that there exists an element $w \in W$ such that w has 2-power order modulo L, and $i \in \mathbb{Q}(\xi(w))$. Also, observe that we can assume that w has 2-power order. Now $\chi(w) = \psi(w)\xi(w)$, and $\psi(w) \in \mathbb{Q}$ because w has 2-power order and ψ is 2-rational. Furthermore, $\psi(w) \neq 0$ by Lemma 2.4 because w is a 2-element and $\psi(1)$ is odd. It follows that $\mathbb{Q}(\chi(w)) = \mathbb{Q}(\xi(w))$, and the proof is complete since we can take x to be the image of w in $H/Z = G$, so x is a 2-element and we have $i \in \mathbb{Q}(\xi(w)) = \mathbb{Q}(\chi(w)) = \mathbb{Q}(\chi(x))$. □

Next we prove Theorem C (assuming Theorem E).

Theorem 2.7. *Suppose that G is a finite group, and $\chi \in \mathrm{Irr}(G)$ has odd degree. If χ is not 2-rational, then $i \in \mathbb{Q}(\chi)$.*

Proof. We argue by induction on $|G|$. Let N be a normal subgroup of G. Let θ be an irreducible constituent of χ_N and let T be the stabilizer 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 the induction formula), we know that ψ is not 2-rational. Notice that $|G : T|$ is odd because $\chi(1)$ is odd. We claim that $|\mathbb{Q}(\psi) : \mathbb{Q}(\chi)|$ is odd. Otherwise, let $\sigma \in \mathrm{Gal}(\mathbb{Q}(\psi)/\mathbb{Q}(\chi))$ have order 2. Then $\chi^\sigma = \chi$. Thus $\theta^\sigma = \theta^g$ for some element $g \in G$, using Clifford's theorem. Notice that $g \in \mathbf{N}_G(T)$. Recall that the action of G on $\mathrm{Irr}(N)$ and the Galois action commute. Now $\theta = \theta^{\sigma^2} = \theta^{g^2}$, so $g^2 \in T$. Since $\mathbf{N}_G(T)/T$ has odd order, it follows that $g \in T$, so $\theta^\sigma = \theta^g = \theta$, and thus $\sigma = 1$. This is a contradiction, and so $|\mathbb{Q}(\psi) : \mathbb{Q}(\chi)|$ is odd, as claimed.

Assume that $T < G$. In this case, $i \in \mathbb{Q}(\psi)$ by the inductive hypothesis. Since $|\mathbb{Q}(\psi) : \mathbb{Q}(\chi)|$ is odd, we deduce that $i \in \mathbb{Q}(\chi)$, as required.

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 2-rational, by the inductive hypothesis.

Suppose that $N = \mathbf{O}^2(G) < G$. Since χ has odd-degree, we see that θ has odd-degree. By Theorem 6.28 of [I2], there is a unique extension $\hat{\theta} \in \mathrm{Irr}(G)$ of θ to G with determinantal order not divisible by 2. By uniqueness, notice that $\hat{\theta}$ is 2-rational, because θ is. By the Gallagher correspondence, it follows that $\chi = \lambda\hat{\theta}$, where $\lambda \in \mathrm{Irr}(G/N)$ is linear (because G/N is a 2-group and $\chi(1)$ is odd). Since χ is not 2-rational, λ has 2-power order exceeding 2. In particular, $\lambda(g) = i$ for some 2-element $g \in G$. Since g is a 2-element and $\hat{\theta}$ is 2-rational, we see that $\hat{\theta}(g)$ is a rational number. By Lemma 2.4, we have that $\hat{\theta}(g) \neq 0$. We deduce that $i \in \mathbb{Q}(\chi)$ in this case.

If G/N has odd order, where N is proper in G, then since θ is 2-rational, we can apply Lemma 2.1 to deduce that χ is 2-rational, contrary to hypothesis.

Thus, by taking a maximal normal subgroup N of G, we may assume that G/N is a non-abelian simple group. Now we apply Theorem 2.6 to conclude that $i \in \mathbb{Q}(\chi)$. □

Next we see that Theorem B is an easy consequence of Theorem C, using the following well-known result.

Theorem 2.8. [W, Corollary 4.5.5] *Let $m \geq 1$ be an integer. Suppose that f is a square-free integer. Set $f' = |f|$ if $f \equiv 1 \pmod 4$, and otherwise set $f' = 4|f|$. Then $\mathbb{Q}(\sqrt{f}) \subseteq \mathbb{Q}_m$ if and only if f' divides m.*

Proof of Theorem B. Let χ be a 2-rational character of a finite group G, and let $\gamma = \sqrt{\epsilon d}$, where $\epsilon = \pm 1$ and $d > 1$ is a square-free integer. Assume that $\gamma \in \mathbb{Q}(\chi)$, and let $m \geq 1$ be an odd integer such that $\mathbb{Q}(\chi) \subseteq \mathbb{Q}_m$. Let $f = \epsilon d$, and let f' be as in Theorem 2.8. By Theorem 2.8, we have that f' divides m. Since m is odd, we cannot have that $f' = 4|f|$. Hence $f \equiv 1 \pmod 4$. Therefore $\epsilon d \equiv 1 \pmod 4$. Thus d is odd and $\epsilon = \epsilon_d$. This proves Theorem B(a). To prove Theorem B(b), we assume now that χ is irreducible and has odd degree, and that it is not 2-rational. We must show that $i \in \mathbb{Q}(\chi)$ and that $\mathbb{Q}(\chi)$ does not have the form $\mathbb{Q}(\sqrt{\epsilon d})$, where $\epsilon = \pm 1$ and $d > 1$ is a square-free number. By Theorem 2.7, we have that $i \in \mathbb{Q}(\chi)$. Suppose finally that $\mathbb{Q}(\chi) = \mathbb{Q}(\sqrt{\epsilon d})$. Then $i \in \mathbb{Q}(\sqrt{\epsilon d})$, and thus $\epsilon = -1$. Hence $i \in \mathbb{Q}(i\sqrt{d})$ and therefore $\sqrt{d} \in \mathbb{Q}(i\sqrt{d})$. Thus $\mathbb{Q}(i, \sqrt{d}) = \mathbb{Q}(i\sqrt{d})$, and this is impossible because these fields have different degrees over $\mathbb{Q}$. □

3. Proof of Theorem D

In this section, we give a proof of Theorem D, which we will need in order to prove Theorem E. This theorem is a direct consequence of the main results of [NT3] and [M].

We review some of these results for the reader's convenience. We use $\mathbb{Q}^{\mathrm{ab}}$ to denote the field generated over $\mathbb{Q}$ by all complex roots of unity.

In [IN], Isaacs and Navarro conjectured the following.

Conjecture 3.1. *Let $e \geq 1$ be an integer. Let σ_e be the automorphism of $\mathbb{Q}^{\mathrm{ab}}$ that fixes roots of unity of order not divisible by p, and sends p-power roots of unity ξ to ξ^{1+p^e}. Let G be a finite group, and let $P \in \mathrm{Syl}_p(G)$. Then the exponent of P/P' is less than or equal to p^e if and only if all the irreducible characters of p'-degree of G are σ_e-fixed.*

It has been recently proved in [NT3, Theorem B] that if the exponent of P/P' is less than or equal to p^e, then all the irreducible characters of p'-degree of G are σ_e-fixed, thereby establishing one direction of Conjecture 3.1. Furthermore, it is proved in the same paper [NT3, Theorem C] that the converse holds provided that it is true for *almost quasi-simple groups*. In [M], this case has been solved for the case $p = 2$, therefore establishing the full Conjecture 3.1 for $p = 2$. We will use this fact below in Theorem 3.3.

We need an easy lemma.

Lemma 3.2. *Let $m \geq 2$ be an integer. Then the group $\Gamma = (\mathbb{Z}/2^m\mathbb{Z})^\times$ is generated by the two elements $\bar{3} = 3 + 2^m\mathbb{Z}$ and $\bar{5} = 5 + 2^m\mathbb{Z}$.*

Proof. The statement is obvious for $m = 2$, so we will assume $m \geq 3$. Then $|\Gamma| = 2^{m-1}$ and both $\bar{3}$ and $\bar{5}$ have order 2^{m-2} in Γ. However, $\bar{3} \notin \langle \bar{5} \rangle$, hence $\Gamma = \langle \bar{3}, \bar{5} \rangle$. □

Now we prove Theorem D, which we restate.

Theorem 3.3. *Let G be a finite group with a Sylow 2-subgroup P. Then $\exp(P/P') \leq 2$ if and only if all odd-degree irreducible characters of G are 2-rational.*

Proof. Again, for any integer $e \geq 1$, let σ_e be the automorphism of the field $\mathbb{Q}^{\mathrm{ab}}$ that fixes roots of unity of odd order, and sends 2-power roots of unity ξ to ξ^{1+2^e}.

Suppose that all odd-degree irreducible characters of G are 2-rational. In particular, they are all σ_1-invariant. Hence $\exp(P/P') \leq 2$ by [NT3, Theorem B].

Conversely now, suppose that $\exp(P/P') \leq 2$. Let $\chi \in \mathrm{Irr}(G)$ have odd-degree. By Conjecture 3.1 for $p = 2$, we have that χ is invariant under both σ_1 and σ_2. Write $|G| = 2^m n$, where n is odd. By Lemma 3.2, we have that the restrictions of σ_1 and σ_2 to $\mathbb{Q}_{|G|}$ generate $\mathrm{Gal}(\mathbb{Q}_{|G|}/\mathbb{Q}_n)$. Hence $\mathbb{Q}(\chi)$ is contained in $\mathbb{Q}_n$, and this proves that χ is 2-rational. □

4. Proof of Theorem E

In this section we prove Theorem E, which we restate:

Theorem 4.1. *Suppose that G is quasi-simple, and that $\chi \in \mathrm{Irr}(G)$ is not 2-rational and has odd degree. Then there exists a 2-element $g \in G$ such that $i \in \mathbb{Q}(\chi(g))$.*

4.1. **Further reductions.**

Lemma 4.2. *The following statements hold.*

(i) *It suffices to prove Theorem 4.1 in the case where* $\mathbf{Z}(G)$ *is of odd order and* $\exp(P/P') > 2$ *for* $P \in \mathrm{Syl}_2(G)$.

(ii) *Furthermore, Theorem 4.1 holds in the case* $G/\mathbf{Z}(G) \cong {}^2F_4(2)'$.

Proof. (i) Modding out by $\mathrm{Ker}(\chi)$ we may assume that χ is faithful. Since $\chi(1)$ is odd, we then have that $|\mathbf{Z}(G)|$ is odd. Furthermore, since χ is not 2-rational, $\exp(P/P') > 2$ by Theorem C.

(ii) Since ${}^2F_4(2)'$ has trivial Schur multiplier, we have that $G \cong {}^2F_4(2)'$. Now the statement can be checked using [Atlas]; indeed, g can be chosen to be of order 32. □

Proposition 4.3. *Let G be a finite simple group and $P \in \mathrm{Syl}_2(G)$. 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 any* $n \geq 5$.

(ii) G *any of the* 26 *sporadic simple groups.*

(iii) $G \not\cong {}^2F_4(2)'$ *a simple group of Lie type in characteristic* 2.

(iv) q *any odd prime power. Furthermore,* $G = \mathrm{PSp}_{2m}(q)$ *with* $m \geq 1$, $P\Omega^{\pm}_n(q)$ *with* $n \geq 7$, $\mathrm{PSL}_{2^m}(q)$ *or* $\mathrm{PSU}_{2^m}(q)$ *with* $m \geq 2$, $G_2(q)$, ${}^2G_2(q)$, ${}^3D_4(q)$, $F_4(q)$, $E_8(q)$, *or the (simple) group* $E_7(q)$.

(v) $\epsilon = \pm 1$, q *any prime power such that* $4|(q+\epsilon)$, *and* $G = \mathrm{PSL}^{\epsilon}_n(q)$ *with* $n \geq 3$, *or G is the (simple) group* $E^{\epsilon}_6(q)$.

Proof. All these statements were proved in [NT1]. Case (i), respectively (ii), is handled in Lemmas 3.3 and 3.4 of [NT1], respectively. Case (iii) is treated in [NT1, Proposition 4.5]. For (iv), see Propositions 3.5, 3.7, 3.8, and 4.1 of [NT1]. Finally, (v) is proved in Propositions 3.8, 4.1, and Corollary 3.9 of [NT1]. □

Corollary 4.4. *It suffices to prove Theorem 4.1 in the case where q is an odd prime power,* $q \equiv \epsilon (\mathrm{mod}\, 4)$ *for some* $\epsilon = \pm 1$, *and either* $G = \mathrm{SL}^{\epsilon}_n(q)$ *with* $n \geq 3$ *not a* 2*-power, or* $G = E^{\epsilon}_6(q)_{\mathrm{sc}}$.

Proof. Let $S = G/\mathbf{Z}(G)$ so that S is simple. By Lemma 4.2, we may assume that $|\mathbf{Z}(G)|$ is odd, $S \not\cong {}^2F_4(2)'$, and that $\exp(P/P') > 2$ for $P \in \mathrm{Syl}_2(G)$. Hence, $\exp(Q/Q') > 2$ for $Q \in \mathrm{Syl}_2(S)$. This implies by Proposition 4.3 that there is some $q \equiv \epsilon (\mathrm{mod}\, 4)$ such that either $S \cong \mathrm{PSL}^{\epsilon}_n(q)$ with $n \geq 3$ not a 2-power, or $S \cong E^{\epsilon}_6(q)$ (the simple group). Inspecting the Schur multiplier of S in those cases, we see that G is a quotient of $\mathrm{SL}^{\epsilon}_n(q)$ or $E^{\epsilon}_6(q)_{\mathrm{sc}}$. Inflating χ if necessary, we may thus assume that $G = \mathrm{SL}^{\epsilon}_n(q)$ or $E^{\epsilon}_6(q)_{\mathrm{sc}}$. □

4.2. **Special linear and unitary groups.** In this subsection we prove Theorem 4.1 for $G = \mathrm{SL}^{\epsilon}_n(q)$. Let $n \in \mathbb{Z}_{\geq 1}$ and consider the 2-adic decomposition

$$n = 2^{m_1} + 2^{m_2} + \ldots + 2^{m_r}, \tag{4.1}$$

with $m_1 > m_2 > \ldots > m_r \geq 0$. In what follows, we will refer to the summands 2^{m_i} in (4.1) as 2-*adic parts* of n. A decomposition $n = n_1 + n_2 + \ldots + n_k$ of n will be called a *proper decomposition* of n, if

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

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

For a fixed $\epsilon = \pm 1$, let $\mu_{q-\epsilon} = \langle \zeta \rangle$ be the cyclic subgroup of order $q - \epsilon$ of $\mathbb{F}_{q^2}^{\times}$, and let $\alpha := \zeta^{(q-\epsilon)_{2'}}$ so that $\langle \alpha \rangle = \mathbf{O}_2(\mu_{q-\epsilon})$. Fix a $(q-\epsilon)^{\text{th}}$ primitive root of unity $\tilde{\zeta} \in \mathbb{C}$, and set $\tilde{\alpha} := \tilde{\zeta}^{(q-\epsilon)_{2'}}$, a $(q-\epsilon)_2^{\text{th}}$ roof 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 labeling 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 4.5. *Let q be an odd prime power, $\epsilon = \pm 1$, $n \in \mathbb{Z}_{\geq 3}$ not a 2-power, and let $G := \mathrm{SL}_n^{\epsilon}(q) \lhd \mathrm{GL}_n^{\epsilon}(q) =: \tilde{G}$. 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 $n = n_1 + n_2 + \ldots + n_k$ of n, k pairwise distinct elements $\boldsymbol{s}_i \in \mu_{q-\epsilon}$, $1 \leq i \leq k$, and k partitions $\boldsymbol{\lambda}_i \vdash n_i$, $1 \leq i \leq k$, such that*

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

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

Proof. (i) follows from [ST, Lemma 10.2]. Next, (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 2-rational, but the conclusion of (iii) does not hold. Multiplying $\tilde{\chi}$ by $S((\boldsymbol{s}_1^{-1}, (n))$, we may assume that $(q-\epsilon)_2/2$ divides $[\boldsymbol{s}_i]$ for all i. Recall that $S(1, \boldsymbol{\lambda}_i)$ is a unipotent character of $\mathrm{GL}_{n_i}^{\epsilon}(q)$ and so takes only integer values. Since

$$S(\boldsymbol{s}_i, \boldsymbol{\lambda}_i) = S(\boldsymbol{s}_i, (n_i)) S(1, \boldsymbol{\lambda}_i), \tag{4.2}$$

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

$$\psi = S(\boldsymbol{s}_1, \boldsymbol{\lambda}_1) \otimes S(\boldsymbol{s}_2, \boldsymbol{\lambda}_2) \otimes \ldots \otimes S(\boldsymbol{s}_k, \boldsymbol{\lambda}_k), \tag{4.3}$$

that is, it is Lusztig induced from the Levi subgroup

$$L = \mathrm{GL}_{n_1}^{\epsilon}(q) \times \mathrm{GL}_{n_2}^{\epsilon}(q) \times \ldots \times \mathrm{GL}_{n_k}^{\epsilon}(q). \tag{4.4}$$

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 2-rational, a contradiction. □

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

Lemma 4.6. *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 above. 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*

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

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

(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 and with all eigenvalues on $\overline{\mathbb{F}}_q^n$ belonging to $\mathbb{F}_{q^{2^{m_1}}}$, if n is written in the form (4.1).*

Theorem 4.7. *Let $n \in \mathbb{Z}_{\geq 3}$ be not a 2-power, $\epsilon = \pm 1$, and let q be an odd prime power such that $(q-\epsilon)_2 = 2^a \geq 4$. Then Theorem 4.1 holds true for $G = \mathrm{SL}_n^\epsilon(q)$.*

Proof. Let $\chi \in \mathrm{Irr}(G)$ be of odd degree and not 2-rational. We set $\tilde{G} := \mathrm{GL}_n^\epsilon(q)$ and apply Lemma 4.5 to get the character $\tilde{\chi}$ as in the lemma. We will write $\tilde{\chi} = \pm R_L^{\tilde{G}}(\psi)$ with ψ given in (4.3). Also let $V := \mathbb{F}_q^n$, respectively $\mathbb{F}_{q^2}^n$, denote the natural module for $\tilde{G}$, and let $\tilde{V} := V \otimes \overline{\mathbb{F}}_q$. Since $n = n_1 + \ldots + n_k$ is a proper decomposition, the Levi subgroup L acts semisimply with pairwise non-isomorphic 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 set

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

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

Case 1a: Suppose in addition that the smallest 2-adic part 2^{m_r} of n, cf. (4.1), is neither a 2-adic part of n_{i_0} nor of n_{j_0}.

Then we consider the following two elements in $\tilde{G}$ using Lemma 4.6:

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

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 $g, g' \in \mathrm{SL}_n^\epsilon(q)$. In the case $\epsilon = -1$, the above decomposition splits V into an orthogonal direct sum of non-degenerate subspaces invariant under g, respectively under g'.

We will show that

$$\sqrt{-1} \in \mathbb{Q}(\chi(g)) \cup \mathbb{Q}(\chi(g')). \tag{4.5}$$

To do this, first we note that the assumption on 2^{m_r} implies that $r \geq 3$. Now we show by induction on $r \geq 3$ that each of g and g' is contained in a unique $\tilde{G}$-conjugate of the Levi subgroup L given in (4.4); equivalently, if $g \in L^x$ for some $x \in \tilde{G}$, then L^x is uniquely determined by g, and similarly for g'. Note that the set of eigenvalues of g on $\tilde{V}$ has a unique F-orbit of length 2^{m_1}, coming from the unique block $g_{2^{m_1}}(\beta)$ of g, with $\beta = \alpha^{\pm 1}$. Recall that $n = n_1 + \ldots + n_k$ is a proper decomposition of n; in particular, each 2-adic part of each n_i, $1 \le i \le k$, is some 2^{m_j}, $1 \le j \le r$. As n_1 is the largest one, it follows that 2^{m_1} is a 2-adic part of n_1, and

$$n_2 + n_3 + \ldots + n_k \le \sum_{e=0}^{m_1-1} 2^e < 2^{m_1}.$$

As the set of eigenvalues of the projection of g onto the factor $\mathrm{GL}^{\epsilon}_{n_1}(q)$ of L^x is F-stable, we see that this projection has to afford the aforementioned F-orbit of length 2^{m_1}, and this orbit accounts for the 2-adic part 2^{m_1} of n_1. Also note that the block $g_{2^{m_1}}(\beta)$ of g corresponds to a g-invariant subspace U which is an orthogonal direct summand of the Hermitian space $\mathbb{F}^n_{q^2}$ in the case $\epsilon = -1$. Now we can mod out by U and work inductively in V/U until we have exhausted all 2-adic parts 2^{m_i}, $1 \le i \le r-1$. The last block $h_{2^{m_r}}(\delta)$ then contributes to the submodule of V for the last remaining factor $\mathrm{GL}^{\epsilon}_{n_e}(q)$. We have shown that all L^x-composition factors on V and on $\tilde{V}$ are uniquely determined by g. Since L^x acts semisimply on V with non-isomorphic simple submodules, this uniqueness implies that L^x is unique.

Without loss we may now assume that $g \in L$. Since each of $g_{2^{m_i}}(\alpha^{\pm 1})$ and $h_{2^{m_r}}(\delta)$ is regular, the above argument also shows that

$$\mathbf{C}_{\tilde{G}}(g) = \mathbf{C}_L(g). \tag{4.6}$$

According to [DM, Proposition 9.6],

$$\mathsf{St}_{\tilde{G}} \cdot \tilde{\chi} = \pm \mathsf{St}_{\tilde{G}} \cdot R^{\tilde{G}}_L(\psi) = \pm(\mathsf{St}_L \cdot \psi)^{\tilde{G}}, \tag{4.7}$$

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

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

On the other hand, as g is semisimple, we have that $\mathsf{St}_{\tilde{G}}(g) = \pm|\mathbf{C}_{\tilde{G}}(g)|_p$ and $\mathsf{St}_L(g) = \pm|\mathbf{C}_L(g)|_p$, see [DM, Corollary 9.3]. It follows that

$$\chi(g) = \kappa\psi(g),\ \chi(g') = \kappa'\psi(g') \tag{4.8}$$

for some $\kappa, \kappa' \in \mathbb{Q}^\times$. (In fact, using (4.6) we see that $\kappa = \pm 1$ and likewise $\kappa' = \pm 1$.)

It remains to evaluate ψ on g and g', using (4.3). 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 Lemma 2.4. Recalling the constructions of g and g' and applying (4.2) to $S(\boldsymbol{s}_{i_0}, \boldsymbol{\lambda}_{i_0})$ and $S(\boldsymbol{s}_{j_0}, \boldsymbol{\lambda}_{j_0})$, we now have that

$$\frac{\psi(g)}{\psi(g')} = \tilde{\alpha}^{2([\boldsymbol{s}_{i_0}]-[\boldsymbol{s}_{j_0}])}. \tag{4.9}$$

As $|\tilde{\alpha}| = 2^a$ and $2^{a-2} \nmid ([\boldsymbol{s}_{i_0}] - [\boldsymbol{s}_{j_0}])$, we see that $\psi(g)/\psi(g')$ is a root of unity of order $2^f \ge 4$. On the other hand, as the unipotent characters $S(1, \boldsymbol{\lambda}_i)$ take only integer values, (4.2) implies that $\psi(g)$ is a $\mathbb{Z}$-multiple of a 2-power root of unity. It follows from (4.9) that this root of unity for at least one of g, g' must have order ≥ 4, say for g. We conclude by (4.8) that $\chi(g)$ is a $\mathbb{Q}$-multiple of a 2-power root of unity of order ≥ 4, and $\chi(g) \ne 0$ by Lemma 2.4. Thus $\sqrt{-1} \in \mathbb{Q}(\chi(g))$, establishing (4.5).

Case 1b: Suppose we are in Case 1, but the smallest 2-adic part 2^{m_r} of n, is a 2-adic part, say of n_{i_0}.

Then we consider the following two elements in $\tilde{G}$ using Lemma 4.6:

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

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 (4.8) and (4.9) hold. Hence we conclude as above that (4.5) holds as desired.

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

Multiplying $\tilde{\chi}$ by $S(\boldsymbol{s}_1^{-1}, (n))$, we may assume that 2^{a-2} divides $[\boldsymbol{s}_i]$ for all $1 \le i \le k$. By Lemma 4.5(iii), there exist some $i_0 < j_0$ such that $2^{a-1} \nmid ([\boldsymbol{s}_{i_0}] - [\boldsymbol{s}_{j_0}])$. Keeping in mind the fact that $n = n_1 + \ldots + n_k$ 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 n_i with $2^{a-1} \nmid [\boldsymbol{s}_i]$ is among $2^{m'_1}, \ldots, 2^{m'_s}$, and vice versa, and
- each 2-adic part of n_j with $2^{a-1} | [\boldsymbol{s}_j]$ is among $2^{m''_1}, \ldots, 2^{m''_t}$, and vice versa.

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

$$L_1 = \prod_{i: 2^{a-1} \nmid [\boldsymbol{s}_i]} \mathrm{GL}^\epsilon_{n_i}(q), \;\; L_2 = \prod_{j: 2^{a-1} | [\boldsymbol{s}_j]} \mathrm{GL}^\epsilon_{n_j}(q).$$

We claim that, to prove (4.5), it suffices to find a 2-element $g \in G$ such that, whenever a conjugate g^x of g is contained in L, then

(4.10) the projection of g^x onto L_1 has determinant $\equiv \alpha (\bmod\, \alpha^2)$.

Indeed, suppose $h_1 h_2 = g^x \in L$, with h_i being 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 (4.2) and the fact that unipotent characters $S(1, \boldsymbol{\lambda}_i)$ 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

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

since by (4.10) we have

$$\alpha^{\sum_{i: 2^{a-1} \nmid [\boldsymbol{s}_i]} a_i} = \det(h_1) \equiv \alpha (\bmod\, \alpha^2).$$

But $|\tilde{\alpha}| = 2^a$, so we have that $\psi(g^x) = \pm\kappa(x)\sqrt{-1}$. It now follows from (4.7) that

$$\chi(g) = \kappa\sqrt{-1}$$

for some $\kappa \in \mathbb{Q}$. Since $\kappa \neq 0$ by Lemma 2.4, we conclude that $\sqrt{-1} \in \mathbb{Q}(\chi(g))$, as desired.

We will now 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 (4.10).

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

Setting

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

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

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

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 $m''_t > m'_s + 1$, 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 $m''_t = m'_s + 1$ and $g \in L^x$ for some $x \in \tilde{G}$. Again we argue as in Case 1a and see that all the 2-adic parts $2^{m_i} > 2^{m''_t}$ are filled up uniquely by the F-orbit of g-eigenvalues of $g_{2^{m_i}}(\alpha^{\pm 1})$. This leaves three F-orbits of g-eigenvalues, of length $2^{m'_s}$ each, and afforded by two blocks $g_{2^{m'_s}}(\alpha)$ and one block $g_{2^{m'_s}}(\alpha^{-1})$, to fill up the two remaining 2-adic parts $2^{m''_t} = 2 \cdot 2^{m'_s}$ and $2^{m'_s}$. Clearly, all possible ways of filling up the remaining 2-adic part $2^{m'_s}$ for L_1^x have determinant α or α^{-1}, and so (4.10) is satisfied.

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

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

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

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 $m'_s > m''_t + 1$. Then 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_1^x and thus gives the same determinant modulo α^2 for the projection on g onto L_1^x, as required in (4.10).

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_1^x and thus gives the same determinant modulo α^2 for the projection on g onto L_1^x, as required in (4.10). $\square$

This completes the proof of Theorem E for $G = \mathrm{SL}_n^\epsilon(q)$.

4.3. **Groups of type E_6 and ${}^2E_6(q)$.** The rest of the section is devoted to prove Theorem E for $G = E_6^\epsilon(q)_{\mathrm{sc}}$. First we recall a useful observation.

Lemma 4.8. *Let G be a finite group with a subgroup L, and let $t \in L$ be such that $\mathbf{C}_G(t') \leq L$ for all $t' \in t^G \cap L$. If $\{t_1 = t, t_2, \dots, t_s\}$ is a set of representatives of L-conjugacy classes in $t^G \cap L$ and φ is a class function on L, then $\varphi^G(t) = \sum_{i=1}^s \varphi(t_i)$.*

Proof. Write $G = \sqcup_{i=1}^m Lg_i$ with $g_1 = 1$, $g_itg_i^{-1} \in L$ for $1 \leq i \leq k$ and $g_itg_i^{-1} \notin L$. Then we have $\varphi^G(t) = \sum_{i=1}^k \varphi(g_itg_i^{-1})$. Suppose that $g_itg_i^{-1}$ is L-conjugate to $g_jtg_j^{-1}$ for some $1 \leq i, j \leq k$. Then $g_jg_i^{-1}(g_itg_i^{-1})g_ig_j^{-1} = xg_itg_i^{-1}x^{-1}$ for some $x \in L$, and so $x^{-1}g_jg_i^{-1} \in \mathbf{C}_G(g_itg_i^{-1}) \leq L$. It follows that $g_jg_i^{-1} \in L$, $g_j \in Lg_i$, and so $i = j$. This shows that $\{g_itg_i^{-1} \mid 1 \leq i \leq k\}$ is another set of representatives of L-conjugacy classes in $t^G \cap L$, and the statement follows. $\square$

In the treatment of groups $G = \mathcal{G}^F = E_6^\epsilon(q)_{\mathrm{sc}}$, we will make frequent use of an F-stable subsystem subgroup D_5T_1 in $\mathcal{G}$ (with T_1 denotes a one-dimensional torus). The existence of such a subsystem can be seen from the extended E_6 Dynkin diagram; it is conjugate to a standard Levi subgroup of $\mathcal{G}$, and has fixed point group $D_5^\epsilon(q) \cdot C_{q-\epsilon}$ under F. An explicit construction of this subgroup is also displayed in the proof of [NT1, Proposition 4.3].

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 centralizes a unique involution v that has centralizer 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*;*
(v) $t^G \cap L = t^L$.

Proof. We will construct t inside a maximal rank subgroup A of G containing the subgroup $A_5^\epsilon A_1 = \mathrm{SL}_6^\epsilon(q) \circ \mathrm{SL}_2(q)$ with index 2. Let $\gamma \in \mathbb{F}_{q^4}$ have order $(q^4-1)_2 = 2^{a+2}$, and set $\delta = \gamma^{-(q^2+1)}$ and $\lambda = \gamma^4$. Define $t = t_1t_2 \in A_5^\epsilon A_1$, where $t_1 \in \mathrm{SL}_6^\epsilon(q)$, $t_2 \in \mathrm{SL}_2(q)$ are conjugate over $\bar{\mathbb{F}}_q$ respectively to

$$\mathrm{diag}(\gamma, \gamma^{\epsilon q}, \gamma^{q^2}, \gamma^{\epsilon q^3}, \delta, \delta^{\epsilon q}), \quad \mathrm{diag}(\lambda, \lambda^{-1}).$$

Then $|\mathbf{C}_A(t)| = (q^4-1)(q^2-1)$. Also by [LS, 11.10], for the ambient algebraic group E_6,

$$L(E_6) \downarrow A_5A_1 = L(A_1A_5) + (V_{A_5}(\lambda_3) \otimes V_{A_1}(1)), \tag{4.11}$$

and the second summand is $\wedge^3(V_6) \otimes V_2$, where V_6, V_2 are the natural modules for A_5, A_1. Using the hypothesis that $(q-\epsilon)_2 = 2^a \geq 8$, we check that t has no nonzero fixed points on this tensor product. It follows that $\dim \mathbf{C}_{L(E_6)}(t) = 6$, and so $\mathbf{C}_G(t)$ is equal to the maximal torus $T := \mathbf{C}_A(t)$ of order $(q^4-1)(q^2-1)$. The structure of T is a direct product $(q^4-1) \times (q^2-1)$ (see [KS, p.377]).

Let $\mathbf{Z}(A) = \langle u \rangle$, and let $v = \mathrm{diag}(-1^4, 1^2) \in \mathrm{SL}_6^\epsilon(q)$. Then T contains precisely three involutions, namely v, u and vu. Now vu is a central element of a root $\mathrm{SL}_2(q)$, hence has centralizer in the algebraic group E_6 of type A_5A_1 (as does u). On the other hand, v is central in a subsystem A_3 subgroup, and restricting from (4.11), we have

$$L(E_6) \downarrow A_3 = L(A_3) + V(\lambda_1)^4 + V(\lambda_2)^4 + V(\lambda_3)^4 + V(0)^7.$$

It follows that $\dim \mathbf{C}_{L(E_6)}(v) = 46$, so that $\mathbf{C}_G(v)$ is of type $D_5^\epsilon T_1$.

Next we establish part (iv). Observe that $\mathbf{C}_G(v)$ contains a subgroup $A_3^\epsilon A_1 A_1 < A_5^\epsilon A_1$, which lies in $D = \mathrm{Spin}_{10}^\epsilon(q)$. Also, if we write $\omega = \gamma^{2^{a-1}}$ (an 8th root of 1) and $\iota = \omega^2$, then

$$t^{2^{a-1}} = \mathrm{diag}(\omega, \omega, \omega, \omega, \iota, \iota) \cdot \mathrm{diag}(-1, -1) \in A_5^\epsilon A_1,$$

and this centralizes $A_3^\epsilon A_1 A_1$. If $t^{2^{a-1}} \in D$, this implies that $t^{2^{a-1}} \in \mathbf{C}_D(A_3^\epsilon A_1 A_1)$. However, $\mathbf{C}_D(A_3^\epsilon A_1 A_1) = \mathbf{Z}(A_3^\epsilon A_1 A_1)$, and this does not contain $t^{2^{a-1}}$. Hence $t^{2^{a-1}} \notin D$, and part (iv) follows.

Finally, suppose $xtx^{-1} \in L$ for some $x \in G$. Since $L = \mathbf{C}_G(v)$, we see that t centralizes the involution $x^{-1}vx$, which has centralizer of type D_5T_1 in $\mathcal{G}$. By (iii), $x^{-1}vx = v$, i.e. $x \in \mathbf{C}_G(v) = L$, as stated in (v). □

Proposition 4.10. *Let* $G = E_6^\epsilon(q)_{\mathrm{sc}}$*, and suppose that* $(q-\epsilon)_2 = 4$*. 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* $(q^4-1) \times (q-\epsilon) \times (q-\epsilon)$*;*
(iii) *there is an involution* $v \in G$ *such that*
  (a) $t \in L = \mathbf{C}_G(v) = D \cdot C_{q-\epsilon}$*, where* $D = [L, L] \cong \mathrm{Spin}_{10}^\epsilon(q)$*,*
  (b) $\mathbf{C}_G(t) \leq L$*, and*
  (c) *the coset* $tD \in L/D$ *has order* 4*;*

(iv) *the set* $t^G \cap L$ *falls into five* L*-conjugacy classes; if we label representatives of these classes* $t_1, \dots, t_5$ *(where* $t_1 = t$*), then there are precisely three values of* i *such that the coset* t_iD *has order* 4 *in* L/D.

Proof. The element t is again chosen inside a maximal rank subgroup $A_5^\epsilon A_1$, but is slightly different from the element in Proposition 4.9. Let $\gamma \in \mathbb{F}_{q^4}$ have order $(q^4-1)_2 = 16$, and let $\iota = \gamma^4 \in \mathbb{F}_{q^2}$. Define $t = t_1t_2 \in A_5^\epsilon A_1$, where

$$t_1 = \mathrm{diag}(\gamma, \gamma^{\epsilon q}, \gamma^{q^2}, \gamma^{\epsilon q^3}, \iota, 1), \quad t_2 = \mathrm{diag}(\iota, -\iota).$$

It is shown in the proof of [GLBST, 7.16] that $\mathbf{C}_G(t)$ is a maximal torus of order $(q^4-1)(q-\epsilon)^2$. Hence using [KS] as before, we have

$$\mathbf{C}_G(t) = T = (q^4-1) \times (q-\epsilon) \times (q-\epsilon).$$

The involutions in T all lie in the subgroup $\langle u, v, w\rangle$, where

$$\begin{aligned} u &= -I_6 \in A_5^\epsilon, \\ v &= (-1,-1,-1,-1,1,1) \in A_5^\epsilon, \\ w &= ((\iota,\iota,\iota,\iota,\iota,-\iota),\ (\iota,-\iota)) \in A_5^\epsilon A_1. \end{aligned}$$

Restricting the Lie algebra $L(E_6)$ to $A_5^\epsilon A_1$ as in the previous proof, we find that the involutions in T that have centralizer in G of type $D_5^\epsilon T_1$ are

$$v,\ w,\ uw,\ vw \text{ and } uvw. \tag{4.12}$$

We next show that (iii) holds. Let $L = \mathbf{C}_G(v)$, and $D = [L, L] \cong D_5^\epsilon(q)$. Clearly $t \in L$ and $T = \mathbf{C}_G(t) \le L$, so it remains to prove (iii)(c). Now $\mathbf{C}_{A_5^\epsilon A_1}(v)' = A_3A_1^{(1)}A_1$, where $A_3A_1^{(1)} < A_5^\epsilon$. Moreover,

$$t^2 = (-\gamma^2, -\gamma^{2\epsilon q}, -\gamma^{2q^2}, -\gamma^{2\epsilon q^3}, 1, -1) \in A_5^\epsilon. \tag{4.13}$$

Hence if $t^2 \in D$, then $t^2 \in \mathbf{C}_D(A_1)$; however $\mathbf{C}_D(A_1) = A_3^\epsilon A_1^{(1)}$, and from (4.13) it is apparent that t^2 does not lie in $A_3A_1^{(1)}$. It follows that $t^2 \notin D$, proving (iii)(c).

Finally we prove (iv). Suppose $t^g \in t^G \cap L$. Then $t \in L^{g^{-1}} = \mathbf{C}_G(v^{g^{-1}})$, and so from (4.12), we have $v^{g^{-1}} \in \{v, w, uw, vw, uvw\}$. Hence $t^G \cap L$ falls into five L-classes, one for each possibility for $v^{g^{-1}}$. Write $t' = t^g$ and $v' = v^{g^{-1}}$.

We consider in turn the possibilities for v' and compute the order of the coset $t'D$ in L/D in each case. If $v' = v$ then the order is 4, by part (iii).

Next suppose that $v' = vw$ or uvw. Then from (4.13) we see that $t^2 \in A_4^\epsilon < \mathbf{C}_{A_5^\epsilon}(v')$, and hence $t^2 \in [\mathbf{C}_G(v'), \mathbf{C}_G(v')] = D^{g^{-1}}$. It follows that $(t')^2 \in D$, so $t'D$ has order less than 4 in this case.

Finally, suppose that $v' = w$ or uw. This time we write t^2 as

$$t^2 = (\gamma^2, \gamma^{2\epsilon q}, \gamma^{2q^2}, \gamma^{2\epsilon q^3}, -1, 1)\, u,$$

so that $t^2 = au$, where $a \in A_4^\epsilon < \mathbf{C}_{A_5^\epsilon}(v')$. Clearly $A_4^\epsilon < D^{g^{-1}}$, so if $t^2 \in D^{g^{-1}}$, then $u \in \mathbf{C}_{D^{g^{-1}}}(A_4^\epsilon)$. However, the only involution in $D_5^\epsilon = \mathrm{Spin}_{10}^\epsilon$ that centralizes an A_4^ϵ subgroup is the central involution; this involution of course has centralizer in G of type $D_5^\epsilon T_1$, whereas u has centralizer $A_5^\epsilon A_1$. Hence $t^2 \notin D^{g^{-1}}$, which implies that the coset $t'D$ has order 4 in this case.

We have shown that $t'D$ has order 4 precisely in the cases where $v' = v, w$ or uw. This completes the proof of (iv). □

Proof of Theorem 4.1. By Corollary 4.4 and Theorem 4.7, it suffices to prove Theorem 4.1 in the case $G = \mathcal{G}^F = E_6^\epsilon(q)_{\rm sc}$, 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 $F : \mathcal{G} \to \mathcal{G}$ a suitable Steinberg endomorphism. Using [Lu] one can see that G has exactly $8(q-\epsilon)$ irreducible characters of odd degree, among which 8 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 $8(q-\epsilon-1)$ non-unipotent characters of odd degree and χ belongs to the rational series $\mathcal{E}(G,(s))$, labeled 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 [NT2, Lemma 4.13], $L := \mathcal{L}^F$ and $\mathcal{L}^{*F^*}$ each has exactly 8 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 8 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 that

$$\chi = \pm R_L^G(\psi\lambda), \tag{4.14}$$

where $\psi \in {\rm Irr}(L)$ is unipotent of odd degree, rational-valued as mentioned above, and $\lambda \in {\rm Irr}(L)$ 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 the mutplication 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. With the assumption that χ is not 2-rational, this implies that λ is not 2-rational. As discussed in the proof of Proposition 4.9, $D = [L,L] \cong {\rm Spin}_{10}^\epsilon(q)$ and $L/D \cong C_{q-\epsilon}$. Hence λ is a character of L/D of order divisible by 4.

Let $(q-\epsilon)_2 = 2^a \geq 4$. We now consider the regular 2-element $t \in L$ constructed in Proposition 4.9 when $a \geq 3$ and in Proposition 4.10 when $a = 2$. 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 Lemma 4.8 to t and obtain from (4.7) and (4.14) that

$$\chi(t) = \pm \mathsf{St}_G(t)\chi(t) = \pm(\mathsf{St}_G \cdot R_L^G(\psi\lambda))(t) = \pm(\mathsf{St}_L\psi\lambda)^G(t) = \sum_{j=1}^{s} \pm\psi(t_j)\lambda_j(t_j), \tag{4.15}$$

if $\{t_1 = t, t_2, \ldots, t_s\}$ is a full set of representatives of L-conjugacy classes in $t^G \cap L$. (Here we have used the fact that any $t' \in t^G \cap L$ is regular in both $\mathcal{G}$ and $\mathcal{L}$, and so $\mathsf{St}_G(t') = \pm 1$ and $\mathsf{St}_L(t') = \pm 1$.) Note that, by Lemma 2.4, $\psi(t_j)$ is an odd integer since ψ is of odd degree and rational-valued.

Suppose $a \geq 3$. Then $s = 1$ by Proposition 4.9. Also, the coset tD generates $\mathbf{O}_2(L/D)$. Since λ has order divisible by 4, it follows that $\lambda(t)$ is a primitive root of unity ξ of order $2^b \geq 4$. Now (4.15) yields $\chi(t) = \pm\psi(t)\xi$, and $\psi(t)$ is an odd integer as mentioned above. Hence, $i \in \mathbb{Q}(\chi(t))$, as required.

Finally, consider the case $a = 2$. Then $s = 5$ by Proposition 4.10, and the order of t_jD in L/D is 4 if $1 \leq j \leq 3$ and ≤ 2 of $j = 4, 5$. As the order of λ is divisible by 4 and $\mathbf{O}_2(L/D) = C_4$, it follows that $\lambda(t_j) = \pm i$ if $1 \leq j \leq 3$ and $\lambda(t_j) = \pm 1$ if $j = 4, 5$. It now follows from (4.15) that there are some odd integers $a_j \in \mathbb{Z}$, $1 \leq j \leq 5$, such that

$$\chi(t) = (a_1 + a_2 + a_3)i + (a_4 + a_5).$$

Since $a_1 + a_2 + a_3$ is odd, we conclude that $i \in \mathbb{Q}(\chi(t))$. □

5. Galois–McKay connections

The main result of this section is Theorem 5.5, which is a weaker version of Theorem B. Our proof of this result does not utilize the simple group classification, but instead, it appeals to the (as yet unproved) Galois-McKay conjecture, which we will explain.

To prove Theorem 5.5, we use the fact that if $\chi \in \mathrm{Irr}(G)$ has odd degree and is not 2-rational, then $i \in \mathbb{Q}(\chi)$. (This was proved using the classification in Theorem 2.7.) Here, we need this result only in the case where G has a normal Sylow 2-subgroup, and although the proof of Theorem 2.7 goes through, we have decided to give an independent proof of a stronger fact: Corollary 5.2 below. We show there that in the case of interest, where G has a normal Sylow 2-subgroup, not only is it true that $i \in \mathbb{Q}(\chi)$, but in fact, $i \in \mathbb{Q}(\chi(x))$ for some 2-element x of G. (We have been unable to determine if this stronger conclusion is true more generally for arbitrary solvable groups.)

We begin with a general lemma.

Lemma 5.1. *Let P be a normal Sylow 2-subgroup of G. Given a linear character λ of P, write*

$$\Xi_\lambda = \sum_{g \in G} \lambda^g \,.$$

Then

(a) $\mathbb{Q}(\Xi_\lambda) = \mathbb{Q}(\lambda)$ *and*
(b) *If $o(\lambda) \geq 4$, there exists an element $x \in P$ such that $i \in \mathbb{Q}(\Xi_\lambda(x))$.*

Proof. For each element $g \in G$, we have $\mathbb{Q}(\lambda^g) = \mathbb{Q}(\lambda)$, and it follows that $\mathbb{Q}(\Xi_\lambda) \subseteq \mathbb{Q}(\lambda)$. Let $f = o(\lambda)$, so f is a power of 2, and since λ is linear, we have $\mathbb{Q}(\lambda) = \mathbb{Q}_f$. Then $|\mathbb{Q}(\lambda) : \mathbb{Q}(\Xi_\lambda)|$ divides $|\mathbb{Q}_f : \mathbb{Q}| = \varphi(f)$, where φ is Euler's function. Since $\varphi(f)$ is a power of 2, we deduce that the Galois group $\mathcal{G} = \mathrm{Gal}(\mathbb{Q}(\lambda)/\mathbb{Q}(\Xi_\lambda))$ is a 2-group.

To complete the proof of (a), we must show that $\mathcal{G}$ is trivial, so suppose that $\sigma \in \mathcal{G}$. Since σ fixes Ξ_λ, it permutes the irreducible constituents of this character, and thus $\lambda^\sigma = \lambda^g$ for some element $g \in G$.

Factoring $g = g_2 g_{2'}$, we see that g_2 lies in P, so g_2 fixes λ. We can thus assume that $g = g_{2'}$, so $o(g)$ is some odd integer r. The actions of G and $\mathcal{G}$ on characters of P commute, and hence $\lambda = \lambda^{g^r} = \lambda^{\sigma^r}$, and we deduce that $\sigma^r = 1$. Now $o(\sigma)$ is a power of 2 that divides the odd number r, and we conclude that $\sigma = 1$, so $\mathcal{G}$ is trivial, as required.

For (b), we have by hypothesis that $f \geq 4$, and we proceed by induction on f. If $f = 4$, then $\mathbb{Q}(\Xi_\lambda) = \mathbb{Q}_4 = \mathbb{Q}(i)$, which has degree 2 over $\mathbb{Q}$. For some element $x \in G$, we have $\Xi_\lambda(x)$ is not rational, so $\mathbb{Q} < \mathbb{Q}(\Xi_\lambda(x)) \subseteq \mathbb{Q}(i)$, and it follows that $\mathbb{Q}(\Xi_\lambda(x)) = \mathbb{Q}(i)$, and thus $i \in \mathbb{Q}(\Xi_\lambda(x))$, as required.

Now assume that $f > 4$. Then $o(\lambda^2) = f/2$, so we can apply the inductive hypothesis with λ^2 in place of λ, and we conclude that there exists $x \in P$ such that $i \in \mathbb{Q}(\Xi_{\lambda^2}(x))$. Finally, we observe that $\Xi_{\lambda^2}(x) = \Xi_\lambda(x^2)$, and this completes the proof. □

Corollary 5.2. *Let $\chi \in \mathrm{Irr}(G)$, where $\chi(1)$ is odd and χ is not 2-rational, and assume that G has a normal Sylow 2-subgroup. Then there exists a 2-element $x \in G$ such that $i \in \mathbb{Q}(\chi(x))$.*

As was mentioned, we will not need the full strength of Corollary 5.2; we will use only the weaker conclusion that $i \in \mathbb{Q}(\chi)$.

Proof of Corollary 5.2. Let $P \in \mathrm{Syl}_p(G)$, so $P \lhd G$. Since $\chi(1)$ is odd, we see that χ_P has a linear constituent λ, and so by Clifford's theorem, χ_P is a nonzero rational multiple of the character Ξ_λ, as defined in Lemma 5.1.

By hypothesis, χ is not 2-rational, and it follows by Lemma 2.1 that λ is not 2-rational, and thus $o(\lambda) \geq 4$. By Lemma 5.1(b), there exists an element $x \in P$ such that $i \in \mathbb{Q}(\Xi_\lambda(x)) = \mathbb{Q}(\chi_P(x)) = \mathbb{Q}(\chi(x))$, as required. □

We are now ready to discuss the Galois-McKay conjecture. Given a prime p and a positive integer n, let $\mathcal{H}_{p,n}$ be the subgroup of $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})$ consisting of those automorphisms of the field $\mathbb{Q}_n$ that send each p'-order root of unity ξ to some power ξ^t, where, t is an arbitrary power of p depending on ξ. In particular, observe that the automorphisms of $\mathbb{Q}_n$ that fix all p'-roots of unity lie in $\mathcal{H}_{p,n}$, so $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}_m) \subseteq \mathcal{H}_{p,n}$, where $m = n_{p'}$.

Given a prime number p and a finite group X, recall that the set of irreducible characters of X having p'-degree is denoted $\mathrm{Irr}_{p'}(X)$, and that the "ordinary" McKay conjecture asserts that for every finite group G and prime p, we have $|\mathrm{Irr}_{p'}(G)| = |\mathrm{Irr}_{p'}(\mathbf{N}_G(P))|$, where P is a Sylow p-subgroup in G.

The Galois-McKay conjecture (see Conjecture 9.8 of [N2]) strengthens the McKay conjecture by asserting that there is a bijection $f : \mathrm{Irr}_{p'}(G) \to \mathrm{Irr}_{p'}(\mathbf{N}_G(P))$ such that $f(\chi^\sigma) = f(\chi)^\sigma$ for every field automorphism $\sigma \in \mathcal{H}_{p,n}$, where n is a multiple of $|G|$.

Next, we concentrate on the prime $p = 2$. Let n be a positive integer, and write $m = n_{2'}$. Also, write $\mathcal{H} = \mathcal{H}_{2,n}$, and let $\mathbb{F} = \mathbb{Q}_n^{\mathcal{H}}$ be the fixed-field of $\mathcal{H}$. Observe that $\mathbb{F} \subseteq \mathbb{Q}_m$ because $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}_m) \subseteq \mathcal{H}$.

Now if d is a positive square-free odd integer, we consider the "Gauss sum"

$$s_d = \sum_{i=0}^{d-1} \zeta^{i^2}$$

where $\zeta = \exp(2\pi i/d)$. It is well known, and not very hard to prove, that $s_d = \pm\sqrt{\epsilon_d d}$, where, as in the introduction, $\epsilon_d = \pm 1$, where $\epsilon_d \equiv d \pmod 4$. It follows that $\sqrt{\epsilon_d d}$ lies in the cyclotomic field $\mathbb{Q}_d$.

Lemma 5.3. *Let $d > 1$ be a square-free odd integer divisor of n, and note that the Gauss sum s_d lies in $\mathbb{Q}_n$. Assume that there is at least one prime divisor p of d such that 2 is not a square modulo p. Then there exists an element $\sigma \in \mathcal{H}$ such that σ fixes all 2-power roots of unity in $\mathbb{Q}_n$ and $\sigma(s_d) = -s_d$.*

Proof. First, recall that for odd integers t, we have $\epsilon_t \equiv t \bmod 4$, so we have

$$\epsilon_d \equiv d = \prod_r r \equiv \prod_r \epsilon_r \pmod 4,$$

where r runs over the distinct prime divisors of d. It follows that

$$\epsilon_d d = \prod_r \epsilon_r r,$$

and thus up to a sign, s_d is the product of the Gauss sums s_r as r runs over the prime divisors of d.

Suppose that p is a prime divisor of d such that 2 is not a square modulo p, and let σ be the unique automorphism of $\mathbb{Q}_n$ that fixes p'-roots of unity and squares p-power roots of unity, so in particular, σ fixes all 2-power roots of unity. Then $\sigma \in \mathcal{H}$, and σ fixes s_r for all prime divisors $r \neq p$ of d. We will show that $\sigma(s_p) = -s_p$, so $\sigma(s_d) = -s_d$, as required.

Now let ζ be a primitive p-th root of unity so (up to a possible sign ambiguity) we have

$$s_p + \sigma(s_p) = \sum_{k=0}^{p-1} \zeta^{k^2} + \sum_{k=0}^{p-1} \zeta^{2k^2} = 2 + \sum_{k=1}^{p-1} \zeta^{k^2} + \sum_{k=1}^{p-1} \zeta^{2k^2}.$$

Since p is prime, we see that as k runs over the set $\{1, \ldots, p-1\}$, the values of k^2 are all of the $(p-1)/2$ quadratic residues modulo p, each taken twice. Also, by assumption, 2 is not a square modulo p, so the values of $2k^2$ are all of the $(p-1)/2$ nonresidues modulo p, each taken twice. We conclude that

$$s_p + \sigma(s_p) = 2 + \sum_{k=1}^{p-1} \zeta^{k^2} + \sum_{k=1}^{p-1} \zeta^{2k^2} = 2 + 2\sum_{j=1}^{p-1} \zeta^j = 2\sum_{j=0}^{p-1} \zeta^j = 0$$

as wanted. □

Lemma 5.4. *Let $d > 1$ be a square-free integer, and suppose that i and $\sqrt{d}$ are contained in $\mathbb{Q}_n$ for some positive integer n. Let $\mathbb{F}$ be the fixed field of $\mathcal{H}$, as above, write $\mathbb{E} = \mathbb{Q}(i, \sqrt{d})$, and assume that $\mathbb{F} \cap \mathbb{E} > \mathbb{Q}$. Then d is odd and 2 is a square modulo each prime divisor of d.*

Proof. Since $\mathbb{Q}(\sqrt{d})$ is a real field, we have $\mathbb{Q}(\sqrt{d}) \neq \mathbb{Q}(i)$, and thus $|\mathbb{E} : \mathbb{Q}| = 4$. It follows that $\mathbb{E}$ has exactly three subfields having degree 2 over $\mathbb{Q}$, namely $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{d})$ and $\mathbb{Q}(i\sqrt{d})$. By assumption, $\mathbb{E} \cap \mathbb{F} > \mathbb{Q}$, so at least one member of the set $\{i, \sqrt{d}, i\sqrt{d}\}$ must lie in $\mathbb{F}$.

The automorphism of $\mathbb{Q}_n$ that fixes odd-order roots of unity and maps each 2-power root of unity to its reciprocal lies in $\mathcal{H}$, and it follows that $i \notin \mathbb{F}$, so either $\sqrt{d}$ or $i\sqrt{d}$ lies in $\mathbb{F}$.

Suppose now that d is even. Write $d = 2e$, and note that since d is square-free, e must be odd. By assumption, $\sqrt{d}$ lies in $\mathbb{Q}_n$, so it follows by Theorem 2.8 that 8 divides n, and thus $\mathbb{Q}_8 \subseteq \mathbb{Q}_n$.

Now $\mathbb{Q}_8$ has an automorphism that fixes i and maps $\sqrt{2}$ to $-\sqrt{2}$, and it is easy to see by elementary Galois theory that this automorphism extends to an automorphism τ of $\mathbb{Q}_n$ that fixes all odd-order roots of unity. Then $\tau \in \mathcal{H}$, so τ acts trivially on $\mathbb{F}$, and thus τ fixes at least one of $\sqrt{d}$ or $i\sqrt{d}$.

Now τ fixes i, and it follows that τ fixes $\sqrt{d}$. Also, since $\sqrt{d} = \sqrt{2}\sqrt{e}$ and $\tau(\sqrt{2}) = -\sqrt{2}$, we see that $\tau(\sqrt{e}) = -\sqrt{e}$.

The Gauss sum s_e lies in $\mathbb{Q}_e$, and since τ fixes odd-order roots of unity, it follows that τ fixes s_e. Also, either $s_e = \pm\sqrt{e}$ or $s_e = \pm i\sqrt{e}$, so τ fixes at least one of $\sqrt{e}$ or $i\sqrt{e}$. This is a contradiction, however, because τ fixes i, but it does not fix $\sqrt{e}$. We deduce that d is odd, as required.

Now suppose that 2 is not a square modulo p for some prime divisor p of d, and let $\sigma \in \mathcal{H}$ be as in Lemma 5.3, so σ fixes i and $\sigma(s_d) = -s_d$, where s_d is the Gauss sum for d.

Either $\sqrt{d}$ or $i\sqrt{d}$ lies in $\mathbb{F}$, so σ fixes at least one of these elements. Also, σ fixes i, and it follows that σ fixes both $\sqrt{d}$ and $i\sqrt{d}$. One of these elements is s_d (up to a sign) and thus σ fixes s_d. This is a contradiction, however, since $\sigma(s_d) = -s_d$ and $s_d \neq 0$. It follows that 2 is a square modulo p for each prime divisor p of d. □

The following result is a weaker version of Theorem B. Its proof does not use the simple group classification, but instead it assumes the validity of the (unproved) Galois-McKay conjecture for the prime 2.

Theorem 5.5. *Let $\chi \in \mathrm{Irr}(G)$, where G is a finite group, and let $\gamma = \sqrt{\epsilon d}$, where $\epsilon = \pm 1$ and $d > 1$ is a square-free integer. Then*

(a) *If χ is 2-rational and $\gamma \in \mathbb{Q}(\chi)$, then d is odd and $\epsilon = \epsilon_d$, where as before, $\epsilon_d \equiv d$ mod 4.*
(b) *If χ is not 2-rational, suppose χ has odd degree, and assume that either 2 divides d, or else that 2 is not a square for some prime divisor p of d. Then $\mathbb{Q}(\chi) \neq \mathbb{Q}(\gamma)$.*

Note that Theorem 5.5 differs from Theorem B in just two respects. Theorem 5.5(b), requires the assumption that either 2 divides d, or else that 2 is not a square modulo p for at least one prime divisor p of d. Also, there is no guarantee in Theorem 5.5(b) that $i \in \mathbb{Q}(\chi)$.

Proof of Theorem 5.5 assuming Galois-McKay. In the case where χ is 2-rational, the result follows from Corollary 2.11, exactly as in the proof of Theorem B. We can thus assume that χ is not 2-rational, that it has odd degree, that either d is even or else 2 is not a square modulo some prime divisor p of d, and that $\mathbb{Q}(\chi) = \mathbb{Q}(\gamma)$, and we work to derive a contradiction.

Let $n = |G|$ and $m = n_{2'}$. Also, let $P \in \mathrm{Syl}_2(G)$, and write $N = \mathbf{N}_G(P)$. By the Galois-McKay conjecture for the prime 2, there exists an odd-degree character $\chi^* \in \mathrm{Irr}(N)$ such that the stabilizers in $\mathcal{H}$ of χ and χ^* are identical, and thus $\mathbb{F}(\chi) = \mathbb{F}(\chi^*)$.

Since χ is not 2-rational, $\mathbb{F}(\chi) \not\subseteq \mathbb{Q}_m$ and thus $\mathbb{F}(\chi^*) \not\subseteq \mathbb{Q}_m$. We have seen, however, that $\mathbb{F} \subseteq \mathbb{Q}_m$, and we deduce that χ^* is not 2-rational. Also, since χ^* has odd degree, we can apply Corollary 5.2 to the group N to deduce that

$$i \in \mathbb{Q}(\chi^*) \subseteq \mathbb{F}(\chi^*) = \mathbb{F}(\chi) = \mathbb{F}(\gamma)$$

where the final equality holds because $\mathbb{Q}(\chi) = \mathbb{Q}(\gamma)$.

Now write $\mathbb{E} = \mathbb{Q}(i, \gamma)$, and note that $\mathbb{E}$ is the field $\mathbb{Q}(i, \sqrt{d})$ of Lemma 5.4. Observe that $\mathbb{E} \subseteq \mathbb{F}(\gamma)$ because $\mathbb{F}(\gamma)$ contains both i and γ. Also, since $\gamma \in \mathbb{E}$, we see that no proper subfield of $\mathbb{F}(\gamma)$ contains both $\mathbb{E}$ and $\mathbb{F}$. By Theorem 18.22 of [I1], therefore, we have $|\mathbb{E} : \mathbb{E} \cap \mathbb{F}| = |\mathbb{F}(\gamma) : \mathbb{F}| \leq 2$, where the inequality holds because $\gamma^2 \in \mathbb{Q} \subseteq \mathbb{F}$.

Now $|\mathbb{E} : \mathbb{Q}| = 4$ and $|\mathbb{E} : \mathbb{E} \cap \mathbb{F}| \leq 2$, so $\mathbb{E} \cap \mathbb{F} > \mathbb{Q}$. We can thus apply Lemma 5.4 to deduce that d is odd and that 2 is a square modulo each prime divisor of d. This is the desired contradiction. □

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.

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

[GKNT] E. Giannelli, A. S. Kleshchev, G. Navarro, and Pham Huu Tiep, Restriction of odd degree characters and natural correspondences, *Int. Math. Res. Not. IMRN* 2017, no. 20, 6089–6118.

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

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

[H] B. Huppert, '*Endliche Gruppen*', Springer–Verlag, Berlin, 1967.

[I1] I. M. Isaacs, '*Algebra (a graduate course)*', Brooks & Cole Publishing Company, California 1994.

[I2] I. M. Isaacs, '*Character Theory of Finite Groups*', AMS, Providence, 2008.

[IN] I. M. Isaacs and G. Navarro, Characters of p'-degree of p-solvable groups, *J. Algebra* **246** (2001), 394–413.

[KS] W. M. Kantor and A. Seress, Prime power graphs for groups of Lie type, *J. Algebra* **247** (2002), 370–434.

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

[LS] M. W. Liebeck and G.M. Seitz, '*Unipotent and Nilpotent Classes in Simple Algebraic Groups and Lie Algebras*', Mathematical Surveys and Monographs, Vol. **180**, American Mathematical Society, Providence, RI, 2012.

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

[M] G. Malle, The Navarro–Tiep Galois conjecture for $p = 2$, *Arch. Math.* **112** (2019), 449–457.

[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, 2018.

[NT1] G. Navarro and Pham Huu Tiep, Real groups and Sylow 2-subgroups, *Adv. Math.* **299** (2016), 331–360.

[NT2] G. Navarro and Pham Huu Tiep, Irreducible representations of odd degree, *Math. Annalen* **365** (2016), 1155–1185.

[NT3] G. Navarro and Pham Huu Tiep, Sylow subgroups, exponents, and character tables, *Trans. Amer. Math. Soc.* **372** (2019), 4263–4291.

[NTT] G. Navarro and Pham Huu Tiep, and A. Turull, p-rational characters and self-normalizing Sylow p-subgroups, *Represent. Theory* **11** (2007), 84–94.

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

[W] S. H. Weintraub, '*Galois Theory*', Universitext, Springer, 2009.

Department of Mathematics, University of Wisconsin,480 Lincoln Drive, Madison, WI 53706, USA
E-mail address: isaacs@math.wisc.edu

Department of Mathematics, Imperial College, London SW7 2BZ, England
E-mail address: m.liebeck@imperial.ac.uk

Department of Mathematics, Universitat de València, 46100 Burjassot, València, Spain
E-mail address: gabriel@uv.es

Department of Mathematics, Rutgers University, Piscataway, NJ 08854, USA
E-mail address: tiep@math.rutgers.edu