Arch. Math. 110 (2018), 99–108

0003-889X/18/020099-10
published online 7 December 2017
https://doi.org/10.1007/s00013-017-1127-z

Archiv der Mathematik

Finite groups with three rational conjugacy classes

Dan Rossi

Abstract. We show that if a finite group G has exactly three rational conjugacy classes, then G also has exactly three rational-valued irreducible complex characters. This generalizes a result of Navarro and Tiep (Trans Amer Math Soc 360:2443–2465, 2008) and partially answers in the affirmative a conjecture of theirs. We also give a family of examples of non-solvable groups with exactly three rational conjugacy classes.

Mathematics Subject Classification. Primary 20C15, 20E45.

Keywords. Rational irreducible character, Rational conjugacy class.

1. Introduction. Let G be a finite group. It is well known that the character theory of G controls, to a degree, the structure of G itself. Over the last decade a picture has begun to emerge that suggests the fields in which these character values lie play some role in understanding the extent of this control. Several classical results involving the irreducible characters of G have been generalized to versions that involve only those irreducible characters taking values in some appropriate field $\mathbb{F}$—see, e.g., [1,7,9].

If $\mathbb{F} \subseteq \mathbb{C}$ is any subfield of the complex numbers and if χ is any complex character of G, then we say that χ is an **$\mathbb{F}$-character** if $\chi(x) \in \mathbb{F}$ for every element $x \in G$. We write $\mathrm{Irr}_{\mathbb{F}}(G)$ for the set of irreducible $\mathbb{F}$-characters of G. Analogously, if $x \in G$ and $\chi(x) \in \mathbb{F}$ for every $\chi \in \mathrm{Irr}(G)$, then we say that x is an **$\mathbb{F}$-element** of G. Of course, if x is an $\mathbb{F}$-element, then so is every G-conjugate of x and we may refer unambiguously to the conjugacy class x^G as an **$\mathbb{F}$-class**. We write $\mathrm{Cl}_{\mathbb{F}}(G)$ for the set of $\mathbb{F}$-classes of G.

It is very natural to wonder about possible relationships between $\mathrm{Irr}_{\mathbb{F}}(G)$ and $\mathrm{Cl}_{\mathbb{F}}(G)$ for various fields $\mathbb{F}$. Of particular interest is the case $\mathbb{F} = \mathbb{Q}$ or

This work constitutes a portion of the author's Ph.D. dissertation under the direction of Pham Huu Tiep. Prof. Tiep's support is gratefully acknowledged. Part of the research was supported by NSF grant DMS-1201374.

more generally $\mathbb{F} = \mathbb{Q}_p$, the p-th cyclotomic field. One reason for this is that $\mathbb{F}$-generalizations mentioned above frequently involve $\mathbb{F} = \mathbb{Q}_p$, especially for statements involving the p-local structure of G. Often, the deepest and most difficult results involve $p = 2$ and, correspondingly, $\mathbb{Q}_2 = \mathbb{Q}$.

One of the most fundamental relationships between the irreducible characters of G, on one side, and the conjugacy classes of G, on the other, is that they are equal in number. In view of this, one might guess that $|\operatorname{Irr}_{\mathbb{F}}(G)| = |\operatorname{Cl}_{\mathbb{F}}(G)|$. But actually this is not true for arbitrary $\mathbb{F}$. This includes the important situation $\mathbb{F} = \mathbb{Q}$, where fairly little is known. (In contrast, for example, it is always true that $|\operatorname{Irr}_{\mathbb{R}}(G)| = |\operatorname{Cl}_{\mathbb{R}}(G)|$, and it is fairly easy to show this—see Lemma 2.1 below). In [8] Navarro & Tiep proved the following result.

Theorem. *Let G be a finite group.*
(a) $|\operatorname{Irr}_{\mathbb{Q}}(G)| = 1$ *if and only if* $|\operatorname{Cl}_{\mathbb{Q}}(G)| = 1$.
(b) $|\operatorname{Irr}_{\mathbb{Q}}(G)| = 2$ *if and only if* $|\operatorname{Cl}_{\mathbb{Q}}(G)| = 2$.

In view of this they conjectured the following (private communication):

Conjecture A. Let G be a finite group. Then $|\operatorname{Irr}_{\mathbb{Q}}(G)| = 3$ if and only if $|\operatorname{Cl}_{\mathbb{Q}}(G)| = 3$.

In fact, this is the best possible generalization of the Navarro–Tiep theorem. For example, the group G of order 672 with GAP `SmallGroup` identifier 128 has $|\operatorname{Irr}_{\mathbb{Q}}(G)| = 4$ and $|\operatorname{Cl}_{\mathbb{Q}}(G)| = 6$.

The main result in this paper shows that one direction of the Navarro–Tiep conjecture is true. Specifically, we show the following.

Theorem A. *Let G be any finite group. If $|\operatorname{Cl}_{\mathbb{Q}}(G)| = 3$, then $|\operatorname{Irr}_{\mathbb{Q}}(G)| = 3$.*

Both the Navarro–Tiep result in [8] and our Theorem A require the classification of finite simple groups, which seems to indicate that rationality questions are of a deep nature.

Remark. The converse to Theorem A is considerably more difficult. The structure of groups G with $|\operatorname{Irr}_{\mathbb{Q}}(G)| = 3$ can be determined. For solvable groups they have 2-length one, by [10]. For non-solvable groups it can be shown that $G/O_{2'}(G)$ contains a normal subgroup S, where S is a quasisimple group of Lie type from an explicit list, and $|G/O_{2'}(G) : S|$ is odd. In particular, such a group has a unique non-abelian composition factor, and the possibilities are rather limited. In either the solvable or the non-solvable case, the main obstacle to proving Conjecture A involves the situation where $O_{2'}(G)$ contains non-trivial rational elements. Details about these results will appear elsewhere.

1.1. Notation. All groups considered are finite and G always denotes a finite group. If n is an integer and p a prime, then n_p, resp. $n_{p'}$, is the p-, resp. p'-part, of n (i.e. the largest p-power dividing n, resp. n/n_p). Likewise, if $g \in G$, then g_p and $g_{p'}$ are the p- and p'-parts of g. We define $\mathbb{Q}_n$ to be the cyclotomic extension of $\mathbb{Q}$ obtained by adjoining a primitive n-th root of unity. The subgroup $O_p(G)$, resp. $O_{p'}(G)$, is the largest subgroup of G having p-power order, resp. order coprime to p. The set of irreducible complex characters of G is $\operatorname{Irr}(G)$. If $N \triangleleft G$

and $\theta \in \mathrm{Irr}(N)$, then $\mathrm{Irr}(G|\theta)$ is the set of irreducible characters of G such that the restriction $\chi_{|N}$ contains θ as an irreducible constituent. If $x \in G$, then $x^G = \mathrm{cl}_G(x)$ is the G-conjugacy class of x. The set of conjugacy classes of G is $\mathrm{Cl}(G)$. The order of $g \in G$ is $o(g)$.

2. Preliminaries. Here, we record some useful results about conjugacy classes, characters, and fields of values.

The following is all well known, and elementary.

Lemma 2.1. *Let G be any finite group.*

(a) *The element $x \in G$ is real if and only if x and x^{-1} are G-conjugate.*
(b) $|\mathrm{Irr}_{\mathbb{R}}(G)| = |\mathrm{Cl}_{\mathbb{R}}(G)|$.
(c) *If $|G|$ is odd, then $|\mathrm{Cl}_{\mathbb{R}}(G)| = 1 = |\mathrm{Irr}_{\mathbb{R}}(G)|$.*

Proof. Part (a) is [6, Problem 2.11]; (b) is [6, Problem 6.13]; and (c) combines (b) and [6, Problem 3.16]. □

The next two statements give a connection between rational characters and rational elements of G, and those of subgroups or quotients of G.

Lemma 2.2. *Let $N \lhd G$ and $\theta \in \mathrm{Irr}_{\mathbb{R}}(N)$. If $|G : N|$ is odd, then there is a unique $\chi \in \mathrm{Irr}_{\mathbb{R}}(G|\theta)$. In particular, if θ is rational, then χ is rational.*

Proof. This is [8, Corollary 2.2]. □

Lemma 2.3. *Let G be a finite group. Then the following statements hold.*

(a) *If $x \in H \leq G$ is rational in H, then x is rational in G.*
(b) *If $N \lhd G$ and $x \in G$ is rational, then $xN \in G/N$ is rational.*
(c) *Let $N \lhd G$. If G/N has a rational element with prime order p, then G has a rational element of order p.*

Proof. See [8, Lemmas 5.1 and 5.2]. □

Let $\mathbb{F} \subseteq \mathbb{C}$ be any subfield of the complex numbers. A subgroup $H \leq G$ is called **$\mathbb{F}$-free in** G if H contains no non-trivial $\mathbb{F}$-elements of G. We emphasize that the notion of H being $\mathbb{F}$-free is always relative to some overgroup G.

Theorem 2.4. *Suppose that $N \lhd G$ is $\mathbb{F}$-free in G. Then $\mathrm{Irr}_{\mathbb{F}}(G) = \mathrm{Irr}_{\mathbb{F}}(G/N)$ and the natural map $G \to G/N$ induces a bijection $\mathrm{Cl}_{\mathbb{F}}(G) \to \mathrm{Cl}_{\mathbb{F}}(G/N)$.*

Proof. Combine Theorems A and B of [4]. □

Theorem 2.4 allows us to argue by induction on $|G|$. It says that we can factor out $\mathbb{Q}$-free normal subgroups without changing the count of rational conjugacy classes or rational irreducible characters.

3. The main results. Now we begin proving the main results of this paper. First, we prove Theorem A in special case, where we make some extra assumption about the orders of rational elements. Then, in the next two subsections, we consider the remaining case of Theorem A: first for non-solvable groups and then for solvable groups. Throughout this section, we repeatedly use the fact that an involution is always rational.

3.1. A special case. We recall the Galois action on conjugacy classes and characters. Fix a finite group G of order n and let $\zeta \in \mathbb{C}$ be any n-th root of unity. Let $\sigma \in \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}) =: \mathcal{G}$, so that $\zeta^\sigma = \zeta^s$ for some integer s coprime to n. Note that σ is completely determined by s, and that s does not depend on the choice of ζ. We define an action of $\mathcal{G}$ on G by $x^\sigma := x^s$, for any $x \in G$. This extends to an action on $\mathrm{Cl}(G)$ by defining $(x^G)^\sigma := (x^\sigma)^G$. For $\chi \in \mathrm{Irr}(G)$ we also define $\chi^\sigma := \sigma \circ \chi$. Clearly, an element, conjugacy class, or character of G is rational if and only if it is $\mathcal{G}$-invariant.

The following observation is trivial.

Lemma 3.1. *Let $n = |G|$ and let $\sigma \in \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})$. Let $x \in G$ and assume that σ fixes every root of unity with order $o(x)$. Then $x^\sigma = x$.*

Proof. Let ζ be an n-th root of unity and assume $\zeta^\sigma = \zeta^s$. Let μ be an $o(x)$-th root of unity. As $o(x)$ divides n, μ is a power of ζ, and thus $\mu = \mu^\sigma = \mu^s$. We conclude that $s \equiv 1 \pmod{o(x)}$, so $x^\sigma = x^s = x$. □

Next, let us establish some notation. Let n be any positive integer and let $\mathcal{G} := \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})$. Let p be any prime dividing n. Then restriction gives an isomorphism

$$\Theta : \mathcal{G} \to \mathrm{Gal}(\mathbb{Q}_{n_p}/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}_{n_{p'}}/\mathbb{Q}); \Theta(\sigma) := (\sigma_{|\mathbb{Q}_{n_p}}, \sigma_{|\mathbb{Q}_{n_{p'}}}).$$

Let $\mathcal{G}_p := \Theta^{-1}(\mathrm{Gal}(\mathbb{Q}_{n_p}/\mathbb{Q}) \times 1)$ and let $\mathcal{G}_{p'} := \Theta^{-1}(1 \times \mathrm{Gal}(\mathbb{Q}_{n_{p'}}/\mathbb{Q}))$, so $\mathcal{G} = \mathcal{G}_p \times \mathcal{G}_{p'}$. By construction, $\mathcal{G}_p \simeq \mathrm{Gal}(\mathbb{Q}_{n_p}/\mathbb{Q})$ and $\mathcal{G}_p$ fixes p'-roots of unity in $\mathbb{Q}_n$. Working by induction on n, we obtain a direct product factorization

$$\mathcal{G}_{p'} = \prod_{r|n_{p'}, r \text{ prime}} \mathcal{G}_r,$$

where $\mathcal{G}_r \simeq \mathrm{Gal}(\mathbb{Q}_{n_r}/\mathbb{Q})$ and $\mathcal{G}_r$ fixes r'-roots of unity in $\mathbb{Q}_{n_{p'}}$. Of course, each $\mathcal{G}_r$ also fixes p-power roots of unity in $\mathbb{Q}_n$ (since $\mathcal{G}_{p'}$ does) and thus $\mathcal{G}_r$ actually fixes r'-roots of unity in $\mathbb{Q}_n$. Putting everything together, we have a direct product factorization

$$\mathcal{G} = \prod_{p|n, p \text{ prime}} \mathcal{G}_p,$$

where $\mathcal{G}_p \simeq \mathrm{Gal}(\mathbb{Q}_{n_p}/\mathbb{Q})$ and fixes p'-roots of unity in $\mathbb{Q}_n$.

When p is odd, $\mathcal{G}_p$ is cyclic and we choose a generator σ_p. When $p = 2$, then we write $\mathcal{G}_2 = \langle \sigma_2 \rangle \times \langle \sigma_0 \rangle$, where σ_2 is inverting 2-power roots of unity and σ_0 has order $n_2/4$ (or $\sigma_0 = 1$ if $n_2 \leq 4$).

We will keep all of this notation in the proof of the following theorem.

Theorem 3.2. *Let G be a finite group and suppose that $|\mathrm{Cl}_\mathbb{Q}(G)| = 3$. Moreover, assume that G has no rational element of order 4. Then $|\mathrm{Irr}_\mathbb{Q}(G)| = 3$.*

Proof. The hypothesis implies that the non-conjugate rational elements of G have orders $1, 2$, and p for some prime p (possibly $p = 2$). Let u^G and x^G denote the non-trivial rational classes of G, where u is an involution and $o(x) = p$.

Aiming for a contradiction, assume that $|\mathrm{Irr}_{\mathbb{Q}}(G)| \geq 4$. Let $n = |G|$ and $\mathcal{G} = \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})$. Using the notation above, define

$$\sigma = \prod_{r|n, r \text{ prime}} \sigma_r.$$

By Brauer's lemma [6, Lemma 6.32], σ fixes the same number of G-conjugacy classes as it does irreducible characters of G. Certainly, every element of $\mathrm{Cl}_{\mathbb{Q}}(G)$ and $\mathrm{Irr}_{\mathbb{Q}}(G)$ is σ-fixed, and so we conclude that there is some class $y^G \notin \mathrm{Cl}_{\mathbb{Q}}(G)$ but with $(y^G)^\sigma = y^G$. Obviously, if z is any power of y, then $(z^G)^\sigma = z^G$ as well. We will find some power z of y, such that $z^G \notin \{1^G, u^G, x^G\}$ but such that z is rational. This is the desired contradiction.

If $4 \mid o(y)$, then we choose $z = y^{o(y)/4}$, having order 4. Now assume $4 \nmid o(y)$. Since y is not rational, $o(y) \neq 2$ and so there is some odd prime r dividing $o(y)$. If $r \nmid o(x)$, we choose $z = y_r$. In the remaining case, y is a $\{2, p\}$-element and $o(y_2) \leq 2$. In this case we choose $z = y$. In every case, $z^G \notin \{1^G, u^G, x^G\}$.

If $o(z) = 4$, then Lemma 3.1 implies that for every odd prime $r \mid n$, z is fixed by $\sigma_r \in \mathcal{G}$. Thus

$$z^G = (z^G)^\sigma = (z^{\sigma_2})^G = (z^{-1})^G,$$

and we conclude that z is rational. Otherwise, write $z = z_2 z_r$ where z_2 is either trivial or an involution and r is the unique odd prime dividing $o(z)$. Using Lemma 3.1 as above, we deduce that z_2 is $\mathcal{G}$-fixed and z_r is fixed by σ_0 and by σ_ℓ for every prime $\ell \neq r$. Thus $z^G = (z^G)^\sigma = (z^G)^{\sigma_r}$ and we conclude that z^G is $\mathcal{G}$-invariant, i.e. rational. The proof is complete. □

3.2. Non-solvable groups. By Theorem 3.2, to complete the proof of Theorem A, we may assume that the rational elements of G have orders $1, 2$, and 4. We now consider this case when G is non-solvable.

In what follows, if $\phi \in \mathrm{Irr}(S)$ and $x \in S$, we shall use the notation $\mathbb{Q}(\phi)$ for the field extension of $\mathbb{Q}$ obtained by adjoining all of the values $\phi(y)$ for $y \in S$ and $\mathbb{Q}(x^S)$ for the extension obtained by adjoining all of the values $\psi(x)$ for $\psi \in \mathrm{Irr}(S)$.

Lemma 3.3. *Suppose that $S \lhd G$ with $|G : S|$ odd. Let $\theta \in \mathrm{Irr}_{\mathbb{R}}(S)$, and let $\{\theta = \theta_1, \ldots, \theta_n\}$ be the set of G-conjugates of θ. If $\sum_{i=1}^n \theta_i$ is rational-valued then there is a unique rational character $\psi \in \mathrm{Irr}(G|\theta)$.*

Proof. By Lemma 2.2, there is a unique character $\psi \in \mathrm{Irr}_{\mathbb{R}}(G|\theta)$. By hypothesis, $\psi_{|S} = e \sum_{i=1}^n \theta_i$ is rational. Let $K := \mathbb{Q}(\psi)$ and $\tau \in \mathrm{Gal}(K/\mathbb{Q})$. Since $\psi_{|S}$ is rational, τ permutes the constituents θ_i. If $\theta^\tau = \theta_i$, then

$$\psi^\tau \in \mathrm{Irr}_{\mathbb{R}}(G|\theta^\tau) = \mathrm{Irr}_{\mathbb{R}}(G|\theta_i) = \mathrm{Irr}_{\mathbb{R}}(G|\theta).$$

It follows from the uniqueness of ψ that $\psi^\tau = \psi$, and so ψ is rational. □

Let $q = 3^{2f+1}$ for some integer $f \geq 1$. For the next lemma, we need a detailed description of the conjugacy classes and characters of $\mathrm{SL}_2(q)$ and $\mathrm{PSL}_2(q)$, and the automorphism action on these classes and characters. We use the notation of [2, Chapter 38], with one change: the (Steinberg) character called ϕ in [2], we will call St. Abusing notation somewhat, we will denote by

the same symbol both an element of $\mathrm{SL}_2(q)$ and its image in $\mathrm{PSL}_2(q)$. It is easy to check that the set

$$\left\{1, u = b^{(q+1)/4}, c, d, a^i, b^j : 1 \leq i, j \leq \frac{q-3}{4}\right\}$$

is a complete set of class representatives for $\mathrm{PSL}_2(q)$, and that

$$\mathrm{Irr}(\mathrm{PSL}_2(q)) = \left\{1, St, \xi_1, \xi_2, \chi_{2i}, \theta_{2j} : 1 \leq i, j \leq \frac{q-3}{4}\right\}.$$

Note that in either $\mathrm{SL}_2(q)$ or $\mathrm{PSL}_2(q)$, the characters ξ_i, η_i can be distinguished by their degree and their value on c; conversely, the classes c^S, d^S, $(zc)^S$, and $(zd)^S$ are distinguished by their value at ξ_1. Similarly, the characters χ_i (resp. θ_j) are distinguished by their degree and values at a (resp. b) and likewise the classes $(a^i)^S$ (resp. $(b^j)^S$) are distinguished by their values at χ_1 (resp. θ_1; also, for $\mathrm{PSL}_2(q)$, the classes are distinguished by their values at χ_2, resp. θ_2, instead).

Finally, recall that $\mathrm{Aut}(S) = \langle\delta\rangle \times \langle\sigma\rangle \simeq C_2 \times C_{2f+1}$, where the diagonal automorphism δ exchanges the members of each pair $\{c^S, d^S\}$, $\{(zc)^S, (dc)^S\}$, $\{\xi_1, \xi_2\}$, and $\{\eta_1, \eta_2\}$ and fixes the remaining classes and characters; and the field automorphism σ fixes all members of the above pairs and permutes the sets $\{(a^i)^S\}$, $\{(b^j)^S\}$, $\{\chi_i\}$, and $\{\theta_j\}$.

Lemma 3.4. *Let $q = 3^{2f+1}$ and let $S = \mathrm{PSL}_2(q)$ or $S = \mathrm{SL}_2(q)$. Then there is a bijection $\phi \mapsto C_\phi$ from $\mathrm{Irr}(S)$ to $\mathrm{Cl}(S)$. If $x \in C_\phi$, $g \in \mathrm{Aut}(S)$, and $\tau \in \mathrm{Gal}(\mathbb{Q}_{|S|}/\mathbb{Q})$, then we can choose the bijection to satisfy the following properties:*

(a) $\mathbb{Q}(\phi) = \mathbb{Q}(C_\phi)$
(b) $(C_\phi)^\tau = (x^\tau)^S$
(c) $(C_\phi)^g = (x^g)^S$
(d) $(C_\phi)^g = (C_\phi)^\tau$ *if and only if* $\phi^g = \phi^\tau$.

Proof. Consider the bijections

$$\begin{cases} 1^S \leftrightarrow 1_S \\ z^S \leftrightarrow St \\ c^S \leftrightarrow \xi_1 \\ d^S \leftrightarrow \xi_2 \\ (zc)^S \leftrightarrow \eta_1 \\ (zd)^S \leftrightarrow \eta_2 \\ (a^i)^S \leftrightarrow \chi_i \\ (b^j)^S \leftrightarrow \theta_j \end{cases} \text{for } S = \mathrm{SL}_2(q), \text{ and } \begin{cases} 1^S \leftrightarrow 1_S \\ u \leftrightarrow St \\ c \leftrightarrow \xi_1 \\ d \leftrightarrow \xi_2 \\ (a^i)^S \leftrightarrow \chi_{2i} \\ (b^j)^S \leftrightarrow \theta_{2j} \end{cases} \text{for } S = \mathrm{PSL}_2(q).$$

Now (a) and (b) follow by inspecting the character tables in [2, Chapter 38]; (c) from the discussion preceding the lemma; and (d) from (b) and (c). □

Lemma 3.5. *Suppose that $S \triangleleft G$ where $S = \mathrm{PSL}_2(q)$ or $S = \mathrm{SL}_2(q)$ and assume that $|G : S|$ is odd. Then $|\mathrm{Irr}_{\mathbb{Q}}(G)| = |\mathrm{Cl}_{\mathbb{Q}}(G)|$.*

Proof. The group G/S contains no non-trivial rational elements by Lemma 2.1. Thus, every rational element of G is actually contained in S, by Lemma 2.3. If $\chi \in \mathrm{Irr}_{\mathbb{Q}}(G|\theta)$ for some $\theta \in \mathrm{Irr}(S)$, then there is some element $g \in G$ such that $\theta^g = \overline{\theta}$. As $|G/S|$ is odd we have $g_2 \in S$ and therefore it is no loss to assume that g has odd order. But because $\theta = \theta^{g^2}$, we conclude that $\theta = \overline{\theta}$ is real. This observation, combined with Lemma 3.3, implies that $|\mathrm{Irr}_{\mathbb{Q}}(G)|$ is equal to the number of G-orbits on $\mathrm{Irr}(S)$ having rational orbit-sum. By Lemma 3.4, this is equal to the number of rational G-conjugacy classes contained in S. □

Recall that the **layer** of a group G is the subgroup $E(G)$ generated by all subnormal, quasisimple subgroups of G (called **components**). In fact, $E(G)$ is a central product of those subgroups. The **generalized Fitting subgroup** of G is $F^*(G) := E(G)F(G)$, where $F(G)$ is the Fitting subgroup.

Lemma 3.6. *Suppose that G is non-solvable, that $F^*(G) = O_2(G)$, and that $O_2(G)$ contains only one G-conjugacy class of involutions. Then G contains a rational element of order* 3.

Proof. This is shown in steps (2)–(4) in the proof of [8, Theorem 11.2]. □

Part of the proof of the next theorem is also adapted from [8, Proof of Theorem 11.2].

Theorem 3.7. *Suppose that G is non-solvable, $|\mathrm{Cl}_{\mathbb{Q}}(G)| = 3$, and the rational elements of G have orders* $1, 2,$ *and* 4. *Then $|\mathrm{Irr}_{\mathbb{Q}}(G)| = 3$.*

Proof. First, note that $O_{2'}(G)$ is $\mathbb{Q}$-free in G. Arguing by induction on $|G|$ and applying Theorem 2.4, we may therefore assume that $O_{2'}(G) = 1$. If, in addition, $E(G) = 1$, then $F = F^*(G) = O_2(G)$. Using Lemma 3.6, we deduce that $E(G) > 1$. Write $E(G) = \prod_{j=1}^{n} K_j$, where each K_j is a component of G and the product is central. We claim that each $K_j/Z(K_j)$ has the form $\mathrm{PSL}_2(3^{2f+1})$ for some (possibly distinct) integers $f \geq 1$; if not, then some $K_j/Z(K_j)$ contains a rational element of order 3 or order 5, by [8, Lemma 11.1], and therefore G does too, by Lemma 2.3. In particular each K_j is isomorphic to either $\mathrm{SL}_2(3^{2n_j+1})$ or to $\mathrm{PSL}_2(3^{2n_j}+1)$.

Next, we claim that $n = 1$. Assume not, and choose involutions $z_1 \in K_1$ and $z_2 \in K_2$. If $K_1 \cap K_2 = 1$, then z_1 and $z_1 z_2$ are non-conjugate involutions of G (as G permutes the K_j). But the hypotheses of the theorem imply that G has a unique class of involutions. Therefore, $1 < K_1 \cap K_2 \leq Z(K_1) \cap Z(K_2)$. In particular, both $K_i \simeq \mathrm{SL}_2(3^{2n_i+1})$ for $i = 1, 2$, $z_1 = z_2$ is the unique central involution in K_i, and $K_1 K_2 \simeq \frac{K_1 \times K_2}{\langle z_1 z_2 \rangle}$. Choose elements $y_i \in K_i$ of order 4. Now, $(y_1 y_2)^2 = y_1^2 y_2^2 = z_1 z_2 = 1$ and $y_1 \neq y_2^{-1}$ (as $y_1 \notin K_2$), so $o(y_1 y_2) = 2$. As above z_1 and $y_1 y_2$ are non-conjugate involutions in G. This contradiction shows that $n = 1$, as claimed.

Let $E(G) = K_1 =: K$ and let $C = C_G(K) \lhd G$. If $K \simeq \mathrm{PSL}_2(3^{2f+1})$, then $C \cap K = Z(K) = 1$. Since G has a unique class of involutions, we conclude that $|C|$ is odd. So $C \leq O_{2'}(G) = 1$. If instead $K \simeq \mathrm{SL}_2(3^{2f+1})$, then G has a unique involution, namely $1 \neq z \in Z(K)$. Let $R \in \mathrm{Syl}_2(C)$. As $z \in R$, we have $1 < R \cap K \leq Z(K) = \langle z \rangle$. Suppose that there is some element $y \in R$ with order

4 and let $x \in K$ have order 4. As in the previous paragraph, $y^2 = z = x^2$ and so $(xy)^2 = x^2y^2 = z^2 = 1$, and we deduce that xy is an involution of G different from z, a contradiction. Since R has a unique involution and no element of order 4, we conclude that R is cyclic of order 2. By Cayley's Theorem, C has a normal 2-complement X. But then $X \lhd G$ and, since $O_{2'}(G) = 1$, we conclude that $C = R = Z(K)$.

In the previous paragraph, we showed that $C = Z(K)$. Now, $\mathrm{Out}(K) \geq G/CK = G/K$. Any outer automorphism of K with even order fuses the two classes of order-3 elements in K. Since G has no rational elements of order 3, this does not occur. We deduce that $|G : K|$ is odd. By Lemma 3.5, $|\operatorname{Irr}_{\mathbb{Q}}(G)| = |\operatorname{Cl}_{\mathbb{Q}}(G)| = 3$. □

3.3. Solvable groups. Finally, we complete the proof of Theorem A by considering solvable groups with exactly three rational classes, the elements of which have orders $1, 2$, and 4. The next lemma is well known.

Lemma 3.8. *Assume that G has a normal Sylow 2-subgroup P. Then every real element of G is a real element of P.*

Proof. The group G/P, having odd order, has no non-trivial real elements. Thus, every real element of G is contained in P. Let $x \in G$ be real and let $g \in G$ satisfy $gxg^{-1} = x^{-1}$. Then $g^2 \in C_G(x)$ and thus $x_{2'} \in C_G(x)$. So it is no loss to assume that g is a 2-element, refore $g \in P$. □

Lemma 3.9. *Assume that G has a normal Sylow 2-subgroup P and that P has exponent 4. Then $\operatorname{Irr}_{\mathbb{Q}}(G) = \operatorname{Irr}_{\mathbb{R}}(G)$ and $\operatorname{Cl}_{\mathbb{Q}}(G) = \operatorname{Cl}_{\mathbb{R}}(G)$. In particular, $|\operatorname{Cl}_{\mathbb{Q}}(G)| = |\operatorname{Irr}_{\mathbb{Q}}(G)|$.*

Proof. Let X be a 2-complement for G. Since P has exponent 4, $\operatorname{Irr}_{\mathbb{R}}(P) = \operatorname{Irr}_{\mathbb{Q}}(P)$ (every character of P takes values in $\mathbb{Q}_4 = \mathbb{Q}(\sqrt{-1})$). Let $\chi \in \operatorname{Irr}_{\mathbb{R}}(G)$ and let $\tau \in \operatorname{Irr}(P)$ be an irreducible constituent of the restriction $\chi_{|P}$. Then the complex conjugate $\bar{\tau}$ is also a constituent of $\chi_{|P}$, and thus there is some $x \in X$ with $\tau^x = \bar{\tau}$. But then $\tau^{x^2} = \tau$ and, since x has odd order, we conclude that $\tau = \bar{\tau}$, i.e. τ is real. Hence τ is rational. By Lemma 2.2, there is some $\theta \in \operatorname{Irr}_{\mathbb{Q}}(G|\tau)$; but also by Lemma 2.2 there is a unique real character in $\operatorname{Irr}(G|\tau)$, and this is χ. We conclude that $\chi = \theta$ is rational. That $\operatorname{Cl}_{\mathbb{Q}}(G) = \operatorname{Cl}_{\mathbb{R}}(G)$ follows from Lemma 3.8 and the observation that an element of order not exceeding 4 is real if and only if it is rational. For the final claim, apply Lemma 2.1. □

Theorem 3.10. *Suppose that G is solvable, $|\operatorname{Cl}_{\mathbb{Q}}(G)| = 3$, and the rational elements of G have orders $1, 2$, and 4. Then $|\operatorname{Irr}_{\mathbb{Q}}(G)| = 3$.*

Proof. By [5], G has 2-length one. Let $P \in \operatorname{Syl}_2(G)$ and let $L := O_{2'}(G)$. As L is $\mathbb{Q}$-free in G, by working by induction on $|G|$ and applying Theorem 2.4, we may assume that $L = 1$. Thus $P \lhd G$. Let X be a 2-complement.

If P has a unique involution then P is either cyclic or generalized quaternion. An abelian 2-group does not have a real element of order 4, so by Lemma 3.8 we conclude that P is not cyclic. If P is generalized quaternion then the

rational elements of order 4 are not all conjugate in P, but they are all conjugate in G; in particular, X acts non-trivially on P. If P has order exceeding 8 then, as is well known, $\mathrm{Aut}(P)$ is a 2-group and thus X acts trivially on P. We conclude that $P = Q_8$ has exponent 4, and now the result follows from Lemma 3.9.

So we may assume that P has more than one involution, all of which are conjugate in G. By Thompson's theorem [3, Theorem IX.8.6], P is either homocyclic or a **Suzuki 2-group**. Again, an abelian group does not have a real element of order 4, so we conclude that P is a Suzuki 2-group. In particular, P has exponent 4 (see [3, Theorem VIII.7.9]), and thus Lemma 3.9 again implies that $|\mathrm{Irr}_{\mathbb{Q}}(G)| = 3$. The proof is complete. □

Theorem A now follows by combining Theorems 3.2, 3.7, and 3.10.

4. Examples. We give examples of some non-solvable groups G with $|\mathrm{Cl}_{\mathbb{Q}}(G)| = 3 = |\mathrm{Irr}_{\mathbb{Q}}(G)|$. Let $S = \mathrm{PSL}_2(27)$ and let $H = S.3 = S\langle\sigma\rangle$, where σ is the field automorphism of S with order 3. We check that $|\mathrm{Cl}_{\mathbb{Q}}(G)| = 3$, the rational elements having orders $1, 2$, and 7. Since $|H : S| = 3$, Lemma 3.5 implies that $|\mathrm{Irr}_{\mathbb{Q}}(H)| = 3$. Now let r be any prime larger than $|H| + 1$ and let V be any $\mathbb{F}_r[H]$-module. Let G be any extension $V.H$. An element $v \in V$ is rational in G if and only if v is conjugate to all $r - 1$ non-trivial powers of itself. But since $r - 1 > |H|$, this is impossible. In other words, V is $\mathbb{Q}$-free in G. By Theorem 2.4, $|\mathrm{Cl}_{\mathbb{Q}}(G)| = 3 = |\mathrm{Irr}_{\mathbb{Q}}(G)|$.

The same construction, but with $S = \mathrm{SL}_2(3^{2f+1})$, furnishes examples where the rational elements have orders $1, 2$, and 4.

References

[1] S. Dolfi, G. Navarro, and P. H. Tiep, Primes dividing the degrees of the real characters, Math. Z. **259** (2008), 755–774.

[2] L. Dornhoff, Group Representation Theory. Part A: Ordinary Representation Theory, Pure and Applied Mathematics, 7, Marcel Dekker, Inc., New York, 1971.

[3] B. Huppert and N. Blackburn, Finite groups. II, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], 242, Springer-Verlag, Berlin-New York, 1982.

[4] I. M. Isaacs and G. Navarro, Group elements and fields of character values, J. Group Theory **12** (2009), 635–650.

[5] I. M. Isaacs and G. Navarro, Solvable groups having only three rational, classes of 2-elements, Arch. Math. **97** (2011), 199–206.

[6] I. M. Isaacs, Character theory of finite groups, AMS Chelsea Publishing, Providence, RI, 2006. Corrected reprint of the 1976 original [Academic Press, New York].

[7] G. Navarro, L. Sanus, and P. H. Tiep, Real characters and degrees, Israel J. Math. **171** (2009), 157–173.

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

[9] G. Navarro and P. H. Tiep, Degrees of rational characters of finite groups, Adv. Math. **224** (2010), 1121–1142.

[10] J. Tent, 2-length and rational characters of odd degree, Arch. Math. **96** (2011), 201–206.

Dan Rossi
Department of Mathematics,
University of Arizona,
617 N. Santa Rita Ave,
Tucson, AZ 85721,
USA
e-mail: drossi@math.arizona.edu

Received: 26 September 2017