TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 360, Number 5, May 2008, Pages 2443–2465
S 0002-9947(07)04375-9
Article electronically published on November 27, 2007

RATIONAL IRREDUCIBLE CHARACTERS AND RATIONAL CONJUGACY CLASSES IN FINITE GROUPS

GABRIEL NAVARRO AND PHAM HUU TIEP

Dedicated to Professor Michel Broué on the occasion of his sixtieth birthday

ABSTRACT. We prove that a finite group G has two rational-valued irreducible characters if and only if it has two rational conjugacy classes, and determine the structure of any such group. Along the way we also prove a conjecture of Gow stating that any finite group of even order has a non-trivial rational-valued irreducible character of odd degree.

1. INTRODUCTION

One of the fundamental questions in the character theory of finite groups is to analyze fields of values of characters. In this paper, we are focused on the rational-valued irreducible characters of G, probably the most important case. Let us write $\mathrm{Irr}_{\mathrm{rat}}(G)$ for the set of complex irreducible characters of G with values in $\mathbb{Q}$, and $\mathrm{cl}_{\mathrm{rat}}(G)$ for the set of conjugacy classes of rational elements in G.

The relationship between the structure of G and the set $\mathrm{Irr}_{\mathrm{rat}}(G)$ is not fully understood. It is known, for instance, that all irreducible characters of G are rational-valued if and only if all conjugacy classes of G are rational; however, the structure of such a group G is not completely determined until now. It is also known that G has no non-trivial rational-valued irreducible characters if and only if G has odd order, equivalently, $|\mathrm{cl}_{\mathrm{rat}}(G)| = 1$. This result (see Theorem 8.2 below for a proof; see also Corollary 9.7) already requires the classification of finite simple groups. This indicates, in our opinion, that rationality questions in finite groups are of deep nature. Our main goal in this paper is to take the next step and prove the following.

Received by the editors February 6, 2006.
2000 *Mathematics Subject Classification.* Primary 20C15, 20C33, 20E45.
Key words and phrases. Rational irreducible character, rational conjugacy class.
The first author was partially supported by the Ministerio de Educación y Ciencia proyecto MTM2004-06067-C02-01.
Part of this work was done while the first author visited the University of Florida in Gainesville, and he would like to thank the Mathematics Department for its hospitality. Special thanks are due to A. Turull. This paper benefited from conversations with M. Isaacs, A. Moretó, A. Turull and B. Wilkens. The authors are grateful to the referee for pointing out some inaccuracies in an earlier version of the paper as well as for helpful comments that greatly improved the exposition of the paper.
The second author gratefully acknowledges the support of the NSA and the NSF.

Theorem A. *Suppose that G is a finite group. Then G has two irreducible rational-valued characters if and only if G has two rational conjugacy classes.*

In general, it is not true that the number of irreducible rational-valued characters and the number of rational conjugacy classes of G coincides, as is very well-known. There are many examples (solvable and non-solvable) illustrating this. However, there are also many important situations when there is equality, and we are hoping that the techniques that we are developing here will help us to study this in the future, as well as to study various rationality questions about ordinary and Brauer characters.

The proof of Theorem A is surprisingly complicated. It is naturally divided into two cases, according to whether the group G is solvable or not. In each of these cases, both implications will be non-trivial. One of the many (but perhaps the most significant) obstacles toward the proof of Theorem A is that we need to prove not only that groups of even order have non-trivial irreducible rational-valued characters but also something stronger. The following was a conjecture of R. Gow, which we can finally prove.

Theorem B. *If G is a finite group of even order, then G has a non-trivial irreducible rational-valued character of odd degree.*

The structure of non-solvable groups with two rational-valued characters is described in the following theorem. We write $\mathbf{O}^{2'}(G)$ for the smallest normal subgroup of G with odd index, and $\mathbf{O}_{2'}(G)$ for the largest of odd order.

Theorem C. *Suppose that G is a finite non-solvable group with exactly two rational-valued irreducible characters. If $M := \mathbf{O}^{2'}(G)$ and $N := \mathbf{O}_{2'}(M)$, then $M/N = PSL_2(3^{2a+1})$ for some $a \geq 1$.*

The structure of solvable groups with exactly two rational-valued characters is completely described in §4 below.

2. Extending characters

Throughout the paper, a character of a finite group G is called **real**, resp. **rational**, if it is real-valued, resp. rational-valued. Furthermore, $\mathbb{Q}_n$ denotes the n-th cyclotomic field. If $K > 0$ is an integer and p is a prime, then K_p, resp. $K_{p'}$, denotes the p-part, resp. the p'-part, of K.

If G has order dividing some integer $n > 0$, then $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})$ acts naturally on $\mathrm{Irr}(G)$ since the representations of G over $\mathbb{C}$ can be realized in $\mathbb{Q}_n$. If $\chi \in \mathrm{Irr}(G)$, then $\mathbb{Q}(\chi)$ is the field generated by the values of χ. In fact, if $\sigma \in \mathrm{Gal}(\mathbb{Q}(\chi)/\mathbb{Q})$, then $\chi^\sigma \in \mathrm{Irr}(G)$.

The purpose of this section is to produce rational characters of G from rational characters of its normal subgroups in some special situations. We will often use Burnside's theorem stating that odd order groups have no non-trivial real irreducible characters.

If $\chi \in \mathrm{Irr}(G)$, we denote by $\mathrm{o}(\chi)$ the order of the linear character $\det(\chi)$. Recall that if $\chi \in \mathrm{Irr}(G)$ is real, then $\mathrm{o}(\chi)$ divides 2. (This follows from the following argument: If $\mathcal{X}$ is a representation affording χ and $\mathcal{Y}(g) = \mathcal{X}(g^{-1})^{\mathrm{t}}$ for $g \in G$, then $\mathcal{X}$ and $\mathcal{Y}$ are equivalent.)

The following lemma was pointed out to us by M. Isaacs.

2.1. Lemma. *Suppose that $N \lhd G$ has odd index. If $\theta \in Irr(N)$ is G-invariant and real, then θ has a unique real extension η to G. Also, $o(\eta) = o(\theta)$.*

Proof. Suppose first that θ extends to G, and let $\chi \in \mathrm{Irr}(G)$ be any character extending θ. Then the map $\lambda \mapsto \lambda\chi$ is a bijection between the linear characters of G/N and the set of extensions of θ to G (by Gallagher's Corollary (6.17) of [14]). Hence, the number of extensions of θ to G is odd, and since complex conjugation acts on them, it follows that there is some real extension $\eta \in \mathrm{Irr}(G)$ of θ. If ψ is another one, then $\psi = \lambda\eta$ for some linear $\lambda \in \mathrm{Irr}(G/N)$. Then $\bar{\lambda}\eta = \psi = \lambda\eta$, and we conclude that λ is real. Hence $\lambda^2 = 1$ and since G/N is of odd order, we have that $\lambda = 1$.

Therefore, it suffices to show that θ extends to G. We prove it by induction on $|G : N|$. By Corollary (11.31) of [14], we may assume that G/N is a p-group. Let $N \subseteq M \lhd G$ be such that $|G : M| = p$. Then θ has a unique real extension $\delta \in \mathrm{Irr}(M)$ by induction. By uniqueness, δ is G-invariant. Since G/M is cyclic, then δ extends to G.

Let $\nu = \det(\theta)$ and let $\mu = \det(\eta)$, where η is the unique real extension of θ to G. Since $\mu_N = \nu$, then $\mathrm{o}(\nu)$ divides $\mathrm{o}(\mu)$. Since θ and η are real, we have that $\mathrm{o}(\nu)$ and $\mathrm{o}(\mu)$ divide 2. If ν has order 2, necessarily μ has order 2. If $\nu = 1$, then $\mu \in \mathrm{Irr}(G/N)$ has order at most 2 in a group of odd order G/N, so μ is trivial. □

The following was already noticed in [21]. If $N \lhd G$ and $\theta \in \mathrm{Irr}(N)$, then $\mathrm{Irr}(G|\theta)$ is the set of $\chi \in \mathrm{Irr}(G)$ that lie above θ.

2.2. Corollary. *Let $N \lhd G$ with G/N of odd order. If $\theta \in Irr(N)$ is real, then there is a unique real character χ in $Irr(G|\theta)$. In particular, if θ is rational, then χ is rational.*

Proof. Let T be the stabilizer of θ in G. By Lemma 2.1, θ has a unique real extension $\hat{\theta} \in \mathrm{Irr}(T)$. Then $\chi = (\hat{\theta})^G$ is real. Every other member of $\mathrm{Irr}(G|\theta)$ is uniquely written in the form $(\hat{\theta}\beta)^G$, where $\beta \in \mathrm{Irr}(T/N)$, by the Clifford correspondence and Gallagher's theorem. By the uniqueness, we see that β is real if and only if $(\hat{\theta}\beta)^G$ is real. Since β is real only if β is principal (because T/N has odd order), it follows that χ is the only real character over θ. If θ is rational, again by uniqueness, it follows that χ is fixed by every $\tau \in \mathrm{Gal}(\mathbb{Q}_n)$, where $n = |G|$. It follows that χ is rational. □

If $N \lhd G$, $\theta \in \mathrm{Irr}(N)$ is G-invariant and $(|G : N|, \theta(1)\mathrm{o}(\theta)) = 1$, then it is well-known that there exists a unique $\chi \in \mathrm{Irr}(G)$ extending θ such that $\mathrm{o}(\chi) = \mathrm{o}(\theta)$ (Corollary (6.28) of [14]). Sometimes we call χ the **canonical extension** of θ to G. Notice, too, that $\mathbb{Q}(\chi) = \mathbb{Q}(\theta)$. (This can be proved as follows. We have that $\mathbb{Q}(\theta) \subseteq \mathbb{Q}(\chi)$. If $\sigma \in \mathrm{Gal}(\mathbb{Q}(\chi)/\mathbb{Q}(\theta))$, then χ^σ is another extension with $\mathrm{o}(\chi^\sigma) = \mathrm{o}(\theta)$. Hence, $\chi^\sigma = \chi$ and σ is the identity.)

2.3. Theorem. *Let N be a normal subgroup of G, and let $\theta \in Irr(N)$ be G-invariant, real of odd degree. Suppose that $o(\theta) = 1$. Then θ has a unique real extension $\eta \in Irr(G)$ such that $o(\eta) = 1$.*

Proof. First we prove that θ extends to G. So it suffices to show that θ extends to P/N, where P/N is a Sylow p-subgroup of G/N (by Corollary (11.31) of [14]). If $p = 2$, this follows from Corollary (6.28) of [14]. If p is odd, this follows from

Lemma 2.1. So now let $\chi \in \mathrm{Irr}(G)$ be any extension of θ to G. We have that the set of extensions of θ to G is $\{\lambda\chi \,|\, \lambda \in \mathrm{Irr}(G/M)\}$, where $M = G'N$.

We prove the theorem by induction on $|G : N|$. Suppose first that $M = G$. Hence χ is the unique extension of θ to G. So it suffices to show that χ is real and that $\mathrm{o}(\chi) = 1$. By uniqueness, we have that χ is real (because θ is real). Also, $\det(\chi)_N = \det(\theta) = 1$, so $\det(\chi)$ is a linear character of G/N. Since $M = G$, we conclude that $\det(\chi) = 1$.

So we may assume that $M < G$. By induction, we have that there exists a unique real extension ν of θ to M such that $\mathrm{o}(\nu) = 1$. Suppose that $N < M$. Then by induction, we will have that there exists a unique real extension $\tau \in \mathrm{Irr}(G)$ of ν with $\mathrm{o}(\tau) = 1$. So τ is a real extension of θ to G with $\mathrm{o}(\tau) = 1$. Suppose that $\chi \in \mathrm{Irr}(G)$ is real and also extends θ with $\det(\chi) = 1$. Then χ_M is a real extension of θ to M with trivial determinantal character. By the inductive hypothesis, $\chi_M = \nu$, and therefore $\chi = \tau$, again by induction.

Hence, we may assume that $M = N$. Thus G/N is abelian. Let P/N be a Sylow 2-subgroup of G/N and let H/N be a 2-complement. By Lemma 2.1, there exists a unique real $\xi \in \mathrm{Irr}(H)$ extending θ. Furthermore, $\mathrm{o}(\xi) = 1$. Also, let $\hat{\theta} \in \mathrm{Irr}(P)$ be the canonical extension of θ to P, so that $\mathrm{o}(\hat{\theta}) = 1$. We have that $\hat{\theta}$ is real and G-invariant by uniqueness. By Corollary (4.2) of [13], we have that restriction defines a bijection

$$\mathrm{Irr}(G \,|\, \hat{\theta}) \to \mathrm{Irr}(H \,|\, \theta)\,.$$

Hence, there exists a unique

$$\rho \in \mathrm{Irr}(G|\hat{\theta})$$

such that $\rho_H = \xi$. In particular, ρ extends θ. Now, ρ is real because the restriction map is one to one. Since $\det(\rho)_P = \det(\hat{\theta}) = 1$ and $\det(\rho)_H = \det(\xi) = 1$, we conclude that $\det(\rho) = 1$. Finally, suppose that $\mu \in \mathrm{Irr}(G)$ is real, extends θ and is such that $\mathrm{o}(\mu) = 1$. Then μ_P is an extension of θ with determinantal order 1, and so $\mu_P = \hat{\theta}$. Also, μ_H is a real extension of θ to H, so $\mu_H = \xi$, and $\mu = \rho$, by the uniqueness of the restriction map. □

2.4. Corollary. *Let N be a normal subgroup of G, and let $\theta \in Irr(N)$ be rational of odd degree. Suppose that $o(\theta) = 1$. Then there exists a rational $\chi \in Irr(G \,|\, \theta)$.*

Proof. Let T be the stabilizer of θ in G. By Theorem 2.3, there exists a unique real extension ψ of θ to T with trivial determinantal order. By uniqueness ψ is rational, and then $\chi = \psi^G \in \mathrm{Irr}(G)$ is rational. □

3. 2-length and rational characters

The solvable case of Theorem B is quite easy.

3.1. Lemma. *Suppose that G is a solvable group of even order. Then G has a non-trivial rational irreducible character of odd degree.*

Proof. Let $K = \mathbf{O}^{2'}(G)$. Since G is of even order, $K > 1$, and since $\mathbf{O}^{2'}(K) = K$, $L = \mathbf{O}^2(K) < K$. Then K/L has a non-trivial linear character of order 2. This character has a canonical extension $\hat{\lambda}$ to its stabilizer, which is also rational by uniqueness. Then $\chi = (\hat{\lambda})^G$ is rational and non-trivial. □

A celebrated theorem of J. G. Thompson, which we will be using later on, asserts that if G is a solvable group with one conjugacy class of involutions and such that its Sylow 2-subgroup S has more than one involution, then G has 2-length one. (See Theorem IX.8.6 in [12].) In fact, the first step in the proof of the solvable case of Theorem A is to show that the 2-length of the group in question is also one. There is something slightly more general.

3.2. Theorem. *Let G be a solvable group of even order. Then the 2-length of G is less than the number of irreducible rational characters of G of odd degree.*

Proof. For $i \geq 1$, let $G_i = \mathbf{O}^{2'2}(G_{i-1})$, where $G_0 = G$. Let $M_i = \mathbf{O}^{2'}(G_{i-1})$. Then $G_i = \mathbf{O}^2(M_i)$, $G_i = \mathbf{O}^2(G_i)$ and $M_i = \mathbf{O}^{2'}(M_i)$. By Lemma 3.1, there exists $\chi_1 \in \mathrm{Irr}(G/G_1)$ non-trivial, rational of odd degree. Suppose that $M_t > 1$ and $M_{t+1} = 1$ for some $t \geq 2$.

Let $k \leq t$, so that $M_k/G_k > 1$. Let P_k/M_k be a Sylow 2-subgroup of G/M_k, so that P_k/G_k is a Sylow 2-subgroup of G/G_k. Thus $[M_k, P_k] < M_k$. Thus there is a non-trivial P_k-invariant linear character $\lambda_k \in \mathrm{Irr}(M_k/G_k)$ of order 2. Now, by considering its canonical extension in G_{k-1} and the Clifford correspondence, there exists $\theta_k \in \mathrm{Irr}(G_{k-1}/G_k)$ over λ_k, with odd degree, rational and P_k-invariant. Since θ_k is real, it follows that $\mathrm{o}(\theta_k)$ divides 2. Since $\mathbf{O}^2(G_{k-1}) = G_k$, it follows that $\mathrm{o}(\theta_k) = 1$. By Theorem 2.3, there exists a unique real extension ψ_k of θ_k to its stabilizer T_k in G with $\mathrm{o}(\psi_k) = 1$. By uniqueness, ψ_k is rational. Since $P_k \subseteq T_k$, it follows that $\chi_k = (\psi_k)^G \in \mathrm{Irr}(G/G_k)$ is rational of odd degree which does not have G_{k-1} in its kernel. □

4. Odd-order groups acting on 2-groups

We start with some elementary lemmas. As usual, in a p-group G, $\Omega_1(G)$ is the set of elements $x \in G$ with $x^p = 1$.

4.1. Lemma. *Suppose that a finite group X acts on a homocyclic p-group G. Then the actions of X on $G/\Phi(G)$ and $\Omega_1(G)$ are permutation isomorphic.*

Proof. Suppose that p^n is the exponent of G. Then

$$\Phi(G) = \{x \in G \,|\, x^{p^{n-1}} = 1\}.$$

If $x, y \in G$, notice that $x\Phi(G) = y\Phi(G)$ if and only if $x^{p^{n-1}} = y^{p^{n-1}}$. Hence, the map $G/\Phi(G) \to \Omega_1(G)$ given by $x\Phi(G) \mapsto x^{p^{n-1}}$ is a natural bijection. □

If X acts coprimely on an abelian group G, by Fitting's Lemma we have that $G = [G, X] \times \mathbf{C}_G(X)$. In particular, the number of X-invariant irreducible characters of G is $|\mathbf{C}_G(X)|$. Thus, as is well-known, the actions of X on $\mathrm{Irr}(G)$ and on G are permutation isomorphic (see Lemma (13.23) of [12]).

4.2. Lemma. *Suppose that X acts coprimely on an abelian p-group G. If X acts transitively on $Irr(G/\Phi(G)) \setminus \{1_G\}$, then X acts transitively on $\Omega_1(G) \setminus \{1_G\}$.*

Proof. The actions of X on $G/\Phi(G)$ and on $\mathrm{Irr}(G/\Phi(G))$ are permutation isomorphic. So we have that X transitively permutes the non-identity elements of $G/\Phi(G)$. The action of X on $G/\Phi(G)$ is therefore irreducible, and hence G is homocyclic (by elementary group theory). Then we may apply Lemma 4.1. □

4.3. Lemma. *Let X be an odd-order group acting on a 2-group P. If X acts transitively on the real non-principal irreducible characters of P, then X is transitive on the involutions of P.*

Proof. Let $G = PX$ be the semidirect product. By Corollary 2.2, we know that G has exactly one real irreducible character lying over the unique X-orbit of non-principal real irreducible characters of P. But every real character $\chi \in \mathrm{Irr}(G)$ lies over some real irreducible character of P because χ_P has an odd number of distinct irreducible constituents, which must be permuted by complex conjugation.

Thus G has a total of two real irreducible characters and thus has exactly two real classes. It follows that all involutions of P are G-conjugate. But P has a central involution z, and thus the X-orbit of z is the G-orbit of Z, which consists of all involutions of P. □

Recall that a non-abelian 2-group with more than one involution and acted on by a solvable group X such that X is transitive on the involutions of P is a **Suzuki 2-group**. A fact that we will need is the following. If P is a Suzuki 2-group, then $\Phi(P) = P' = \mathbf{Z}(P) = \Omega_1(P)$. (See Theorem VIII.7.9 of [12].) Note that a Suzuki 2-group has exponent 4, and so all real characters are actually rational.

M. Isaacs simplified our proof of the next theorem below.

4.4. Theorem. *Let P be a 2-group and suppose X has odd order and acts on P, acting transitively on the non-principal rational irreducible characters. Then X acts transitively on the involutions in P, and either P is homocyclic abelian or P is a Suzuki 2-group. In particular, all real characters of P are rational.*

Proof. Note that X acts transitively on the non-principal linear characters of $P/\Phi(P)$ and these are the only non-principal rational irreducible characters of P. By Lemma 4.2, we may assume that P is not abelian.

Now P has more than one involution or else it must be Q_8 since larger generalized quaternion groups do not admit an odd group X acting non-trivially on $P/\Phi(P)$. But Q_8 has a rational character not in $\mathrm{Irr}(P/\Phi(P))$, and this is a contradiction. Thus P has more than one involution.

Assume that X is not transitive on involutions, and thus by Lemma 4.3, it is not transitive on non-principal real irreducible characters of P. Thus there exists a real character $\theta \in \mathrm{Irr}(P)$ with $\Phi(P) \not\leq \ker(\theta)$, and in particular, θ is not rational. Then θ is non-linear and therefore $P' \not\leq \ker(\theta)$. We now want to derive a contradiction.

If P' is minimal normal in PX, then it is central in P and elementary abelian. Let $\lambda \in \mathrm{Irr}(P')$ lie under θ and note that since λ is P-invariant and P/P' is abelian, there exists a subgroup R with $P' \leq R \leq P$ and a character $\mu \in \mathrm{Irr}(R)$ extending λ and fully ramified with respect to θ (by Lemma 2.2 of [25], for instance). As θ is real, so is μ. But μ is linear, and so is rational, and it follows that θ is rational, which is not the case.

Then P' is not minimal normal in PX and we choose $Z \leq P'$ so that Z is minimal normal in PX. In particular Z is elementary. Then X acts on P/Z and the original hypotheses are satisfied here. Working by induction on $|P|$, we deduce that X is transitive on the involutions of P/Z and P/Z is a Suzuki 2-group. (It is not abelian since $Z < P'$.) In particular, we have that $P'/Z = \mathbf{Z}(P/Z) = \Omega_1(P/Z)$ is elementary, X acts transitively on the involutions of P/Z (which are the involutions of P'/Z) and P/P' is elementary.

Now, $[P, P'] \leq Z$ and therefore $[P, P', P] = 1$. By the three subgroups lemma, we have that P' is abelian. If P' is elementary, then P has exponent 4 and so all real characters are rational, which is not the case. Thus P' is abelian, but not elementary abelian. But P'/Z is elementary, and thus $1 < \Phi(P') \leq Z$ and we deduce that $\Phi(P') = Z$. Also, since X acts irreducibly on P'/Z and $Z \leq \Omega_1(P') < P'$, we deduce that $Z = \Omega_1(P')$.

Each involution of P maps to an involution (or the identity) of P/Z, and so by the structure of Suzuki 2-groups, it lies in P', and hence in Z, and we conclude that $Z = \Omega_1(P)$. Now X acts transitively on the non-identity elements of $P'/\Phi(P')$ and P' is abelian, so by Lemma 4.2, we have that X is transitive on the non-identity elements of $\Omega_1(P') = Z = \Omega_1(P)$. Hence, X is transitive on the involutions of P, and this is a contradiction.

Finally, suppose that $\tau \in \mathrm{Irr}(P)$ is real. If P is abelian, then $\tau^2 = 1$ and τ is rational. If P is not abelian, then P is a Suzuki 2-group, and then τ is rational. □

4.5. Lemma. *Suppose that G has a normal Sylow 2-subgroup P, and let X be a 2-complement of G. Then $|Irr_{rat}(G)| = 2$ if and only if X acts transitively on the non-trivial rational irreducible characters of P.*

Proof. Let $1 \neq \delta \in \mathrm{Irr}(P)$ be rational. If $\hat{\delta}$ is the canonical extension of δ to its stabilizer, then $\psi = (\hat{\delta})^G$ is a rational non-trivial irreducible character of G lying over δ, and it is the only one by Corollary 2.2. Hence, if G has exactly two rational irreducible characters, then X acts transitively on the non-trivial rational irreducible characters of P.

Now, suppose that $\chi \in \mathrm{Irr}(G)$ is rational. Let $\theta \in \mathrm{Irr}(P)$ be an irreducible constituent of χ_P. If τ is a Galois automorphism of the cyclotomic field $\mathbb{Q}_{|P|}$, then θ^τ lies under χ, and therefore $\theta^\tau = \theta^x$ for some $x \in X$. Since τ has 2-power order and x is of odd order, it follows that $\theta^\tau = \theta$. Thus θ is rational.

Suppose now that X acts transitively on the non-trivial rational irreducible characters of P. If $\chi \in \mathrm{Irr}(G)$ is rational, non-trivial, then the irreducible constituents of χ_P are rational. Suppose that $\theta \in \mathrm{Irr}(P)$ is one of those. Since P is not in the kernel of χ, we have that the X-orbit of θ is the unique orbit of rational characters of P. By Corollary 2.2, χ is the unique rational character over θ. □

4.6. Corollary. *Suppose that $|Irr_{rat}(G)| = 2$ and assume that G has a normal Sylow 2-subgroup. Then G has exactly two real irreducible characters.*

Proof. Let X be a 2-complement of G, and let P be the Sylow 2-subgroup of G. By Lemma 4.5, X acts transitively on the non-trivial rational irreducible characters of P, and by Theorem 4.4, we have that every real irreducible character of P is rational. Now, let $\tau \in \mathrm{Irr}(G)$ be real, and let $\theta \in \mathrm{Irr}(P)$ be an irreducible constituent. Then $(\bar{\theta})^x = \theta$ for some $x \in X$. Then $\theta^{x^2} = \theta$ and since $x \in \langle x^2 \rangle$, it follows that $\theta^x = \theta$. Therefore, θ is real, and therefore it is rational by Theorem 4.4. Thus θ lies under the unique rational non-trivial character ψ of G. Now, $\tau = \psi$ by Corollary 2.2. □

Although groups with a normal Sylow 2-subgroup and exactly two rational irreducible characters necessarily have two real irreducible characters (as shown in Corollary 4.6); this fact is not true for solvable groups in general. Iwasaki studied in [15] groups with exactly two real characters. It is easy to check that these groups have a normal Sylow 2-subgroup, and the main work in [15] is to classify their Sylow 2-subgroups. So we can conclude that solvable groups with exactly two rational

characters have 2-length 1 (by Theorem 3.2), and that their Sylow 2-subgroups are of the type described in [15].

5. Rational classes

Now, we take some time to prove a few elementary properties of rational classes. Recall that an element $x \in G$ is **rational** (in G) if whenever $\langle y \rangle = \langle x \rangle$, then y is G-conjugate to x. In this case, we say that the class $K = \mathrm{cl}_G(x)$ is rational.

5.1. Lemma. *Let G be a finite group.*

(a) *Assume that $x \in G$ is rational. Then xN is rational in G/N for every $N \lhd G$.*

(b) *If $g \in H \leq G$ is rational in H, then g is rational in G.*

(c) *Suppose that $x \in G$ has order p, a prime. Then x is rational in G if and only if there is a p'-element $g \in G$ such that $x^g = x^t$, where $t (\mathrm{mod}\, p)$ is any generator of $\mathbb{Z}_p^\times$.*

(d) *Assume $x \in G$ is rational. Then every power of x is also rational. In particular, x_π is rational for every set of primes π.*

(e) *If $N \lhd G$, $(o(x), |N|) = 1$ and xN is rational, then x is rational.*

Proof. Parts (a) and (b) are obvious. We start with part (c). If x is rational in G and $t (\mathrm{mod}\, p)$ is any generator of $\mathbb{Z}_p^\times$, then there is some $g \in G$ such that $x^g = x^t$. Now, $g \in \mathbf{N}_G(\langle x \rangle) = U$ and since $U/\mathbf{C}_G(x)$ is not divisible by p, it is clear that we may replace g by $g_{p'}$. For the converse, if $\langle y \rangle = \langle x \rangle$, then $y = x^k$ for some $1 \leq k \leq p-1$. Now $x^g = x^t$ for some $g \in G$. Thus

$$x^{g^m} = x^{t^m}$$

for every natural m. Since $\mathbb{Z}_p^\times$ is generated by $t (\mathrm{mod}\, p)$, it follows that y is G-conjugate to x.

(d) Assume that y is a power of x, with order n/a, where $n = \mathrm{o}(x)$, and that $\langle z \rangle = \langle y \rangle$. Since $\langle x^a \rangle$ is the unique subgroup of order n/a in $\langle x \rangle$, we can write $y = x^{ak}$, $z = x^{al}$ for some integers k, l that are coprime to n/a. Claim that we can find $k_1 \in k + (n/a)\mathbb{Z}$ coprime to n. We proceed by induction on a. Suppose $p|k$ for some prime $p|n$; in particular $(p, n/a) = 1$. By the pigeonhole principle, one can find $k' \in k + (n/a)\mathbb{Z}$ such that $(k', p) = 1$. Now k' is coprime to $np/a = n/(a/p)$. By the induction hypothesis we can find $k_1 \in k' + (np/a)\mathbb{Z}$ that is coprime to n. Thus, we may assume that k and l are coprime to n. By assumption, x^k and x^l are conjugate, and so are x^{ak} and x^{al}.

(e) First, we claim that if $xN = zN$, where $\mathrm{o}(z)$ is coprime with $|N|$, then x and z are N-conjugate. By the Schur-Zassenhaus Theorem, we have that $\langle x \rangle = \langle z \rangle^n$ for some $n \in N$. Hence, $x = (z^k)^n$ for some integer k. Thus $zN = xN = (z^k)^n N = z^k N$ and we deduce that $z = z^k$, proving the claim.

Suppose finally that $\langle y \rangle = \langle x \rangle$. Then $\langle yN \rangle = \langle xN \rangle$ and there exists $g \in G$ such that $x^g N = yN$. It follows that $x^{gn} = y$ for some $n \in N$ by the previous claim. □

5.2. Lemma. *Assume that p is a prime and that N is a normal subgroup of G such that G/N contains a rational element of order p. Then G contains a rational element of order p.*

Proof. If $p = 2$, then the lemma is clear. So we may assume that p is odd. We proceed by induction on $|N||G|$. If $Q \in \mathrm{Syl}_q(N)$, then $\mathbf{N}_G(Q)/\mathbf{N}_N(Q) \cong G/N$ contains a rational element of order p. Hence, by induction, we may assume that N is nilpotent.

Suppose now that $x \in G$ is such that xN is a rational element of order p in G/N. Clearly, we can choose x to be a p-element.

Now, if $1 < M < N$ is a normal subgroup of G, then G/M has a rational element of order p by induction. Again by induction, we will have that G has a rational element of order p. So we may assume that N is an elementary abelian q-group for some prime q. If $q \neq p$, then x has order p and is rational by Lemma 5.1(d). Hence, we may assume that N is a minimal normal subgroup of G, and therefore an elementary abelian p-group.

Let t be an integer such that $t(\mathrm{mod}\, p)$ generates $\mathbb{F}_p^\times$. By assumption, there is $g \in G$ such that

$$gxg^{-1} = x^t n$$

for some $n \in N$. Without loss we may assume that $G = \langle N, x, g\rangle$. Let $C := \mathbf{C}_N(x)$. Notice that $C \neq 1$ and $C \lhd G$, so $C = N$ by the minimality of N. Thus $[x, N] = 1$, and x has order p or p^2. Now if $\mathrm{o}(x) = p^2$, then $gx^p g^{-1} = (x^t n)^p = (x^p)^t$, whence x^p is rational of order p. So we may assume that x has order p. Also, if $gmg^{-1} = m^t$ for some $1 \neq m \in N$, then m is rational of order p (by Lemma (5.1.c)). Thus we may assume that the map $y \mapsto y^{g^{-1}} y^{-t}$ is a bijection $N \to N$. In particular, we can find $y \in N$ such that

$$gyg^{-1}y^{-t} = n^{-1}\,.$$

It follows that $g(xy)g^{-1} = x^t n n^{-1} y^t = (xy)^t$, and xy is a rational element of order p. □

6. Galois and group actions on solvable groups

Before we proceed to start proving the main results in this paper, we need a few results on how Galois and group actions on solvable groups are related.

If G has order dividing n, then, as we already said, $\mathcal{G} = \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})$ acts naturally on $\mathrm{Irr}(G)$ and $\mathrm{cl}(G)$. Indeed, if ξ is a primitive n-th root of unity and $\sigma \in \mathcal{G}$, then there is a unique $1 \leq k \leq n$ coprime with n such that $\sigma(\xi) = \xi^k$. If $K = \mathrm{cl}_G(x) \in \mathrm{cl}(G)$, then $K^\sigma = \mathrm{cl}_G(x^k)$. Also, $\chi^\sigma(g) = \chi(g)^{\sigma^{-1}}$. We define the action this way so that $\chi^\sigma(g^\sigma) = \chi(g)$, where g^σ is in the class of g^k. Of course, $\chi \in \mathrm{Irr}(G)$ is rational-valued if and only if χ is $\mathcal{G}$-fixed, and $x \in G$ is rational if and only if $K = \mathrm{cl}_G(x)$ is $\mathcal{G}$-fixed.

6.1. Lemma. *With the previous notation, suppose that A acts as an automorphism group on G and let $\sigma \in \mathcal{G}$ and $a \in A$. Then there exists $1 \neq \chi \in Irr(G)$ such that $\chi^\sigma = \chi^a$ iff there exists $1 \neq K \in cl(G)$ such that $K^\sigma = K^a$.*

Proof. Let $B = A \times \mathcal{G}$. We claim that B acts on $\mathrm{Irr}(G)$ and $\mathrm{cl}(G)$ such that

$$\chi^b(g^b) = \chi(g)\,,$$

where $b \in B$ and g^b is in the class $\mathrm{cl}_G(g)^b$. Suppose that $b = (u, \sigma) \in B$. We define $\chi^b = (\chi^u)^\sigma = (\chi^\sigma)^u$ and $K^b = (K^u)^\sigma = (K^\sigma)^u$.

Now, let $z = (a, \sigma^{-1}) \in B$. By Brauer's lemma on character tables (Theorem (6.32) of [14]), we have that z fixes the same number of classes as characters. □

In the next lemma, we find it very useful to use the Isaacs B_p-characters [13]. If G is a finite p-solvable group, then $B_p(G) \subseteq \mathrm{Irr}(G)$ is a canonical subset of the irreducible characters of G with values in $\mathbb{Q}_{|G|_p}$. If G is a p-group, then $B_p(G) = \mathrm{Irr}(G)$, and if G is a p'-group, then $B_p(G)$ consists of only the trivial character. The

reader needs to know the following. If $N \lhd G$ and $\theta \in B_p(N)$, then all irreducible constituents of θ^G lie in $B_p(G)$ if G/N is a p-group; and exactly one of them lie in $B_p(G)$ if G/N is a p'-group.

The following rather technical lemma is essential for our purposes.

6.2. Lemma. *Let p be an odd prime and L be a finite group of order dividing n. Suppose that $\sigma \in Gal(\mathbb{Q}_n/\mathbb{Q})$ fixes p'-roots of unity and has order $p-1$ and write $\xi^\sigma = \xi^k$, where ξ is any p-th root of unity. Suppose that a acts as an automorphism on L and let $Z \lhd L$ be a-invariant where L/Z is p-solvable. Assume that the order of a on its action on L/Z is not divisible by p. Suppose that $1 \neq \lambda \in Irr(Z)$ lies in $B_p(Z)$ is such that $\lambda^a = \lambda^\sigma$.*

(a) *Then there exists $1 \neq \psi \in B_p(L)$ over λ such that $\psi^a = \psi^\sigma$.*

(b) *If L/M has no elements x of order p such that $x^a = x^k$ for every a-invariant $Z \subseteq M \lhd L$, and $\mathbb{Q}(\lambda) \subseteq \mathbb{Q}_p$, then ψ can also be taken such that $\mathbb{Q}(\psi) \subseteq \mathbb{Q}_p$.*

Proof. Write $|L|_p = p^e$ and $\mathrm{Gal}(\mathbb{Q}_{p^e}/\mathbb{Q}_p) = \langle\tau\rangle$. By hypothesis, notice that $k \pmod p$ is a generator of $\mathbb{Z}_p^\times$.

Among all a-invariant normal subgroups K of L containing Z having some $\theta \in B_p(K)$ over λ with $\theta^\sigma = \theta^a$, we choose K of the largest possible order. (In part (b); then we choose K adding the condition that $\mathbb{Q}(\theta) \subseteq \mathbb{Q}_p$.) Of course, we wish to prove that $K = L$.

If $K < L$, then let $1 < E/K$ be a minimal a-invariant normal subgroup of L/K.

Suppose first that E/K is a p'-group. Then there exists a unique ψ in $\mathrm{B}_p(E)$ lying over θ. Now, $\psi^{\sigma a^{-1}}$ is in B_p and also lies over θ, and therefore $\psi^\sigma = \psi^a$. Suppose that we are in case (b). We know that $\mathbb{Q}(\psi) \subseteq \mathbb{Q}_{p^e}$. Since $\theta^\tau = \theta$, then by uniqueness $\psi^\tau = \psi$, and therefore $\mathbb{Q}(\psi) \subseteq \mathbb{Q}_p$.

So we have that E/K is an elementary abelian p-group. Notice that $u \mapsto (u^k)^{a^{-1}} = u^\rho$ is an isomorphism $E/K \to E/K$ of p'-order s. If we are in case (b), then we will have that $\mathbf{C}_{E/K}(\rho) = 1$.

Now, let T be the stabilizer of θ in E. Since $\theta^\sigma = \theta^a$, notice that the stabilizer of θ in E is a-invariant. Since T/K is abelian, there exists a unique $K \subseteq U \subseteq T$ such that θ extends to U and every extension is fully ramified in T/U (by Lemma 2.2 of [25]). Since $\lambda^a = \lambda^\sigma$, we conclude that U is also a-invariant. Also, in case (b), we have that $\mathbf{C}_{U/K}(\rho) = 1$.

Now, let $\delta \in \mathrm{Irr}(U)$ be any extension of θ to K. With certain abuse of notation, write $\rho = \sigma a^{-1}$, and notice that $\lambda^\rho = \lambda$. Hence $\delta^\rho = \epsilon\delta$ for a unique $\epsilon \in \mathrm{Irr}(U/K)$ by Gallagher's theorem. Now, by coprime action, we have that

$$U/K = \mathbf{C}_{U/K}(\rho) \times [U/K, \rho] \, .$$

Hence, we may write

$$\epsilon = \mu(\nu^{-1})^\rho \nu \, ,$$

where μ is fixed by ρ. Hence, by replacing δ by $\nu\delta$, we may find an extension, call it δ again, such that $\delta^\rho = \mu\delta$, where μ is fixed by ρ. Now

$$\delta^{\rho^m} = \mu^m \delta$$

for every number m. If s is the order of the action of ρ on E/K, then $\mu^s = 1$, and therefore $\mu = 1$ and δ is ρ-invariant. If we are in case (b), then notice that δ is the unique ρ-invariant extension of θ. Also, δ lies in $B_p(U)$ and since $\theta^\tau = \theta$, we conclude that $\delta^\tau = \delta$. Hence, $\mathbb{Q}(\delta) \subseteq \mathbb{Q}_p$. Now, $\delta^T = f\phi$, for some $\phi \in \mathrm{Irr}(T)$

with $\mathbb{Q}(\delta) = \mathbb{Q}(\phi)$, and $\psi = \phi^E \in \mathrm{Irr}(E)$. Since E/K is a p-group, we have that $\psi \in B_p(E)$, $\psi^\rho = \psi^a$, and in case (b), we also have that $\mathbb{Q}(\psi) \subseteq \mathbb{Q}_p$. □

We shall need the following two results later on.

6.3. Corollary. *Suppose that $L \lhd G$ and let p be an odd prime number. Suppose that $\langle\sigma\rangle$ is the unique subgroup of $Gal(\mathbb{Q}_{|G|}/\mathbb{Q})$ which fixes p'-roots of unity and has order $p-1$. Assume that there exists $\theta \in Irr(L)$ such that $\theta^g = \theta^\sigma$ for some $g \in G$ with $\mathbb{Q}(\theta) \subseteq \mathbb{Q}_p$. Assume that T is p-solvable, where T is the stabilizer of θ in G, and that $\theta \in B_p(L)$. If G/L has no rational elements of order p, then there exists $\chi \in Irr(G|\theta)$ rational valued.*

Proof. Since $o(\sigma)$ is not divisible by p, then we notice that g_p fixes θ, so we may assume that the order of g is not divisible by p. Now $T^g = T$ and g acts on T. If $L \leq M \lhd T$ is g-invariant and $T\langle g\rangle/M$ has a rational element of order p, then we will have that $T\langle g\rangle/L$ has a rational element of order p (by Lemma 5.2), and this is against our hypothesis. Hence, by Lemma 6.2(b), there exists $\psi \in \mathrm{Irr}(T|\theta)$ such that $\mathbb{Q}(\psi) \subseteq \mathbb{Q}_p$, and $\psi^\sigma = \psi^g$. Now, we claim that $\chi = \psi^G \in \mathrm{Irr}(G)$ is rational-valued. First notice that $\mathbb{Q}(\chi) \subseteq \mathbb{Q}(\psi) \subseteq \mathbb{Q}_p$, so we only need to check that $\chi^\sigma = \chi$. However,

$$\chi^\sigma = (\psi^\sigma)^G = (\psi^g)^G = \psi^G = \chi\,,$$

as claimed. □

6.4. Corollary. *Let p be an odd prime. Suppose that a acts as an automorphism on a p-solvable group L, has order not divisible by p and is such that there exists an element $x \in L$ of order p such that $x^a = x^k$, where $k \pmod p$ is a generator of $\mathbb{Z}_p^\times$. Then there exists $1 \neq \psi \in Irr(L)$ such that $\mathbb{Q}(\psi) \subseteq \mathbb{Q}_p$, $\psi \in B_p(L)$ and $\psi^a = \psi^\sigma$, where $\langle\sigma\rangle$ is the unique subgroup of $Gal(\mathbb{Q}_{|G|}/\mathbb{Q})$ which fixes p'-roots of unity and has order $p-1$.*

Proof. We argue by induction on $|L|$. Let $1 < K < L$ be a-invariant and normal in L. If $x \notin K$, then $xK \in L/K$ is a rational element of order p with $(xK)^a = (xK)^k$, and so we are done by induction. So we may assume that $x \in K$. Therefore x lies in some normal a-invariant elementary subgroup Z of L. By Lemma 6.1, there exists $\lambda \in \mathrm{Irr}(Z)$ such that $\lambda^a = \lambda^\sigma$. Since x has order p, Z is a p-group, and therefore $\lambda \in B_p(Z)$. Now, apply Lemma 6.2(b). □

7. Solvable groups

We will need the following simple statement:

7.1. Lemma. *If G has a normal Sylow 2-subgroup G, then every real element of G is a 2-element.*

Proof. Let $Q \lhd G$ be the Sylow 2-subgroup of G and suppose that $x^g = x^{-1}$. Then $x^{g^2} = x$, and hence, $g_{2'}$ centralizes x. So there is no loss to assume that g has 2-power order. Thus $g \in Q$. Now $x_{2'}^g = x_{2'}^{-1}$. Hence $[x_{2'}, g] \in \langle x_{2'}\rangle$, and thus g commutes with $x_{2'}$. Then $x_{2'} = x_{2'}^{-1}$, $x_{2'} = 1$, and we are done. □

7.2. Theorem. *Suppose that G is solvable. Then we have that $|cl_{rat}(G)| = 2$ if and only if $|Irr_{rat}(G)| = 2$.*

Proof. Let $P \in \mathrm{Syl}_2(G)$. Let $L = \mathbf{O}_{2'}(G)$.

Suppose first that $|\mathrm{cl}_{\mathrm{rat}}(G)| = 2$. Let $\mathrm{cl}_G(u)$ be the unique class of involutions of G. We prove that G has two rational characters by induction on $|G|$. Suppose first that $L > 1$ and let N be a minimal normal odd order subgroup of G. We claim that $|\mathrm{cl}_{\mathrm{rat}}(G/N)| = 2$. Suppose that $1 \neq xN$ is rational in G/N. Hence $x_{2'}N$ is also rational. If this element is non-trivial, then by using Lemma 5.1, we may assume that G/N has a rational element of order an odd prime p. In this case, by Lemma 5.2, G has a rational element of order p, and this is impossible. Thus xN is a 2-element. But in this case x is rational, again by Lemma 5.1. Hence, x is an involution, proving the claim. By induction, we will have that G/N has exactly two rational characters. Suppose that $\chi \in \mathrm{Irr}(G)$ is rational and does not contain N in its kernel. We know that N is an elementary abelian p-group, for some odd prime p. Now, let $\sigma \in \mathrm{Gal}(\mathbb{Q}_{|G|}/\mathbb{Q})$ be any extension of a generator τ of $\mathrm{Gal}(\mathbb{Q}_p/\mathbb{Q})$. Since $\chi^\sigma = \chi$, there exists $1 \neq \lambda \in \mathrm{Irr}(N)$ and $g \in G$ such that $\lambda^g = \lambda^\sigma = \lambda^\tau$. Let ζ be a complex primitive p-th root of unity and let $\tau(\zeta) = \zeta^t$ for some $t \in (\mathbb{Z}/p\mathbb{Z})^\times$. Identifying $\mathrm{Irr}(N)$ with the dual space N^* we see that g acting on N^* has an eigenvalue t. It follows that g^{-1} acting on N has an eigenvalue t. In other words, there exists $1 \neq x \in N$ such that $g^{-1}xg = x^t$, whence x is rational. This contradiction proves that we may assume $L = 1$.

If P is cyclic, then G has a normal 2-complement. Hence G is a 2-group, and the theorem is true in this case. If P is generalized quaternion, then P has rational elements of order 4, and this is against our hypothesis. So we may assume that P has more than one involution.

By Thompson's theorem (IX.8.6 of [12]), we have that $P \lhd G$. Now, let X be a 2-complement of G. We have that X acts transitively on the involutions of P (start with an involution in the center of P). If P is abelian, then P is homocyclic, and the theorem follows from Lemmas 4.1 and 4.5 since the rational characters of P are those containing $\Phi(P)$ in its kernel.

So we may assume that P is a Suzuki 2-group. In this case the exponent of P is 4. Now, let $\mathrm{cl}_G(z)$ be a real class of G. By Lemma 7.1, we have that z is a 2-element. Then $z^4 = 1$ and therefore $\mathrm{cl}_G(z)$ is rational. Thus $z^2 = 1$, and we conclude that G has exactly two real characters. So G has exactly two rational characters.

Suppose now that G has exactly two rational irreducible characters. We prove by induction on $|G|$ that G has a unique class of involutions and that there are no more non-trivial rational elements. We know that G has 2-length one by Theorem 3.2. Let $L = \mathbf{O}_{2'}(G)$ and $K = PL$. Since G/L has even order, then all rational irreducible characters of G have L in its kernel by Lemma 3.1 and our hypothesis.

Assume that $L > 1$. By induction, we have that the class of involutions of G/L is the unique rational class of elements in G/L. Suppose that $1 \neq x \in L$ is rational. Then by Lemma 5.1, we may assume that x has order a prime p. If $t \pmod p$ generates $\mathbb{Z}_p^\times$, then there exists a p'-element $g \in G$ such that $x^g = x^t$. Let $\sigma \in \mathrm{Gal}(\mathbb{Q}_{|G|}/\mathbb{Q})$ be an element of order $p-1$ fixing p'-roots of unity such that $\xi^\sigma = \xi^t$, where $\mathrm{o}(\xi) = p$. By Corollary 6.4, there exists $1 \neq \psi \in B_p(L)$ such that $\psi^\sigma = \psi^g$ and $\mathbb{Q}(\psi) \subseteq \mathbb{Q}_p$. By Corollary 6.3, there exists a rational character of G over ψ, and this is impossible. All of this proves that there are no rational elements in L. This easily implies that we may assume that $L = 1$. By Corollary 4.6, we

have that G has exactly two real classes, and therefore, G has exactly two rational classes. □

8. Groups with one rational character

In this section we study finite groups with no non-trivial irreducible rational characters. We use the classification of finite simple groups.

8.1. Lemma. *Suppose that G is a simple sporadic group. Then $|Irr_{rat}(G)| \geq 6$. Also G has a non-trivial irreducible rational character of odd degree.*

Proof. Check the Atlas [4]. □

Next we prove that groups with no non-trivial rational irreducible character have odd order.

8.2. Theorem. *Let G be a finite group. If G has exactly one irreducible rational character, then G has odd order.*

Proof. We argue by induction on $|G|$. Let N be a minimal normal subgroup of G. By induction, G/N has odd order. If $|N|$ is odd, then G has odd order. So we may assume that N has even order, and if $N < G$, by induction N has a non-trivial rational irreducible character. Hence so has G by Corollary 2.2. So we may assume that G is simple. If G is sporadic, then Lemma 8.1 applies. If G is of Lie type, then the Steinberg character is a rational irreducible character of G. If $G = \mathrm{Alt}_n$, then G has a rational irreducible character of degree $n-1$, for instance. □

We have to work much harder, however, to prove that every group of even order has a non-trivial rational irreducible character of odd degree. (See Theorem 9.6 below.)

9. Rational characters of simple groups

In this section we will need some basic facts from the Deligne-Lusztig theory of complex irreducible characters of finite groups of Lie type [3], [5], [6], [17], [18]. Let $\mathcal{G}$ be a connected reductive algebraic group in characteristic p and F a Frobenius morphism of $\mathcal{G}$. Recall that to each F-stable maximal torus $\mathcal{T}$ of $\mathcal{G}$ and a character $\theta \in \mathrm{Irr}(\mathcal{T}^F)$ one can define the Deligne-Lusztig (virtual) character $R_{\mathcal{T}}^{\mathcal{G}}(\theta)$; cf. [3], [6]. The characters $R_{\mathcal{T}}^{\mathcal{G}}(\theta)$ are parametrized by the $\mathcal{G}^F$-conjugacy classes of pairs $(\mathcal{T}, \theta)$. Let $\mathcal{G}^*$ be a simple algebraic group with a Frobenius map F^* such that $(\mathcal{G}^*, F^*)$ is dual to $(\mathcal{G}, F)$. Then the $\mathcal{G}^F$-conjugacy classes of $(\mathcal{T}, \theta)$ are in bijective correspondence Π with the ${\mathcal{G}^*}^{F^*}$-conjugacy classes of pairs $(\mathcal{T}^*, s)$, where $s \in {\mathcal{G}^*}^{F^*}$ is semisimple and $\mathcal{T}^*$ is an F^*-stable maximal torus containing s (cf. Prop. 13.13 of [6]); in particular, one can label $R_{\mathcal{T}}^{\mathcal{G}}(\theta)$ by $R_{\mathcal{T}^*,s}$. This correspondence Π is explicitly described in [6]. Now assume that $s \in {\mathcal{G}^*}^{F^*}$ is semisimple and $\mathbf{C}_{\mathcal{G}^*}(s)$ is connected. Then to the ${\mathcal{G}^*}^{F^*}$-conjugacy class of s one can associate the **semisimple** character

$$\chi_s = \frac{\pm 1}{|W(s)|} \sum_{w \in W(s)} R_{\mathcal{T}_w^*, s} \ ,$$

where $W(s)$ is the Weyl group of $\mathbf{C}_{\mathcal{G}^*}(s)$, $\mathcal{T}_w^*$ is a torus of $\mathcal{G}^*$ of type w and the sign $\pm$ is chosen such that $\chi_s(1) > 0$; cf. [6]. By Corollary 14.47 of [6], χ_s is an irreducible character of $\mathcal{G}^F$, of degree $|{\mathcal{G}^*}^{F^*} : \mathbf{C}_{\mathcal{G}^{*F^*}}(s)|_{p'}$.

A construction of rational characters of G of p'-degree is provided in the following statement.

9.1. Lemma. *Assume $s \in \mathcal{G}^{*F^*}$ is a rational semisimple element such that $\mathbf{C}_{\mathcal{G}^*}(s)$ is connected. Then χ_s is a rational irreducible character of p'-degree of $\mathcal{G}^F$.*

Proof. It suffices to show that χ_s is rational. Observe that $\mathcal{T}^{*F^*}$ is isomorphic to $\mathrm{Irr}(\mathcal{T}^F)$ (considered under multiplication), and the above correspondence Π specifies an isomorphism between them (cf. Remark 10.3 of [10]). Hence if $(\mathcal{T}, \theta)$ corresponds to $(\mathcal{T}^*, s)$ under Π, then the multiplicative order of θ is equal to $n = \mathrm{o}(s)$. In particular, $\mathbb{Q}(R_{\mathcal{T},\theta})$ is contained in the n-th cyclotomic field $\mathbb{Q}_n$. Fix a primitive n-th root γ of unity in $\mathbb{Q}_n$ and consider any Galois automorphism σ of $\mathbb{Q}_n$ over $\mathbb{Q}$. Then $\sigma(\gamma) = \gamma^k$ for some integer k coprime to n. Recall (Theorem 7.2.8 of [3]) that if t and u are the semisimple and unipotent parts of any element $g \in \mathcal{G}^F$ and $\mathcal{C}$ is the connected component of $\mathbf{C}_{\mathcal{G}}(t)$, then

$$R_{\mathcal{T}}^{\mathcal{G}}(\theta)(g) = \frac{1}{|\mathcal{C}^F|} \sum_{x \in \mathcal{G}^F} \theta(x^{-1}tx) Q^{\mathcal{C}}_{x\mathcal{T}x^{-1}}(u).$$

Since the Green functions $Q^{\mathcal{C}}_{x\mathcal{T}x^{-1}}(\cdot)$ are rational, it follows that $(R_{\mathcal{T}}^{\mathcal{G}}(\theta))^\sigma = R_{\mathcal{T}}^{\mathcal{G}}(\theta^k)$. But $(\mathcal{T}, \theta^k)$ corresponds to $(\mathcal{T}^*, s^k)$ under Π, so $(\chi_s)^\sigma = \chi_{s^k}$. Since s and s^k are $\mathcal{G}^{*F^*}$-conjugate by rationality of s, we conclude that χ_s is stable under σ. □

9.2. Corollary. *Let $\mathcal{G}$ be a simple algebraic group of adjoint type in characteristic 2, and let F be a Frobenius map on $\mathcal{G}$. Assume in addition that $\mathcal{G}^F$ is not solvable. Then $\mathcal{G}^F$ has an irreducible rational character χ_s of odd degree > 1.*

Proof. Note that $\mathbf{Z}(\mathcal{G}) = 1$ is connected, whence the centralizer of any semisimple element in $\mathcal{G}^*$ is connected; cf. Remark 13.15 of [6]. First we consider the case where $G := \mathcal{G}^F$ is not a Suzuki group. Then one can embed $X = SL_2(q)$ in $\mathcal{G}^{*F^*}$ for some power q of 2. Clearly, X contains a rational non-central element s of order 3. Now Lemma 9.1 implies that χ_s is irreducible, rational of odd degree. We claim that $\chi_s(1) > 1$. Assume the contrary. The assumption that $\mathcal{G}^F$ is not solvable implies by the classification of finite groups of Lie type [3] that $S := [G, G]$ is simple non-abelian. Furthermore, $S = L/\mathbf{Z}(L)$ where L is the finite Lie-type group of simply connected type in the same isogeny class of G, and $|L| = |G|$. Moreover, we can identify L with $\mathcal{G}^{*F^*}$ since the defining characteristic for L is 2. Obviously, G has at most $|G : S| = |L|/|S| = |\mathbf{Z}(L)|$ irreducible characters of degree 1. On the other hand, Lusztig's classification of irreducible characters of G gives at least $|\mathbf{Z}(L)|$ irreducible characters of degree 1, namely the semisimple characters χ_z corresponding to central elements $z \in \mathbf{Z}(L)$. It follows that $\chi_s = \chi_z$ for some $z \in \mathbf{Z}(L)$. Since Lusztig series are disjoint (cf. Prop. 14.41 of [6]), we conclude that s and z are L-conjugate, whence $s \in \mathbf{Z}(L)$, contrary to the choice of s. Next assume $G \cong {}^2B_2(q)$ with $q > 2$. Then $\mathcal{G}^{*F^*}$ contains a rational non-central element s of order 5. Then we can again apply Lemma 9.1 to χ_s and argue as above. □

9.3. Lemma. *Assume $n \geq 5$. Then the alternating group Alt_n has at least 2 irreducible rational characters α, β of distinct degrees d and $d + 1$ with $d > 1$.*

Proof. The case $n = 5$ is clear, so we will assume $n \geq 6$. Under this assumption, the Specht modules of Sym_n corresponding to the partitions $(n-2,2)$ and $(n-2,1^2)$ are irreducible over Alt_n and have degrees d and $d+1$ with $d = n(n-3)/2$. □

9.4. Lemma. (i) *Let $S = PSL_2(q)$ with $q \geq 4$ and $q \neq 3^{2a+1}$ for any $a \geq 1$. Then S has at least two irreducible rational characters α, β of distinct degrees $d, e > 1$ with d odd. The same is true for $SL_2(3^{2a+1})$ with $a \geq 1$.*

(ii) *Let $S = PSL_2(3^{2a+1})$ for some $a \geq 1$. Then S has one class of involutions and exactly one non-trivial irreducible rational character α. Furthermore, $\alpha(1) = 3^{2a+1}$.*

Proof. We will prove this lemma by using the character table of $G = SL_2(q)$ (both for odd and even q) as given in [7] (and the notation therein for the irreducible characters of G). Clearly, the Steinberg character α of G is rational of degree q and it is trivial on $Z = \mathbf{Z}(G)$. If $q \equiv 1 (\mathrm{mod}\ 3)$, then one can take β to be the character $\chi_{(q-1)/3}$ of degree $q+1$. If $q \equiv -1 (\mathrm{mod}\ 3)$, then take β to be the character $\theta_{(q+1)/3}$ of degree $q-1$. If 3 divides q and $q \equiv 1 (\mathrm{mod}\, 4)$, then take β to be the character $\chi_{(q-1)/4}$ of degree $q+1$. In all of these cases, β_Z is trivial.

From now on we assume that $q = 3^{2a+1}$ for some $a \geq 1$. Observe that $\theta_{(q+1)/4}$ is a faithful irreducible rational character of G. It is straighforward to check that every $\rho \in \mathrm{Irr}(S) \setminus \{1_S, \alpha\}$ is not rational (indeed, either $\rho = \chi_{2k}$ and $\mathbb{Q}(\rho) = \mathbb{Q}(\cos(4\pi k/(q-1)))$, or $\rho = \theta_{2k}$ and $\mathbb{Q}(\rho) = \mathbb{Q}(\cos(4\pi k/(q+1)))$, for some k with $1 \leq k \leq (q-3)/4$). Finally, every involution in S lifts to an element of order 4 in G, and G has exactly one class of elements of order 4. □

In what follows, we will use the notation $GL_n^\epsilon(q)$ to denote $GL_n(q)$ if $\epsilon = +$ and $GU_n(q)$ if $\epsilon = -$. Similarly, E_6^ϵ denotes type E_6 if $\epsilon = +$ and type ${}^2E_6$ if $\epsilon = -$.

9.5. Theorem. *Let S be a non-abelian finite simple group. Then exactly one of the following statements holds:*

(i) *S has at least two irreducible rational characters α, β of distinct degrees $d, e > 1$ with d odd.*

(ii) *$S \cong PSL_2(3^{2a+1})$ for some $a \geq 1$ and S has exactly one non-trivial irreducible rational character α. Furthermore, $\alpha(1) = 3^{2a+1}$.*

Proof. In view of Lemmas 8.1, 9.3 and 9.4, we may assume that S is a Lie type group in characteristic p and moreover $S \ncong PSL_2(q)$. We can consider S as the commutator subgroup of $G := \mathcal{G}^F$ for some simple algebraic group $\mathcal{G}$ of adjoint type and some Frobenius map F on $\mathcal{G}$.

1) First we consider the case $p > 2$. Then we can take α to be the Steinberg character. If $S = PSL_n(q)$ with $n \geq 3$, then choose $\beta = \rho - 1_S$, where ρ is the doubly transitive permutation character of degree $(q^n - 1)/(q-1)$ of S. If $S = PSU_3(q)$, then choose β to be the cuspidal unipotent character of degree $q(q-1)$. Next assume that S is one of the groups $PSU_n(q)$ with $n \geq 4$, $PSp_{2n}(q)$ with $n \geq 2$, $P\Omega_{2n+1}(q)$ with $n \geq 3$, and $P\Omega_{2n}^\pm(q)$ with $n \geq 4$. It is well known (see [23], for instance) that S has a rank 3 permutation character, with two non-trivial irreducible constituents of distinct degrees, which are not p-powers. By the uniqueness of their degrees, any of these two constituents is rational, and we can choose β to be any of these two. Now we can suppose S is an exceptional group of Lie type. If $S = G$, then by Lemma 9.1 we can choose $\beta = \chi_s$, with s any (non-central) involution in $\mathcal{G}^{*F^*} \cong S$. There remain groups of types $E_6^\pm$ and E_7 to

be considered. For these groups, it is shown in [20] that S has a unique non-trivial (unipotent) irreducible character of smallest degree. For the reader's convenience we list this smallest degree e. We have that $e = q(q^4+1)(q^6+\epsilon q^3+1)$ if $S = E_6^\epsilon(q)$ with $\epsilon = \pm$, and $e = q(q^6+1)(q^{14}-1)/(q^4-1)$ if $S = E_7(q)$. So we can choose β to be this smallest degree character.

2) From now on we may assume $p = 2$. Choosing β to be the Steinberg character, we need to find an $\alpha \in \mathrm{Irr}(S)$ of odd degree $d > 1$. By Corollary 9.2, G has a rational irreducible character χ_s of odd degree > 1. If $|G:S|$ is a 2-power we can take α to be $(\chi_s)_S$. It remains to consider groups of types $A_{n-1}^\epsilon(q)$ and $E_6^\epsilon(q)$ with $\epsilon = \pm$ and $n \geq 3$ (and $|G:S|$ not a 2-power). Here we consider the case where $S = PSL_3^\epsilon(q)$ with $3|(q-\epsilon 1)$. It suffices to show that any irreducible S-constituent θ of the character χ_s of G constructed in Corollary 9.2 is rational, and we may assume that $(\chi_s)_S = \sum_{i=1}^3 \theta_i$ with θ_i being G-conjugate to θ. Let $g \in S$. If $\mathrm{cl}_G(g) = \mathrm{cl}_S(g)$, then $\theta(g) = \chi_s(g)/3 \in \mathbb{Q}$. The conjugacy classes of $SL_3^\epsilon(q)$ are described in [22]. In particular, we see that $\mathrm{cl}_G(g) \neq \mathrm{cl}_S(g)$ can happen only when g is a regular unipotent element (of order 4) of S, in which case g turns out to be rational and so $\theta(g) \in \mathbb{Q}$ as well.

3) For the remaining groups S, we can find a simple simply connected algebraic group $\mathcal{H}$ and a Frobenius map F on $\mathcal{H}$ such that $S = L/\mathbf{Z}(L)$ for $L := \mathcal{H}^F$. Let the pair $(\mathcal{H}^*, F^*)$ be dual to $(\mathcal{H}, F)$. Here we consider the case where S is of type $E_6^\epsilon(q)$. Then $F_4(2)$ embeds in $\mathcal{H}^{*F^*}$ and so $\mathcal{H}^{*F^*}$ contains a rational non-central element s of order 5. Note that $\mathcal{H}$ is the universal cover for $\mathcal{H}^*$ and 5 is coprime to $|\mathbf{Z}(\mathcal{H})|$. Hence by Corollary E-II.4.6 of [1], $\mathbf{C}_{\mathcal{H}^*}(s)$ is connected. Therefore the semisimple character χ_s is an irreducible rational character of odd degree > 1 of L by Lemma 9.1. But $s \in [\mathcal{H}^{*F^*}, \mathcal{H}^{*F^*}]$, so χ_s is trivial at $\mathbf{Z}(L)$ by [18], and so we can view χ_s as an S-character and we are done in this case.

Finally, we consider the case $S = PSL_n^\epsilon(q)$ with $n \geq 5$. Then $\mathcal{H}^{*F^*} = PGL_n^\epsilon(q)$ contains a rational non-central element s of order 3, which lifts to an element $\hat{s}$ in $GL_n^\epsilon(q)$ that is conjugate to $\mathrm{diag}(\omega, \omega^{-1}, 1, \ldots, 1)$ in $\hat{\mathcal{H}}^* := GL_n(\overline{\mathbb{F}}_q)$, where $\omega \in \overline{\mathbb{F}}_q$ has order 3. Now if $g \in \mathbf{C}_{\mathcal{H}^*}(s)$, then $\hat{g}\hat{s}\hat{g}^{-1} = \lambda\hat{s}$ for an inverse image $\hat{g} \in \hat{\mathcal{H}}^*$ of g and $0 \neq \lambda \in \overline{\mathbb{F}}_q$. Recall that $n \geq 5$, so $\hat{s}$ has eigenvalue 1 with multiplicity $n-2 \geq 3$ and eigenvalues ω, ω^{-1} both with multiplicity 1. The same is true for $\hat{g}\hat{s}\hat{g}^{-1} = \lambda\hat{s}$. It follows that $\lambda = 1$. Thus $\mathbf{C}_{\mathcal{H}^*}(s) = \mathbf{C}_{\hat{\mathcal{H}}^*}(s)/\mathbf{Z}(\hat{\mathcal{H}}^*)$ and so $\mathbf{C}_{\mathcal{H}^*}(s)$ is connected (as the centralizer of any element in $\hat{\mathcal{H}}^*$ is connected). Furthermore, $s \in [\mathcal{H}^{*F^*}, \mathcal{H}^{*F^*}]$. Arguing as above, we see that the semisimple character χ_s of L is in fact an irreducible rational character of odd degree > 1 of S. □

The following is Theorem B. The reduction to simple groups (which was already noticed in [21]) is the same as in Theorem 8.2.

9.6. Theorem. *Let G be a finite group of even order. Then G has a non-trivial irreducible rational character of odd degree.*

Proof. The same argument as in the proof of Theorem 8.2 shows that we may assume that G is simple. Now, we apply Theorem 9.5. □

9.7. Corollary. *Let G be a finite group. Then the following are equivalent:*

(i) *G has odd order.*

(ii) *G has exactly one irreducible rational character.*

(iii) *G has exactly one rational conjugacy class.*
(iv) *G has exactly one absolutely irreducible representation over $\mathbb{Q}$.*

Proof. It is well known that (i) implies (ii) – (iv). Assume $|G|$ is even. Then (iii) obviously fails. By Theorem 9.6, G has a non-trivial irreducible rational character χ of odd degree, and χ has Schur index 1 over $\mathbb{Q}$ by the Brauer-Speiser Theorem. □

Corollary 9.7 is false if one replaces "absolutely irreducible" by "irreducible" in (iv) – C_3 is a counterexample. Furthermore, the example of $SL_2(27)$ shows that G may have two absolutely irreducible representations over $\mathbb{Q}$, but more than two rational conjugacy classes, resp. more than two irreducible rational characters.

10. Non-solvable groups with two irreducible rational characters

We will need the following orbit theorem.

10.1. Theorem. *Let V be a non-trivial finite dimensional $\mathbb{F}_2$-module for the group $S = PSL_2(3^{2a+1})$ with $a \geq 1$. Then there is $v \in V$ such that $\mathbf{C}_S(v)$ has odd order.*

Proof. Since S is perfect, the non-triviality of V implies that V has submodules $U \supset W$ such that U/W is a non-trivial irreducible S-module. Assuming the statement is proved for irreducible modules, we can find $u \in U$ such that $\mathbf{C}_S(u+W)$ has odd order. Since $\mathbf{C}_S(u) \leq \mathbf{C}_S(u+W)$, the statement also holds for V.

Thus we may assume that V is irreducible. By Lemma 9.4, S has a unique class of involutions, say $\mathrm{cl}_S(g)$, of length $q(q-1)/2$ for $q = 3^{2a+1}$. For each $h \in S$, let $V^h := \ker(h-1)$. It suffices to show that $V \neq \bigcup_{h \in \mathrm{cl}_S(g)} V^h$ (indeed, for any $v \in V \setminus \bigcup_{h \in \mathrm{cl}_S(g)} V^h$, $\mathbf{C}_S(v)$ does not contain any involution and so has odd order). Since $|\mathrm{cl}_S(g)| = q(q-1)/2$, it suffices to show that $|V| > |V^g| \cdot q(q-1)/2$. Let $m = \dim(V)$. It is well known that $m \geq (q-1)/2$.

By [9], we have that three conjugates of g generate S. Hence by Lemma 3.2 of [11], $\dim(V^g) \leq m - \lceil m/3 \rceil$. If $a \geq 2$, then $q \geq 243$ and so $|V|/|V^g| \geq 2^{(q-1)/6} > q(q-1)/2$. Assume $a = 1$. Since V is an irreducible $\mathbb{F}_2$-module, $m \geq 26$ by [16], and so $\lceil m/3 \rceil \geq 9$. It follows that $|V|/|V^g| \geq 2^9 > q(q-1)/2$. □

We are finally ready to give a proof of Theorem C.

10.2. Theorem. *Suppose that G is a finite non-solvable group with exactly two rational irreducible characters. If $M := \mathbf{O}^{2'}(G)$ and $N := \mathbf{O}_{2'}(M)$, then $M/N = PSL_2(3^{2a+1})$.*

Proof. Let $\psi \in \mathrm{Irr}(G)$ be the unique non-trivial rational character of G. Let $1 < M$ be the smallest normal subgroup of G such that G/M is solvable. Thus M is perfect. Now, let M/N be a minimal normal subgroup of G/N. Since M/N has even order, it follows by Theorem 9.6, that there exists $\eta \in \mathrm{Irr}(M/N)$ non-trivial, rational of odd degree. By Corollary 2.4, there exists a rational irreducible character of G lying over η, which necessarily is ψ. In particular, it follows that $N \subseteq \ker(\psi)$, while M is not contained in the kernel of ψ. Hence, G/M has odd order (by Lemma 3.1). Also $M = \mathbf{O}^{2'}(G)$.

Now, if $1 \neq \nu \in \mathrm{Irr}(M)$ is rational, by Corollary 2.2 we have that ν lies under ψ. Hence, all non-trivial rational irreducible characters of M are G-conjugate. In particular, all of them have N contained in its kernel.

We may write

$$M/N = S_1 \times \cdots \times S_a\,,$$

where the non-abelian simple groups S_i are transitively permuted by G. Write $S = S_1$ and by Theorem 9.6, let $\theta \in \mathrm{Irr}(S)$ be rational, non-trivial, of odd degree. Suppose that $a \geq 2$. Since $\theta \times 1 \times \cdots \times 1 \in \mathrm{Irr}(M/N)$ and $\theta \times 1 \times \cdots \times \theta \in \mathrm{Irr}(M/N)$ cannot be G-conjugate, we deduce that $a = 1$. Now, we know that all irreducible non-trivial rational characters of S are G-conjugate, and in particular they have the same degree. By Theorem 9.5, we have that $S = M/N = PSL_2(3^{2a+1})$.

Suppose that $\mathbf{O}^2(N) < N$, and let N/U be a chief factor of G with N/U a 2-group. We are going to prove that G/U has more than two irreducible rational characters. This contradiction will prove that $\mathbf{O}^2(N) = N$. Working in G/U, we may assume that $U = 1$. By Corollary 2.2, it is enough to show that there exists an irreducible rational character τ of M such that N is not in the kernel of τ.

We have that $N \subseteq \mathbf{C}_M(N) \subseteq M$. If $N = \mathbf{Z}(M)$, then we deduce that $M = SL_2(3^{2a+1})$. In this case, M has a rational irreducible character τ such that N is not contained in $\ker(\tau)$ by Lemma 9.4.

Thus, we may assume that $\mathbf{C}_M(N) = N$. Now, we have that $V = \mathrm{Irr}(N)$ is a non-trivial $GF(2)$-module for S. By Theorem 10.1, there exists $\lambda \in \mathrm{Irr}(N)$ such that if T is the stabilizer of λ in M, then T/N is of odd order. Now, let $\hat{\lambda} \in \mathrm{Irr}(T)$ be the canonical extension, and notice that $(\hat{\lambda})^M$ is a rational irreducible character of M which does not contain N in its kernel. This shows that $N = \mathbf{O}^2(N)$.

Finally, suppose that N has even order. Then there exists a non-trivial rational character ρ of odd degree by Theorem 9.6. Since $\mathrm{o}(\rho) = 1$ (because $\mathbf{O}^2(N) = N$), by Corollary 2.4, we have that ψ lies over ρ. But this is impossible since $N \subseteq \ker(\psi)$. We deduce that N has odd order, and the proof of the theorem is complete. □

11. Non-solvable groups with two rational classes

We start with the following result.

11.1. Theorem. *Let S be a finite non-abelian simple group. Then either S contains a rational element of order 3, or $S = {}^2B_2(q)$ and S contains a rational element of order 5, or $S = PSL_2(3^n)$ for some odd $n \geq 3$.*

Proof. The sporadic groups can be checked directly. Also, any simple alternating group contains a 3-cycle which is rational. So let S be a finite simple group of Lie type in characteristic p. The claim is well known for ${}^2B_2(q)$. On the other hand, the Ree groups ${}^2G_2(3^n)$ contain ${}^2G_2(3) = PSL_2(8) \cdot 3$, and $PSL_2(8)$ contains a rational element of order 3. For all other groups, if $p \neq 3$, then S contains either $SL_2(p)$ or $PSL_2(p)$, which both contain rational elements of order 3. Assume $p = 3$. Notice that $PSL_2(3^{2a})$ contains $PSL_2(9) \simeq \mathrm{Alt}_6$ for any integer $a \geq 1$. So we may assume S is not of type A_1. Next we observe that the groups $SL_3(3)$, $SU_2(9)$, $SU_3(3)$, $\Omega_5(3)$, and $G_2(3)$ all contain rational elements of order 3. So we are done if $S = PSL_m(3^n)$ with $m \geq 3$ (as it contains $SL_3(3)$), or if $S = PSU_m(3^n)$ with $m \geq 3$ (as it contains $SU_3(3)$ for odd n and $SL_2(9)$ for even n). All the other classical groups in characteristic 3 contain $\Omega_5(3)$. Finally, all the remaining exceptional Lie-type groups contain $G_2(3)$, and so we are done. □

One can show using Lemma 5.2 that if a finite group G has subgroups $K \lhd H$ such that $H/K \simeq \mathrm{Sym}_3$, then G has a rational element of order 3. Hence one can also deduce Theorem 11.1 from the determination of the finite simple groups that are Sym_3**-free** obtained by G. Glauberman and B. Stellmacher without using the classification of finite simple groups.

Now we will work with the following condition:

($\star$) : The group G has one class of involutions, no real elements of order 4, and no rational element of odd prime order.

Note that if G is of even order, then ($\star$) is equivalent to the condition $|\mathrm{cl}_{\mathrm{rat}}(G)| = 2$ by Lemma 5.1.

11.2. Theorem. *Assume that G is any finite non-solvable group with property ($\star$). Then $S \lhd G/\mathbf{O}_{2'}(G) < Aut(S)$ and $|G|/|S|$ is odd, where $S = PSL_2(3^{2a+1})$ for some $a \geq 1$.*

Proof. By Lemmas 5.1 and 5.2, $G/\mathbf{O}_{2'}(G)$ satisfies ($\star$). So without loss we may assume that $\mathbf{O}_{2'}(G) = 1$. Consider the generalized Fitting subgroup $F^*(G) = F(G)E(G)$.

1) First assume that $E(G) \neq 1$. Then $E(G)$ is a central product of quasisimple subgroups K_i, $1 \leq i \leq m$. By Theorem 11.1 and Lemma 5.2, $K_i/\mathbf{Z}(K_i) = PSL_2(3^{n_i})$ for some odd $n_i \geq 3$. But $SL_2(3^{n_i})$ contains a real element of order 4. Hence ($\star$) implies that $\mathbf{Z}(K_i) = 1$ for all i. It follows that $E(G) = K_1 \times \ldots \times K_m$. Notice that G permutes the subgroups $K_1, \ldots, K_m$. If $m \geq 2$, then by choosing involutions $x_i \in K_i$ we see that x_1 and $x_1 \ldots x_m$ are two involutions which are not G-conjugate, contrary to ($\star$). We have shown that $E(G) = S = PSL_2(3^{2a+1})$ for some $a \geq 1$. Clearly, $\mathbf{O}_2(G) \cap S = 1$, whence ($\star$) implies that $\mathbf{O}_2(G) = 1$. Thus $F(G) = \mathbf{O}_{2'}(F(G)) \leq \mathbf{O}_{2'}(G) = 1$, and so $F^*(G) = S$. By the fundamental property of the generalized Fitting subgroup, $\mathbf{C}_G(S) = \mathbf{Z}(S) = 1$, and so G embeds in $\mathrm{Aut}(S)$. Notice that the elements of order 3 in S form two conjugacy classes in S which are permuted by any outer automorphism of order 2 of S. We conclude that $|G/S|$ is odd.

2) From now on we may assume that $E(G) = 1$ and, as above, $\mathbf{O}_{2'}(F(G)) = 1$, whence $F := F^*(G) = \mathbf{O}_2(G) \neq 1$. Again, $\mathbf{C}_G(F) = \mathbf{Z}(F)$ and G is non-solvable, so $\mathrm{Aut}(F)$ must be non-solvable. Now if F has only one involution, then F is either cyclic or (generalized) quaternion, and so $\mathrm{Aut}(F)$ is solvable, a contradiction. Thus F has more than 1 involution and G acts transitively on the set of involutions of F; in other words, F is a 2-automorphic 2-group [8]. Let $r := |\Omega_1(\mathbf{Z}(F))|$. By the main results of [8] and [24], such a group F is either homocyclic, or of exponent 4, class 2 and order r^2 or r^3. Moreover, it is proved in [2] that if F has class 2 and order r^3, then F is a Suzuki 2-group and $\mathrm{Aut}(F)$ is solvable, which is impossible under our assumptions. In the remaining two cases, $W := F/\Phi(F)$ is an elementary abelian group of order r, and F acts (via conjugation) trivially on W.

3) We claim that G/F acts faithfully on W and moreover it permutes the non-trivial elements of W transitively. Indeed, it is well known that $\mathbf{C}_G(W)/\mathbf{C}_G(F)$ contains no non-trivial element of odd order, whence it is a 2-group. But $\mathbf{C}_G(W) \geq F$, $\mathbf{C}_G(F) = \mathbf{Z}(F)$, and $F = \mathbf{O}_2(G)$, so $\mathbf{C}_G(W) = F$. Now pick any involution $z \in \mathbf{Z}(F)$. Then the set of 2^{b-1}-th roots (in the homocyclic case), resp. of square roots (in the class 2 case), of z is exactly a coset in $F/\Phi(F)$. Since G permutes the involutions in $\mathbf{Z}(F)$ transitively, we conclude that G permutes the non-trivial elements of W transitively.

4) The results of 3) show that the semidirect product $W : (G/F)$ is a doubly transitive affine permutation group (on the elements of W), with a point stabilizer G/F. Recall that G/F is non-solvable. Now we can apply Hering's theorem as stated in [19] to this affine permutation group. This implies that G/F contains a normal quasisimple subgroup H, either of type A_{t-1} or C_t with $t \geq 2$, or G_2, all in

characteristic 2, or Alt_7. By Theorem 11.1, H, and so G/F and G as well, contains a rational element of order 3, a contradiction. □

We will need the following trivial lemma:

11.3. Lemma. *Let ζ be a complex primitive p-th root of unity for some prime $p \geq 3$. Assume that $\sum_{i=1}^{m}(\zeta^{t_i}+\zeta^{-t_i}) \in \mathbb{Q}$ for some sequence $t_1, \ldots, t_m$ of integers coprime to p. Then the sequence $\pm t_1, \ldots, \pm t_m$ contains each residue $l \in (\mathbb{Z}/p\mathbb{Z})^\times$ with the same multiplicity. Moreover, $\sum_{i=1}^{m}(\zeta^{kt_i}+\zeta^{-kt_i}) \in \mathbb{Q}$ for any $k \in \mathbb{Z}$.*

Proof. For each k, $1 \leq k \leq p-1$, let n_k denote the multiplicity that the residue $k(\mathrm{mod}\, p)$ occurs in the sequence $\pm t_1, \ldots, \pm t_m$, and let

$$f(x) := \sum_{k=1}^{p-1} n_k x^k - \sum_{i=1}^{m}(\zeta^{t_i}+\zeta^{-t_i}) \in \mathbb{Q}[x].$$

Then $f(\zeta) = 0$ by the assumption, whence $f(x) = a\sum_{k=0}^{p-1} x^k$ for some $a \in \mathbb{Q}$. It follows that $n_1 = \ldots = n_{p-1} = a$ as stated. The second statement is now obvious. □

11.4. Lemma. *Let $q = 3^{2c+1} \geq 27$ and $S = PSL_2(q)$ be a normal subgroup of odd index of G. Assume in addition that $C_G(S) = 1$. Then $|cl_{rat}(G)| = 2$ if and only if $|Irr_{rat}(G)| = 2$.*

Proof. We will use the notation for irreducible characters and conjugacy classes of $SL_2(q)$ as given in [7]. The condition $\mathbf{C}_G(S) = 1$ implies that $S \lhd G \leq \mathrm{Aut}(S)$. Since $|G/S|$ is odd, G/S can induce only field automorphisms of S. Now we can write $G/S = C_r = \langle \sigma_{3^s} \rangle$ for some integers r, s, where σ_k is the map sending any field element x to x^k for a given integer k. Set $T := \{3^{(i-1)s} \mid 1 \leq i \leq r\}$. Observe that $SL_2(q)$ has a unique conjugacy class of cyclic subgroups of order $q-1$, resp. $q+1$. Moreover one can choose a cyclic subgroup $\langle a \rangle$ of order $q-1$ and a cyclic subgroup $\langle b \rangle$ of order $q+1$ inside $SL_2(q)$ that are invariant under field automorphisms of $SL_2(q)$. For the sake of convenience we will sometimes denote an element $y \in S$ and a preimage of it in $SL_2(q)$ by the same symbol. Note that $\sigma_k(a^l)$ is S-conjugate to a^{kl} and $\sigma_k(b^l)$ is S-conjugate to b^{kl}.

1) First assume that $|\mathrm{Irr}_{\mathrm{rat}}(G)| > 2$. Recall that since $|G/S|$ is odd, G has two rational irreducible characters lying above the principal character and the Steinberg character of S. So G must have another rational irreducible character χ. Consider an irreducible constituent μ of χ_S. Since $|G/S|$ is odd, μ must be real, whence $\mu = \chi_i$ or θ_i for some even integer i with $2 \leq i \leq (q-3)/2$, in the notation of [7]. The two cases are similar, so we will assume that $\mu = \chi_i$ (in particular, it has degree $q+1$).

Let ρ be a complex primitive $(q-1)$-th root of unity. Then χ_k can be labeled in such a way that $\chi_k(a^j) = \rho^{jk} + \rho^{-jk}$. For convenience, we define $\chi_k := \chi_j$ if $k \equiv \pm j(\mathrm{mod}\, (q-1))$, for any integer $k \notin (q-1)/2 + (q-1)\mathbb{Z}$. Then χ_k is uniquely determined by its degree $q+1$ and its value at a. Hence we may represent the G-orbit of χ_i as $\{\chi_{it_j} \mid 1 \leq j \leq m\}$ for some $t_1, \ldots, t_m \in T$. Also let $n := \mathrm{o}(\rho^i)$; in particular $n|(q-1)/2$ and $n \geq 3$. Since $q \equiv 3(\mathrm{mod}\, 8)$, we can find a prime divisor $p \geq 3$ of n and consider $\zeta := \rho^{ni/p}$. Since χ is rational, $\sum_{j=1}^{m}\chi_{it_j}(a^{n/p}) = \sum_{j=1}^{m}(\zeta^{t_j}+\zeta^{-t_j})$ is rational. By Lemma 11.3, this implies that the set $\{\pm t_1, \ldots, \pm t_m\}$ covers all residues in $(\mathbb{Z}/p\mathbb{Z})^\times$. Now the element $g := a^{ni/p}$ has order p (both in $SL_2(q)$ and

in S). Given any residue $l \in (\mathbb{Z}/p\mathbb{Z})^\times$, we have $l = \pm t_j (\mathrm{mod}\ p)$ for some j, whence $\sigma_{t_j}(g)$ is S-conjugate to g^l. Since the automorphism σ_{t_j} is induced by some $x_j \in G$, we conclude that g is rational in G, and so $|\mathrm{cl}_{\mathrm{rat}}(G)| > 2$.

2) Now we assume that $|\mathrm{cl}_{\mathrm{rat}}(G)| > 2$. Consider a non-trivial rational element $g \in G$ which is not conjugate to a (fixed) involution in S. Since $|G/S|$ is odd, no element in $G \setminus S$ and no element of order 3 of S can be real in G; in particular, $g \in S$ and $\mathrm{o}(g) \neq 3$. Thus $\mathrm{o}(g) > 3$ is odd or twice an odd number. By Lemma 5.1 we may assume that g has prime order $p \geq 3$, and write $g = a^i$ or b^i for some integer i. Moreover, we can choose $i \in 2\mathbb{Z}$ if $g = a^i$, and $i \in 4\mathbb{Z}$ if $g = b^i$. The two cases are similar, so we assume $g = a^i$. Notice that a^i and a^j are S-conjugate if and only if $i \equiv \pm j (\mathrm{mod}\ (q-1)/2)$. Also, our choice of i ensures that $p = \mathrm{o}(\rho^i)$, where ρ is defined in 1). The rationality of a^i implies that for any residue $l \in (\mathbb{Z}/p\mathbb{Z})^\times$, there is some $t_l \in T$ such that a^{il} and $\sigma_{t_l}(a^i)$ are S-conjugate, i.e. $t_l \equiv \pm l (\mathrm{mod}\ p)$. In this case, $\chi_i^{\sigma_{t_l}} = \chi_{il}$. Thus the G-orbit of χ_i contains all the distinct ones among the χ_{il} with $l \in (\mathbb{Z}/p\mathbb{Z})^\times$. Observe that each such distinct character occurs twice among the χ_{il} with $l \in (\mathbb{Z}/p\mathbb{Z})^\times$. By Lemma 11.3, $\sum_{l \in (\mathbb{Z}/p\mathbb{Z})^\times} \chi_{il}$ is rational at S. (Indeed, Lemma 11.3 implies the rationality at any power of a. At any other element, χ_k is always rational.)

Note that χ_i is real. Since $|G/S|$ is odd, by Corollary 2.2 there is a unique real irreducible character χ of G that lies above χ_i. We will show that χ is rational, which concludes the proof of the lemma (as G contains two other rational irreducible characters that lie above the principal character and the Steinberg character of S). Indeed, χ_S is a rational multiple of $\sum_{l \in (\mathbb{Z}/p\mathbb{Z})^\times} \chi_{il}$ and so it is rational. Let $\mathbb{K} := \mathbb{Q}(\chi) \subseteq \mathbb{R}$ and consider any $\tau \in \mathrm{Gal}(\mathbb{K}/\mathbb{Q})$. Then $\chi_S^\tau = \chi_S$ (because χ_S is rational), whence χ^τ is a real irreducible character of G lying above χ_i. By uniqueness, $\chi^\tau = \chi$. Consequently, χ is rational. □

11.5. Corollary. *Let G be a finite non-solvable group with exactly two rational classes. Then G also has exactly two rational irreducible characters.*

Proof. Clearly, G satisfies condition $(\star)$, so we may apply Theorem 11.2 to G. Arguing as in the first part of Theorem 7.2, we clearly may assume that $\mathbf{O}_{2'}(G) = 1$. Now apply Theorem 11.2 and Lemma 11.4. □

Finally, this will complete the proof of Theorem A:

11.6. Theorem. *Let G be a finite non-solvable group with exactly two rational irreducible characters. Then G also has exactly two rational classes.*

Proof. We proceed by induction on $|G|$. The structure of such a G is described in Theorem 10.2. In particular, G has a unique composition factor of form $S := PSL_2(3^{2a+1})$, $|G|/|S|$ is odd, and the only rational irreducible characters of G are of degree 1 and 3^{2a+1}. First we consider the case $L := \mathbf{O}_{2'}(G) = 1$. Then, S is in fact a normal subgroup of odd index in G. Setting $C := \mathbf{C}_G(S)$, we have $C \cap S = 1$, whence $|C|$ is odd and so $C = 1$. Thus $S \lhd G \leq \mathrm{Aut}(S)$. Consequently, $|\mathrm{cl}_{\mathrm{rat}}(G)| = 2$ by Lemma 11.4.

Hence, we may assume that $L > 1$. Since G/L is non-solvable, we have that $\mathrm{Irr}_{\mathrm{rat}}(G) = \mathrm{Irr}_{\mathrm{rat}}(G/L)$ by hypothesis. Hence, by induction, we have that the class of involutions of G/L is the unique rational non-trivial class of G/L.

Suppose that $1 \neq x \in L$ is rational. Arguing as in the last paragraph of the proof of Theorem 7.2, we will obtain some $1 \neq \psi \in B_p(L)$ with values in $\mathbb{Q}_p$, for

some odd prime p, such that $\psi^\sigma = \psi^g$, where $g \in G$ and $\sigma \in \mathrm{Gal}(\mathbb{Q}_{|G|}/\mathbb{Q})$ fixes p'-roots of unity and has order $p-1$.

Let I be the stabilizer of ψ in G, and $J := \langle I, g\rangle$. We claim that J is solvable. Indeed, some element in J must invert ψ, whence $|J/I|$ is even. But notice that $|G|/|S|$ is odd and $|S|$ is not divisible by 8. It follows that $|I|$ is not divisible by 4, and so I is solvable. By Corollary 6.3, there exists an irreducible rational character (of even degree) of G over ψ. This is impossible. This proves that if $1 \neq x \in G$ is rational, then $1 \neq xL$ is rational in G/L, easily concluding the theorem. □

Theorem A now follows immediately from Theorem 7.2, Corollary 11.5, and Theorem 11.6.

We conclude by observing that there are examples of groups with exactly two irreducible rational characters which have the exact form as in Theorem C.

Let $S = PSL_2(q)$ with $q = 3^7$ and $H = S \cdot 7$ (the extension by the field automorphism σ of order 7). Next, suppose that V is a non-trivial irreducible $\mathbb{F}_{11}H$-module. We claim that the semidirect product $G := VH$ has exactly two rational irreducible characters. First observe that H has exactly two rational irreducible characters. Indeed, $q-1 = 2 \cdot 1093$, $q+1 = 4 \cdot 547$, and 1093 and 547 are primes. Now it is easy to check that H has exactly two rational conjugacy classes and so the observation follows from Corollary 11.5. Next, let $\sigma \in \mathrm{Gal}(\mathbb{Q}_{|G|}/\mathbb{Q})$ be fixing $11'$-roots of unity and sending every 11-th root of unity ξ to ξ^4, so that σ has order 5. Now, if $\psi \in \mathrm{Irr}(G)$ is non-trivial rational and $\lambda \in \mathrm{Irr}(V)$ is an irreducible constituent of ψ_V, then it follows that $\lambda^\sigma = \lambda^h$ for some $h \in H$ by Clifford's theorem. Then

$$\lambda = \lambda^{\sigma^5} = \lambda^{h^5}.$$

Since H is a $5'$-group, it follows that $\lambda = \lambda^h = \lambda^\sigma$. But then $\lambda = 1_V$ and thus $\psi = \chi$, the unique non-trivial rational character of $G/V = H$.

References

[1] A. Borel, R. Carter, C. W. Curtis, N. Iwahori, T. A. Springer, R. Steinberg, *Seminar on Algebraic Groups and Related Finite Groups, Lect. Notes in Math.* **131**, Springer-Verlag, Berlin, 1970.

[2] E. G. Bryukhanova, *Automorphism groups of* 2*-automorphic* 2*-groups*, Algebra i Logika **20** (1981), 5–21, 123. MR635647 (83c:20036)

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

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

[5] P. Deligne, G. Lusztig, *Representations of reductive groups over finite fields*, Annals of Math. **103** (1976), 103–161. MR0393266 (52:14076)

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

[7] L. Dornhoff, *Group Representation Theory*, Marcel Dekker, New York, 1972. MR0347960 (50:458b)

[8] F. Gros, 2*-automorphic* 2*-groups*, J. Algebra **40** (1976), 348–353. MR0409642 (53:13394)

[9] R. M. Guralnick, J. Saxl, *Generation of finite almost simple groups by conjugates*, J. Algebra **268** (2003), 519–571. MR2009321 (2005f:20057)

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

[11] R. M. Guralnick, Pham Huu Tiep, *The non-coprime* $k(GV)$*-problem*, J. Algebra **293** (2005), 185–242. MR2173972 (2006g:20018)

[12] B. Huppert, N. Blackburn, *Finite Groups II*, Springer-Verlag, Berlin et al., 1982. MR650245 (84i:20001a)
[13] I. M. Isaacs, *Characters of π-separable groups*, J. Algebra **86** (1984), 98–128. MR727371 (85h:20012)
[14] I. M. Isaacs, *Character Theory of Finite Groups*, Dover, New York, 1994. MR1280461
[15] S. Iwasaki, *On finite groups with exactly two real conjugate classes*, Arch. Math. **33** (1979/80), 512–517. MR570486 (81g:20051)
[16] C. Jansen, K. Lux, R. A. Parker, R. A. Wilson, *An ATLAS of Brauer Characters*, Oxford University Press, Oxford, 1995. MR1367961 (96k:20016)
[17] G. Lusztig, *Characters of Reductive Groups over a Finite Field, Annals of Math. Studies* **107**, Princeton Univ. Press, Princeton, 1984. MR742472 (86j:20038)
[18] G. Lusztig, *On the representations of reductive groups with disconnected centre*, Orbites Unipotentes et Représentations, I. Astérisque, vol. 168, 1988, pp. 157–166. MR1021495 (90j:20083)
[19] M. W. Liebeck, *The affine permutation groups of rank three*, Proc. London Math. Soc. **54** (1987), 477–516. MR879395 (88m:20004)
[20] F. Lübeck, *Smallest degrees of representations of exceptional groups of Lie type*, Comm. Algebra **29** (2001), 2147–2169. MR1837968 (2002g:20029)
[21] I. M. Richards, *Characters of groups with quotients of odd order*, J. Algebra **96** (1985), 45–47. MR808839 (87g:20016)
[22] W. Simpson, J. S. Frame, *The character tables for $SL(3,q)$, $SU(3,q^2)$, $PSL(3,q)$, and $PSU(3,q^2)$*, Can. J. Math. **25** (1973), 486–494. MR0335618 (49:398)
[23] P. Sin, Pham Huu Tiep, *Rank 3 permutation modules of the finite classical groups*, J. Algebra **291** (2005), 551–606. MR2163483 (2006j:20019)
[24] B. Wilkens, *A note on 2-automorphic 2-groups*, J. Algebra **184** (1996), 199–206. MR1402576 (97h:20024)
[25] T. R. Wolf, *Character correspondences in solvable groups*, Ill. J. Math. **22** (1978), 327–340. MR0498821 (58:16858)

Facultat de Matemàtiques, Universitat de València, Burjassot, València 46100, Spain
E-mail address: gabriel@uv.es

Department of Mathematics, University of Florida, Gainesville, Florida 32611
E-mail address: tiep@math.ufl.edu