ILLINOIS JOURNAL OF MATHEMATICS
Volume 33, Number 1, Spring 1988

ON FINITE RATIONAL GROUPS AND RELATED TOPICS[1]

BY

WALTER FEIT AND GARY M. SEITZ

1. Introduction

If H is a finite group and $\chi_1, \dots, \chi_s$ are characters of H let $\mathbf{Q}(\chi_1, \dots, \chi_s)$ be the field generated by all $\chi_i(x)$, $x \in H$, $1 \le i \le s$. If $\chi_1, \dots, \chi_k$ are all the irreducible characters of H let $\mathbf{Q}(H) = \mathbf{Q}(\chi_1, \dots, \chi_k)$.

A character χ is *rational* if $\mathbf{Q}(\chi) = \mathbf{Q}$. A group H is a *rational group* if $\mathbf{Q}(H) = \mathbf{Q}$.

Let Σ_n denote the symmetric group of order n and let A_n denote the alternating group. Σ_n is a rational group. More generally, every Weyl group is a rational group. See [6].

In this paper we prove several results related to the study of rational groups. We determine all nonabelian simple groups which can occur as composition factors of rational groups, in particular the simple rational groups. In addition, we prove that the rational group algebra of any non-trivial finite group has an outer automorphism and show that any outer automorphism of a finite simple group must move a conjugacy class. All these results use the classification of finite simple groups in an essential manner.

THEOREM A. *Let m be a natural number. There is a finite set $\mathscr{F}_m$ of simple groups such that if G is a finite noncyclic simple group which occurs as a composition factor of a group H satisfying $[\mathbf{Q}(H)\colon \mathbf{Q}] \le m$, then G is isomorphic to an alternating group or to a group in $\mathscr{F}_m$.*

Theorem A partially answers a question of John Thompson, leaving open the problem of whether or not there are only finitely many cyclic groups of prime order which occur as composition factors of groups H satisfying $[\mathbf{Q}(H)\colon \mathbf{Q}] \le m$.

Let $\mathscr{S}_m$ be the set of all primes which divide the order of any solvable group H with $[\mathbf{Q}(H)\colon \mathbf{Q}] \le m$. It is known that $\mathscr{S}_m$ is finite [7]. It has

Received January 30, 1987.

[1] Each author was supported in part by a grant from the National Science Foundation.

previously been shown by Gow [11] that $\mathscr{S}_1 = \{2, 3, 5\}$. Conceivably any cyclic composition factor of a group H with $[\mathbf{Q}(H): \mathbf{Q}] \leq m$ has order in $\mathscr{S}_m$.

THEOREM B. *Let G be a noncyclic finite simple group. Then G is a composition factor of a rational group if and only if G is isomorphic to an alternating group or one of the following groups*:
(i) $PSp_4(3)$, $Sp_6(2)$, $O_8^+(2)'$,
(ii) $PSL_3(4)$, $PSU_4(3)$.

Alternating groups and the groups listed in Theorem B(i) are composition factors of Weyl groups. However, the groups in Theorem B(ii) seem almost accidental. It is curious to note that these two groups are also the finite simple groups with the most complicated Schur multipliers.

As corollaries to Theorem B we get:

COROLLARY B.1. *Let G be a noncyclic simple group. Then G is a rational group if and only if $G \approx Sp_6(2)$ or $O_8^+(2)'$.*

COROLLARY B.2. *Let G be a finite group such that any two elements of the same order are conjugate. Then $G \approx \Sigma_n$ for $n = 1, 2$ or 3.*

Corollary B.2 answers a question that appears to have been around a long time. See [13], 7.48, where it is referred to as a well known problem. Graham Higman and John Thompson have drawn our attention to a result of P. Hall which asserts the existence of an infinite torsion group with the property that any two elements of the same order are conjugate. See the Journal of the London Math. Society, vol. 34 (1959), p. 305. This may explain the apparent need of the classification of finite simple groups for the proof of Corollary B.2.

Added in proof. We have been informed by P. Fitzpatrick that he had previously proved Corollary B2 (Proc. Roy. Irish Acad., vol. 85A (1985), pp. 53–58). His proof also depends on the classification of the finite simple groups.

The methods used in proving the above mentioned results also enable us to prove the next two theorems which answer questions of G. Janusz [12].

THEOREM C. *Let α be an outer automorphism of the finite simple group G. Then there exists a conjugacy class C of G with $C^\alpha \neq C$.*

THEOREM D. *Let $G \neq (1)$ be a finite group. Then the group algebra $\mathbf{Q}[G]$ has an outer automorphism.*

The proofs of Theorems A and B are based on some detailed results about finite simple groups of Lie type which may be of independent interest. Of particular importance is the existence of certain self-centralizing cyclic maximal tori, see Theorem 3.1. The investigation of various groups of relatively small order, including the sporadic simple groups, is greatly facilitated by the existence of the ATLAS [6]. This is used throughout the paper.

2. Numerical preliminaries

Let a and n be integers greater than 1. *A Zsigmondy prime for* (a, n) is a prime l such that $l|(a^n - 1)$ but $l \nmid (a^i - 1)$ for $1 \leq i \leq n - 1$. If l is a Zsigmondy prime for (a, n) then $l \equiv 1 \pmod n$ and so $l \geq n + 1$.

If m is a natural number and l is a prime let $|m|_l$ denote the l-part of m. In other words $|m|_l = l^k$ where $l^k|m$ but $l^{k+1} \nmid m$.

A large Zsigmondy prime for (a, n) is a Zsigmondy prime l for (a, n) so that $|a^n - 1|_l > n + 1$. Thus either $l > n + 1$ or $l^2|(a^n - 1)$.

For any natural number n let $\Phi_n(x)$ denote the nth cyclotomic polynomial. Let $\varphi(n)$ be the degree of $\Phi_n(x)$. Thus $\varphi(n)$ is the Euler function. Observe that if l is a Zsigmondy prime for (a, n) then $|\Phi_n(a)|_l = |a^n - 1|_l$.

The next result is proved in [10].

THEOREM 2.1. *If a and n are integers greater than* 1, *then there exists a large Zsigmondy prime for* (a, n) *except in the following cases*:

(i) $n = 2$ *and* $a = 2^s3^t - 1$ *for some natural number* s, *and* $t = 0$ *or* 1.
(ii) $a = 2$ *and* $n = 4, 6, 10, 12$ *or* 18.
(iii) $a = 3$ *and* $n = 4$ *or* 6.
(iv) $a = 5$ *and* $n = 6$.

This immediately implies the following result of Zsigmondy.

THEOREM 2.2. *If a and n are integers greater than* 1, *then there exists a Zsigmondy prime for* (a, n) *unless* $(a, n) = (2, 6)$ *or* $n = 2$ *and* $a = 2^s - 1$ *for some natural number* s.

The following results will also be needed.

LEMMA 2.3. *Let a and n be integers greater than* 1. *Let l be a large Zsigmondy prime for* (a, n) *and let* $l^k = |a^n - 1|_l$. *Let N be a natural number such that* $|\Phi_n(a)|_l|N$ *and* $N|(a^n - 1)$. *Then* $\varphi(N) \geq 2n$. *Furthermore,* $\varphi(N) = 2n$ *if and only if* $l = 2n + 1$ *and* $N = l$ *or* $2l$.

Proof. Since $l^k|N$ it follows that

$$\varphi(N) \geq \varphi(l^k). \tag{2.1}$$

Suppose that $l \geq 2n + 1$. Then (2.1) implies that

$$\varphi(N) \geq \varphi(l) \geq 2n.$$

If $N > 2l$ the first inequality becomes strict. If $l > 2n + 1$, the second inequality becomes strict.

Suppose that $l < 2n + 1$. Thus $l = n + 1$ and $k \geq 2$. By (2.1),

$$\varphi(N) \geq nl^{k-1} \geq n(n+1) > 2n. \qquad \square$$

LEMMA 2.4. *Let m be a natural number. Then $\varphi(m) \geq 1/2\sqrt{m}$ and $\varphi(m) \geq \sqrt{m}$ if m is odd.*

Proof. If p is a prime then $\varphi(p^b) = (p-1)p^{b-1}$ for $b \geq 1$. Thus $\varphi(p^b) \geq \sqrt{p^b}$ if $p \neq 2$ and $\varphi(2^b) \geq 1/2\sqrt{2^b}$. If s, t are relatively prime then $\varphi(st) = \varphi(s)\varphi(t)$. The result follows. □

3. Self centralizing cyclic subgroups of simple groups

Let p be a prime and let $\bar{G}$ be a connected, simple, adjoint, algebraic group over the algebraic closure of $\mathbf{F}_p$. Let σ be an endomorphism of $\bar{G}$ such that the fixed point group $\bar{G}_\sigma$ is finite. Set $G = \mathbf{O}^{p'}(\bar{G}_\sigma)$. Then $G = G(q)$ is a finite group of Lie type, where $q = p^f$ for some natural number f. Throughout this section we assume that G is a simple group. Consequently, we regard $Sp_4(2)'$ as $PSL_2(9)$, $G_2(2)'$ as $PSU_3(3)$, ${}^2G_2(3)'$ as $PSL_2(8)$, and we omit ${}^2F_4(2)'$.

Identify G with $\mathrm{Inn}(G)$, the group of inner automorphisms of G. Thus $G \lhd A$, the group of all automorphisms of G. Set $G_1 = \bar{G}_\sigma$, so G_1 is the group generated by all inner and diagonal automorphisms of G. Set $d = |G_1 \colon G|$. Let

Table I

G	g	d
$A_1(q)$	1	$(2, q-1)$
$A_n(q)$, $n \geq 2$	2	$(n+1, q-1)$
${}^2A_n(q)$, $n \geq 2$	2	$(n+1, q+1)$
$B_n(q)$, $n \geq 3$	1	$(2, q-1)$
$C_n(q)$, $n \geq 3$ or, $n \geq 2$ and q odd	1	$(2, q-1)$
$C_2(2^f)$	2	1
$D_n(q)$, $n \geq 5$	2	$(4, q^n - 1)$
$D_4(q)$	6	$(4, q^n - 1)$
${}^2D_n(q)$, $n \geq 4$	2	$(4, q^n + 1)$

Table II

G	g	d	(a, m)
${}^3D_4(q)$	3	1	$(p, 3f) \neq (2,6)$
$E_6(q)$	2	$(3, q-1)$	$(p, 12f)$
${}^2E_6(q)$	2	$(3, q+1)$	$(p, 12f)$
$E_7(q)$	1	$(2, q-1)$	$(p, 12f)$
$E_8(q)$	1	1	$(p, 30f)$
$F_4(q)$, q odd	1	1	$(p, 8f)$
$F_4(2^f)$	2	1	$(2, 8f)$
$G_2(q)$, $3 \nmid q$	1	1	$(p, 3f) \neq (2,6)$
$G_2(3^f)$	2	1	$(3, 3f)$
${}^2C_2(2^{2a+1})$, $a \geq 1$	1	1	$(2, 4(2a+1))$
${}^2F_4(2^{2a+1})$, $a \geq 1$	1	1	$(2, 12(2a+1))$
${}^2G_2(3^{2a+1})$, $a \geq 1$	1	1	$(3, 6(2a+1))$

g denote the order of the group of graph automorphisms of G. Then $G = G_1'$ is the commutator group of G_1 and

$$|A\colon G| = |G_1\colon G|fg = dfg.$$

See [5], Section 12.5.

Tables I and II contain the values of d and g as G ranges over all simple groups of Lie type (except ${}^2F_4(2)'$). The fourth column in Table II contains a pair of integers (a, m) such that by Theorem 2.2 there always exists a Zsigmondy prime for (a, m).

Table III contains a root α and an element γ of the Weyl group.

w_0 denotes the long word in the Weyl group.

The root r in column 4 of $F_4(q)$ denotes the highest root.

The root r in column 4 of $E_7(q)$ denotes the highest root in the E_6-subsystem.

The main result of this section is the following.

THEOREM 3.1. *Assume $G = \mathbf{O}^{p'}(\overline{G}_\sigma)$ is a simple group of Lie type. Then there exists a maximal torus T of G_1 with the following properties.*

(i) *$T \cap G$ is cyclic and $\mathbf{C}_{G_1}(T \cap G) = T$.*

(ii) *$|T|$ and $e = |\mathbf{N}_{G_1}(T \cap G)\colon T|$ are as in Table III. In the last three rows either square root may be chosen.*

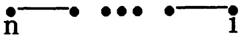
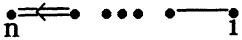
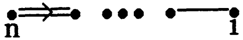
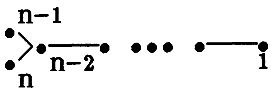
(iii) *$|\mathbf{N}_A(T \cap G)\colon T| \leq efg$.*

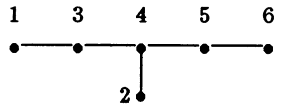
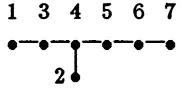
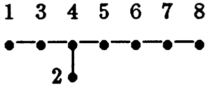
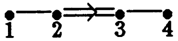
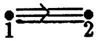
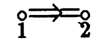
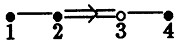
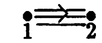
(iv) *If $G \neq PSU_4(2)$ or $D_4(q)$ for $q \leq 5$ then $\mathbf{C}_A(T \cap G) = T$.*

(v) *If $G = D_4(q)$ then $\mathbf{C}_{G_2}(T \cap G) = T$, where G_2 is generated by G_1 and all field automorphisms. Furthermore*

$$|\mathbf{N}_A(T \cap G)\colon \mathbf{C}_A(T \cap G)| \leq 24f.$$

Table III

G_1	Dynkin diagram $\overline{G}$	α	γ	$\lvert T\rvert$	e
$A_n(q)$		$10\cdots0$	$s_1\ \cdots\ s_n$	$(q^{n+1}-1)(q-1)^{-1}$	$n+1$
${}^2A_n(q)$		$10\cdots0$	$s_1\ \cdots\ s_n w_0\tau$	$(q^{n+1}+(-1)^n)(q+1)^{-1}$	$n+1$
$B_n(q)$		$10\cdots0$	$s_1\ \cdots\ s_n$	q^n+1	$2n$
$C_n(q)$		$0\cdots01$	$s_n\ \cdots\ s_1$	q^n+1	$2n$
$D_n(q),\ n\geq 4$		${}^{0}_{1}0\cdots0$	$s_1\ \cdots\ s_{n-1}$	q^n-1	$(2,n)n$
${}^2D_n(q),\ n\geq 4$		${}^{0}_{1}0\cdots0$	$s_1\ \cdots\ s_{n-1}\tau$	q^n+1	n
${}^3D_4(q)$		${}^{0}_{1}0\,0$	$s_1s_2s_3w_0\tau$	$(q^3-1)(q+1)$	4

$E_6(q)$		1000 0	$s_1s_6s_3s_5s_4s_2$	$\Phi_{12}(q)\Phi_3(q)$	12
$^2E_6(q)$		100000 0	$s_1s_6s_3s_5s_4s_2w_0\tau$	$\Phi_{12}(q)\Phi_6(q)$	12
$E_7(q)$		000000 1	$s_rs_6s_4s_2s_7s_5s_3$	$\Phi_{12}(q)(q^3 + 1)$	24
$E_8(q)$		1000000 0	$s_8s_1s_4s_6s_7s_5s_3s_2$	$\Phi_{30}(q)$	30
$F_4(q)$		0001	$s_1s_2s_3s_r$	$q^4 + 1$	8
$G_2(q)$		01	$s_1s_2w_0$	$\Phi_3(q)$	6
$^2C_2(q)$, $q = 2^{2a+1}$		10	$s_1\hat{\tau}$	$q + \sqrt{2q + 1}$	4
$^2F_4(q)$, $q = 2^{2a+1}$		0001	$s_2s_1w_0\hat{\tau}$	$q^2 + q\sqrt{2q} + q + \sqrt{2q} + 1$	12
$^2G_2(q)$, $q = 3^{2a+1}$		10	$s_1w_0\hat{\tau}$	$q + \sqrt{3q} + 1$	6

We will first construct T and then verify that it has the required properties.

Let $\overline{G}$, σ, G and G_1 be as before. Let $\overline{H}$ be a σ-invariant maximal torus of $\overline{G}$ contained in a σ-invariant Borel subgroup. The maximal tori of G_1 are the groups $T = \overline{T}_\sigma$ for $\overline{T}$ a σ-invariant conjugate of $\overline{H}$. Then σ may be considered as an automorphism of the abstract group $\overline{G}$, hence as an element of the semi-direct produce $\overline{G}\langle\sigma\rangle$. Thus if $\overline{T} = \overline{H}^x$ then $[x, \sigma] \in \mathrm{N}_{\overline{G}}(\overline{H}) = \overline{N}$. Consequently there is an element $w \in \overline{N}$ such that $h^{x\sigma} = (h^{w\sigma})^x$ for all $h \in H$. Hence $T \approx \overline{H}_{w\sigma}$. Let $X = X(\overline{H})$ be the character group of $\overline{H}$. Then X is a free Z-module with basis a set of fundamental roots $\alpha_1, \dots, \alpha_n$ of the root system of $\overline{G}$. Both w and σ induce actions on X and $\overline{H}_{w\sigma} \approx X/X(1 - w\sigma)$ [17, II.1.7].

Suppose that $G \neq {}^2C_2(q), {}^2F_4(q), {}^2G_2(q)$. Then σ induces q or $q\tau$ on X, where τ is a graph automorphism. Set $\gamma = w$ or $w\tau$ respectively. By [15, (2.1)] we have

$$|T| = |\overline{H}_{w\sigma}| = f_\gamma(q), \tag{3.1}$$

where f_γ is the characteristic polynomial of γ on $\mathbf{R} \otimes X$.

Let α and γ be chosen as in Table III. Assume $G \neq D_n(q)$. A direct check shows that $\{\alpha_i = \alpha\gamma^{i-1} | 1 \leq i \leq n\}$ is a Z-basis of X, so T is cyclic by [15, (2.2) (iii)]. Now suppose $G = D_n(q)$ and let $*$ denote the image in $X^* = X/X(1 - w\sigma)$. Computing $\alpha_i(1 - w\sigma) = \alpha_i(1 - qw)$ yields the following relations in X^*:

$$\alpha_2^* = q\alpha_1^*, \dots, \alpha_{n-1}^* = q^{n-2}\alpha_1^*,$$
$$\{(q^n - 1)/(q - 1)\}\alpha_1^* = 0,$$
$$(1 - q)\alpha_n^* = q^{n-2}(q + 1)\alpha_1^*.$$

So

$$X^* = \langle\alpha_1^*, \alpha_n^*\rangle \quad \text{and} \quad |\langle\alpha_1^*\rangle| = (q^n - 1)/(q - 1).$$

When n is odd $X^* = \langle\alpha_n^*\rangle$ as $((q^n - 1)/(q - 1), q + 1) = 1$, whence T is cyclic. But for n even X^* has rank 2 and contains a unique cyclic subgroup with quotient $Z_2 \times Z_2 \approx G_1/G$. Hence $T \cap G$ is cyclic.

In the remaining cases let $q = 2^{2a+1}, 2^{2a+1}, 3^{2a+1}$ respectively. Let τ be the graph automorphism of the Dynkin diagram (ignoring lengths of roots). Then σ induces $q_1\bar{\tau}$, where $q_1 = q^{1/2}$ and $\bar{\tau}$ is the isometry of $\mathbf{R} \otimes X$ sending α to $p^{-1/2}\alpha^\tau$ or $p^{1/2}\alpha^\tau$, according to whether α is a short or long root. Then (3.1) again holds, where q is replaced by q_1.

Choose α and γ as in Table III. A direct computation shows that T is cyclic. Therefore $T \cap G$ is cyclic.

LEMMA 3.2. $\mathbf{C}_{G_1}(T \cap G) = T$.

Proof. Suppose this is not the case. Then $\mathbf{C}_{G_1}(T \cap G) \not\subseteq T$. Thus [15], (2.9) implies that $\mathbf{C}_{G_1}(T \cap G)$ contains a unipotent element u. Hence $T \cap G \subseteq \mathbf{C}_{G_1}(u)$. Therefore $T \cap G_1$ is contained in a maximal parabolic subgroup P of G by [3], Proposition 3.12. Let L be a Levi factor of P.

Suppose G occurs in Table I. Let $T \cap G = \langle y \rangle$ and let $\tilde{G}$ be the corresponding covering group which acts on the classical module V associated with G. From the description in [14] of maximal tori in $\tilde{G}$ we see that preimages of y in $\tilde{G}$ have distinct characteristic values. Thus y is centralized by no unipotent element in G_1.

Now suppose that G occurs in Table II. If $G \neq G_2(4)$ or ${}^3D_4(4)$ let r be a Zsigmondy prime for (a, m) and let R be a S_r-group of $T \cap G$. Thus $R \neq \langle 1 \rangle$ is cyclic. Since $r \mid |P|$ it follows that $G = {}^3D_4(q)$ or $E_7(q)$.

If $G = G_2(4)$ then $|T \cap G| = 21$ but no parabolic subgroup of G has order divisible by 7.

If $G = {}^3D_4(q)$, then P must be a parabolic subgroup for which $L' = SL_2(q)$. A consideration of the action of L on $\mathbf{O}_p(P)$ shows that $T \cap G$ centralizes no unipotent element of P, a contradiction.

Suppose $G = E_7(q)$. Here P must be the parabolic subgroup with $L' = E_6(q)$. Let * denote images in $P/\mathbf{O}_P(P)$. Then $(T \cap G)^* \subseteq L^*$ and R^* is a S_r-subgroup of L^*. Also, since $|L^*\colon L'^*| \mid (q-1)$, $(T \cap L')^*$ has index at most 2 in $(T \cap G)^*$. Since r divides the order of no proper parabolic subgroup of L', $\mathbf{C}_{L'}(R)$ is a maximal torus. By Table III, this maximal torus has order $\Phi_{12}(q)\Phi_3(q)$. Now $T \cap L' \subseteq \mathbf{C}_{L'}(R)$, which is inconsistent with the orders of the groups involved. □

LEMMA 3.3. *In each case e has the value in Table III.*

Proof. By Lemma 3.2, $\mathbf{C}_{\overline{G}}(T)^\circ_\sigma \subseteq \mathbf{C}_{G_1}(T \cap G) = T$ where $^\circ$ denotes the connected component of 1. Thus $\mathbf{C}_{\overline{G}}(T)^\circ$ contains no unipotent elements and so $\mathbf{C}_{\overline{G}}(T)^\circ = \overline{T}$. See the argument in [15, (2.6)]. Furthermore, Lemma 3.2 implies that $\mathbf{N}_{G_1}(T \cap G) = \mathbf{N}_{G_1}(T)$. By [17, II.1.8] this yields

$$e = |\mathbf{N}_{G_1}(T \cap G)\colon T| = |\mathbf{C}_W(w\sigma)|.$$

If γ is a Coxeter element then $e = |\langle \gamma \rangle| = 2N/n$, where N is the number of positive roots in the root system associated to $\overline{G}$. See [4], Proposition 30 and [5], Theorem 10.5.3. If γ is a coxeter element times $w_0\tau$ in $A_n(q)$ or $E_6(q)$ the same conclusion holds as $w_0\tau$ inverts $\overline{T}$ and centralizes W.

If $G = E_7(q)$ then $e = 24 = 2|\langle \gamma \rangle|$ and $\mathbf{C}_W(w\sigma) = \langle \gamma \rangle \times \langle w_0 \rangle$. See [4]. If $G = F_4(q)$ or $G_2(q)$ the value of e can be found in [4]. If $G = D_n(q)$, the value of e can be determined directly by viewing γ as an n-cycle in $\Sigma_n \subseteq W(D_n)$.

Let $G = {}^2D_n(q)$. Since $W(D_n) \subseteq W(B_n)$ and τ may be viewed as the reflection corresponding to the missing node, it follows that γ is the Coxeter element in $W(B_n)$. Hence the centralizer of γ in $W(B_n)$ has order $2n$ and so the centralizer in $W(D_n)$ has order n.

The verification for the remaining cases ${}^3D_4(q)$ ${}^2C_2(2^{2a+1})$, ${}^2F_4(2^{2a+1})$ and ${}^2G_2(3^{2a+1})$ can be done explicitly. □

Proof of Theorem 3.1. Lemmas 3.2 and 3.3 imply (i) and (ii). Since $|A\colon G_1| = fg$, (iii) is a consequence of (ii). Note that (2.8) of [15] proves (iv) if $G = D_4(q)$ and $q > 5$. Thus to prove (iv) it may be assumed that $G \neq D_4(q)$. If $G = D_n(q)$ with $n \geq 6$ even, then $\mathbf{N}_A(G)$ is contained in the group G_2 generated by all inner, diagonal, and field automorphisms. Indeed, it follows from [14] that $T \cap G$ is contained in precisely two maximal parabolic subgroups of G (with Levi factors of type A_{n-1}) and the stabilizer of this pair of parabolics is contained in G_2. Since σ is conjugate to $w\sigma$, we may work with $w\sigma$. Let

$$D = \mathbf{N}_{\mathrm{Aut}(\bar{G}'_{w\sigma})}\left(\bar{H}_{w\sigma}\right), \quad C = \mathbf{C}_{\mathrm{Aut}(\bar{G}'_{w\sigma})}\left(\bar{H}_{w\sigma}\right).$$

To prove (iv) it suffices by (iii) to show that $|D\colon C| \geq ef$ if $G = D_n(q)$ with n even and $|D\colon C| \geq efg$ otherwise.

Let δ be the field automorphism of $\bar{G}$ which induces the pth power map on $\bar{H}$. Thus δ induces the pth power map on $\bar{H}_{w\sigma}$, which will also be denoted by δ. Hence $\delta \in D$.

Suppose that $g = 1$ or $G = D_n(q)$ with n even. By Tables I, II and III, δ has order ef on $H_{w\sigma}$ unless $G = E_7(q)$ or $G_2(q)$, when δ has order $ef/2 = 12$ or 3. Therefore $|D\colon C| \geq ef$ except possibly when $G = E_7(q)$ or $G_2(q)$. If one of these cases occurs then w_0 inverts $\bar{H}_{w\sigma}$ and no power of δ inverts $\bar{H}_{w\sigma}$. Thus $|D\colon C| \geq ef$ also in these cases.

If $G = {}^2D_n(q)$ then δ has order efg and if $G = {}^3D_4(q)$ then w_0 inverts $\bar{H}$ and δ has order $efg/2$, so $|\langle \delta, w_0\rangle C\colon C| = efg$. Thus in both of these cases $|D\colon C| \geq efg$.

Suppose that G is $E_6(q)$, ${}^2E_6(q)$, $A_n(q)$, $D_n(q)$ for n odd, or ${}^2A_n(q)$ with $n \geq 2$. Then $w_0\tau$ inverts $\bar{H}_{w\sigma}$. If no power of δ inverts $\bar{H}_{w\sigma}$ then $|D\colon C| \geq efg$ as required. Suppose that some power δ^m of δ inverts $\bar{H}_{w\sigma}$. Then $ef = 2m$. If $\bar{H}_{w\sigma} = \langle y \rangle$ this implies that $y^{p^m+1} = 1$ and so $|T|\,|\,p^m + 1$.

If $G = E_6(q)$ or ${}^2E_6(q)$ then $m = 6f$ and $|T|\,|\,q^6 + 1$ which is not the case as there exists a Zsigmondy prime for $(q, 12)$.

If $G = A_n(q)$ or ${}^2A_n(q)$, then $p^{2m} + \varepsilon\,|\,(p^f + \varepsilon')(p^m + 1)$, where $\varepsilon, \varepsilon' \in \{\pm 1\}$. Also, $2m = (n+1)f > 2f$, so $m > f$. Hence

$$p^{2m} - 1 \leq (p^m + 1)(p^{m-1} + 1),$$

and so $p = m = 2$. The divisibility condition forces $\varepsilon = -1$, $\varepsilon' = 1$, and $G = PSU_4(2)$.

Suppose $G = C_2(2^f)$, $G_2(3^f)$, or $F_4(2^f)$, and recall that in the first two cases we are assuming $f > 1$. Then δ has order ef on $\overline{H}_{w\sigma}$. We have $G = G_1$ and $G_2 = \langle G, \delta\rangle$ has index 2 in A. Suppose $C \neq T$. By Lemma 3.2 and the above remarks, $C \cap G_2 = T$, so $|C\colon T| = 2$. Since $|T|$ is odd there is an involution $t \in C - T$. Since $t \in A - G_2$ and A/G is cyclic, f must be odd. An argument with Lang's theorem yields $\mathbf{C}_G(t) \approx {}^2C_2(2^f)$, ${}^2F_4(2^f)$ or ${}^2G_2(3^f)$ respectively. As T is cyclic, T is contained in a maximal torus of $\mathbf{C}_G(t)$. But then (2.4) (iii) of [15] implies $|T| \leq (q^{1/2} + 1)^r$, for r the Lie rank of G. This is possible only if $q = 2$ and so $G = F_4(2)$ and $|T| = 17$. However, $17 \nmid |{}^2F_4(2)|$, a contradiction.

At this point we have verified (iv). It remains to establish (v). Assume $G = D_4(q)$. From (iv) we have $C_A(T \cap G) = T$ for $q > 5$, so to establish the first assertion in (v) we may assume $q \leq 5$. By Lemma 3.2 we may assume $q = 4$. But here δ has order $8 = 4f$ on $\overline{H}_{w\sigma}$ and no power of δ is inversion, the assertion follows. Finally, if the second assertion in (v) is false then

$$|\mathbf{N}_A(T \cap G)\colon \mathbf{C}_A(T \cap G)| = 48f.$$

But then $A = G\mathbf{N}_A(T \cap G)$, so $\mathbf{N}_A(T \cap G)$ induces a noncommutative group of automorphisms on the cyclic group $T \cap G$. This is a contradiction. □

THEOREM 3.4. *Suppose $G \neq A_6$ is an alternating or sporadic group. Let $A = \mathrm{Aut}(G)$. Then G contains a nonrational element y such that $\mathbf{C}_A(y) = \langle y\rangle$ and $A = G\mathbf{N}_A(\langle y\rangle)$.*

Proof. Suppose G is a sporadic group. If $G \neq J_2$ or Mc, let y be an element of prime order p for p the largest prime divisor of $|G|$. For $G = J_2$ or Mc, let $|\langle y\rangle| = 15, 14$, respectively. The result follows from [6].

Suppose $G = A_n$. If $n = 5$ let y have order 5. Assume $n \geq 7$. Suppose x is an l-cycle for $l \equiv 3 \pmod 4$. Then x is inverted by the product of $\frac{1}{2}(l-1)$ disjoint transpositions, an odd permutation. If n or $n-1$ is such a number l, then $\mathbf{C}_{\Sigma_n}(x) = \langle x\rangle$, so x is not inverted in A_n.

If $n = 2k + 1$ with k even, set $l_1 = k - 1$ and $l_2 = k + 1$. Then l_1 and l_2 are odd, $(l_1, l_2) = 1$, and one of these numbers is congruent to $3 \pmod 4$. Set $y = y_1 y_2$, where y_1, y_2 are disjoint cycles of lenghs l_1, l_2, respectively. Then $\langle y\rangle$ is self-centralizing in Σ_n and is normalized by an odd permutation, inverting one of y_1 and y_2, centralizing the other. Finally assume $n = 2k$ with k odd. Here we set

$$(l_1, l_2) = (k-2, k+2) \quad \text{or } (k-4, k+4),$$

according to whether $k \equiv 1$ or $3 \pmod 4$. Then use $y = y_1 y_2$ as above. ■

4. Some properties of characters

If G is a finite group let $\mathrm{Aut}(G)$ denote the group of all automorphisms of G, and let $\mathrm{Inn}(G)$ denote the group of all inner automorphisms of G. Thus $\mathrm{Inn}(G) \triangleleft \mathrm{Aut}(G)$.

If the center of G has order 1 then $G \approx \mathrm{Inn}(G)$. We will frequently identify G with $\mathrm{Inn}(G)$. Thus $G \triangleleft \mathrm{Aut}(G)$.

LEMMA 4.1. *Let G be a noncyclic simple group which is a composition factor of H. Then there exists a group A_0 with $G \subseteq A_0 \subseteq \mathrm{Aut}(G)$ such that if χ is a faithful irreducible character of A_0 then $\mathbf{Q}(\chi) \subseteq \mathbf{Q}(H)$.*

Proof. Induction on $|H|/|G|$. If $H = G$, the result is clear with $A_0 = G$. If $\langle 1 \rangle \neq K \triangleleft H$ and G is a composition factor of H/K, the result follows by induction as $\mathbf{Q}(H/K) \subseteq \mathbf{Q}(H)$. Suppose that no such K exists. Then H has a unique minimal normal subgroup $K = G_1 \times \cdots \times G_s$ with $G_i \approx G$ for $1 \leq i \leq s$.

The group H acts as a transitive permutation group on the set $\{G_i | 1 \leq i \leq s\}$ by conjugation. Let H_i be the stabilizer of G_i. Thus $H_i = \mathbf{N}_H(G_i)$. Furthermore $\prod_{j \neq i} G_j \triangleleft H_i$.

Let $A_1 = H_1/\mathbf{C}_H(G_1)$. Then $A_1 \approx A_0$ with $G \subseteq A_0 \subseteq \mathrm{Aut}(G)$. Let χ be a faithful irreducible character of A_1. Hence χ is a character of H_1 with $\mathbf{C}_H(G_1)$ in its kernel. In particular, G_i is in the kernel of χ for $i \neq 1$. Let $\zeta = \chi^H$. Then $\mathbf{Q}(\zeta) \subseteq \mathbf{Q}(\chi)$. It suffices to show that $\mathbf{Q}(\chi) = \mathbf{Q}(\zeta)$, because in that case $\mathbf{Q}(\chi) \subseteq \mathbf{Q}(H)$.

The definition of H_1 implies that $\zeta_K = \chi_K + \theta$, where θ is a sum of irreducible characters of K which have G_1 in their kernel. Thus χ is the unique irreducible constituent of ζ_{H_1} which does not have G_1 in its kernel. If $\alpha \in \mathrm{Gal}(\mathbf{Q}(\chi)/\mathbf{Q}(\zeta))$ then χ^α is an irreducible constituent of $\zeta_{H_1}^\alpha = \zeta_{H_1}$. As G_1 is not in the kernel of χ^α, this implies that $\chi^\alpha = \chi$. Thus $\mathbf{Q}(\chi) = \mathbf{Q}(\zeta)$ as required. □

LEMMA 4.2. *Let G be a noncyclic simple group which is a composition factor of a group H with $[\mathbf{Q}(H)\colon \mathbf{Q}] \leq m$. Let $x \in G \triangleleft A = \mathrm{Aut}(G)$. Then*

$$|\mathbf{N}_A(\langle x \rangle)\colon \mathbf{C}_A(x)| \geq \frac{\varphi(|\langle x \rangle|)}{m}.$$

Proof. Let A_0 be defined as in Lemma 4.1. Let λ be a faithful linear character of $\langle x \rangle$. Then λ^{A_0} is a sum of irreducible faithful characters of A_0 and so $\mathbf{Q}(\lambda^{A_0}) \subseteq \mathbf{Q}(H)$ by Lemma 4.1. As $\mathbf{Q}(\lambda^A) \subseteq \mathbf{Q}(\lambda^{A_0})$ this implies that $[\mathbf{Q}(\lambda^A)\colon \mathbf{Q}] \leq m$. Therefore

$$m \geq [\mathbf{Q}(\lambda^A(x))\colon \mathbf{Q}] = \frac{\varphi(|\langle x \rangle|)}{|\mathbf{N}_A(\langle x \rangle)\colon \mathbf{C}_A(x)|}. \qquad \square$$

LEMMA 4.3. *Let $G \lhd H$ with $|H\colon G| = 3$ and G a noncyclic simple group. Let $\chi \neq 1$ be an irreducible character of G such that $\chi^x = \chi$ for $x \in H$. Then H has a faithful irreducible character which is not rational valued.*

Proof. Since H/G is cyclic, there exists a character ζ of H with $\zeta_G = \chi$. If ζ vanishes on $H - G$ then

$$\frac{1}{|H|} \sum_{y \in H} |\zeta(y)|^2 = \frac{1}{3}$$

which is impossible. Hence there exists $x \in H - G$ with $\zeta(x) \neq 0$. Let λ be a faithful linear character of H/G. Then $\lambda(x)$ is a primitive cube root of unity. Hence, either $\zeta(x)$ or $\zeta(x)\lambda(x)$ is irrational. Thus either ζ or $\zeta\lambda$ is irrational. □

LEMMA 4.4. *Let G be a noncyclic simple group. Let $G \lhd H \subseteq$ Aut(G). Suppose that G has a cyclic S_p-group P for some prime p such that $p \nmid |H\colon G|$ and $1 < e = |\mathbf{N}_G(P)\colon \mathbf{C}_G(P)| < p - 1$. Let χ be an exceptional character in the principal p-block $B = B(p)$ of G. Assume that one of the following holds.*

(i) *e is odd and* $\chi(1) \equiv -e \pmod p$.

(ii) *e is even and* $\chi(1) \equiv e \pmod p$.

Then H has a faithful irreducible character which is not rational valued.

Proof. Suppose that every faithful irreducible character of H is rational valued.

Let $G_0 = G\mathbf{C}_H(P)$. Thus $G_0 \lhd H = G\mathbf{N}_H(P)$. Let B_0, B' be the principal p-block of G_0, H respectively. Let $e' = |\mathbf{N}_H(P)\colon \mathbf{C}_H(P)|$. Then

$$e = |\mathbf{N}_{G_0}(P)\colon \mathbf{C}_{G_0}(P)| \quad \text{and} \quad |H\colon G_0| = e'/e.$$

Let τ, τ' be the Brauer tree of B, B' respectively. Then τ is also the Brauer tree of B_0. See [9], Lemma 4.1. If $e' < p - 1$ then an exceptional character in B' is irrational and faithful (since its values are in the field of $|P|$th roots of unity). Thus $p - 1 = e' > e$.

By Lemma 4.1 of [9], τ is similar to τ' in the sense of [9]. Since τ', τ has e', e edges respectively and $|H\colon G_0| = e'/e$ it follows that every nonexceptional character in B_0 extends to a non-exceptional character in B'. Hence every nonexceptional character in B is rational valued and so τ is an open polygon with e edges. Let V_0 be the vertex of τ corresponding to the principal character and let V be the exceptional vertex of τ. As either (i) or (ii) holds, V cannot be an endpoint of τ. Thus $\tau = \tau_1 \cup \tau_2$, where V is an endpoint of τ_i and τ_i has $e_i > 0$ edges for $i = 1$ and 2. Thus, $e = e_1 + e_2$. Choose the notation so that $e_1 \leq e_2$.

By [9], Lemma 4.3 there exists a vertex V' of τ' such that τ' is the union of open polygons τ_{ij} for $i = 1, 2, 1 \leq j \leq e'/e$, where V' is an endpoint of each τ_{ij} and τ_{ij} has e_i edges. Thus the real stem of τ' has at most $2e_2$ edges. Since B' contains e'/e nonfaithful irreducible characters, we get

$$2e_2 + e'/e - 1 \geq e' = p - 1.$$

Hence,

$$2e - 2 + \frac{p-1}{e} - 1 \geq p - 1.$$

Therefore

$$2e \geq \frac{(p-1)(e-1)}{e} + 3 > \frac{(p-1)}{2}. \tag{4.1}$$

Hence $4e > p - 1$ and so $p - 1 = 2e$ or $3e$. In neither of these cases is (4.1) satisfied. □

5. Theorem A

Proof of Theorem A. Since there are only finitely many sporadic simple groups, it suffices to show that there are only a finite number of simple groups of Lie type which are composition factors of groups H with $[\mathbf{Q}(H)\colon \mathbf{Q}] \leq m$.

Let $G = G_n(p^f)$ be a simple group of Lie type of rank n over $\mathbf{F}_{p^f}$. Let T be the torus defined in Table III and let $T_0 = T \cap G$. Let $A = \operatorname{Aut}(G)$. By Theorem 3.1 and Table III there exists a constant C so that

$$|\mathbf{N}_A(T_0) \colon \mathbf{C}_A(T_0)| < Cfn.$$

By Lemmas 2.4 and 4.2,

$$Cfn \geq \varphi(|T_0|)/m \geq \tfrac{1}{2}\sqrt{|T_0|}/m. \tag{5.1}$$

It is clear from Table III and the inequality $|T\colon T_0| \leq \min\{n+1, p^f+1\}$, that (5.1) can hold for only finitely many values of p, f, and n. □

6. A technical lemma

LEMMA 6.1. *Let $q = p^f$ with p a prime. Let $G = G_n(q)$ be a simple group of Lie type over $\mathbf{F}_q$ of rank n distinct from ${}^2F_4(2)'$. Assume that G is not isomorphic to an alternating group or to one of the groups $PSp_4(3)$, $Sp_6(2)$, $O_8^+(2)'$, $PSL_3(4)$ or $PSU_4(3)$. Let T, d, e, f, g be defined as in Section 3. In the last three lines of*

Table III choose T so that the positive square root is taken in the fifth column. Assume that

$$efg \geq \varphi\left(\frac{|T|}{d}\right),$$

$$24f \geq \varphi\left(\frac{|T|}{d}\right) \quad \text{if } G = D_4(q). \tag{6.1}$$

Then G is isomorphic to one of the following groups:

(i) $PSL_2(7)$, $PSL_2(11)$, $PSU_3(3)$, $G_2(3)$, $G_2(4)$, $O_7(3)'$, $PSp_6(3)$, $F_4(2)$;
(ii) $PSL_2(8)$, $Sz(8)$, $PSU_5(2)$, ${}^3D_4(2)$;
(iii) $PSL_2(27)$, $PSU_3(4)$, $PSU_3(5)$, $Sp_4(4)$, $PSU_3(8)$, $PSU_6(2)$, $PO_8^+(3)'$; ${}^2E_6(2)$;
(iv) $PSL_4(3)$.

Proof. Each case in Tables I and II will be considered separately.

$G = A_1(p^f)$. By (6.1),

$$2f \geq \varphi\left(\frac{p^f+1}{d}\right). \tag{6.2}$$

Thus Lemma 2.3 implies that there are no large Zsigmondy primes for $(p, 2f)$. Hence one of the cases listed in Theorem 2.1(i)–(iv) must occur.

Suppose that $f = 1$. By (6.2), $2 \geq \varphi((p+1)/d)$. Hence $(p+1)/d = 2$, 3, 4 or 6. Thus $p + 1 \leq 6d \leq 12$ and so $p \leq 11$. $A_1(2)$ and $A_1(3)$ are solvable and $A_1(5) = A_5$. Hence $q = 7$ or 11. Now suppose $f \neq 1$.

If $p = 2$ then $f = 2$, 3, 5, 6 or 9. Hence (6.2) implies that $f = 2$ or 3. $A_1(4) \approx A_5$. Thus $G = A_1(8)$.

If $p = 3$ then $f = 2$ or 3. Since $A_1(9) \approx A_6$ this yields $G = A_1(27)$.

If $(p, 2f) = (5, 6)$ then (6.2) is not satisfied.

$G = A_n(p^f)$ *with* $n \geq 2$. By (6.1),

$$2(n+1)f \geq \varphi\left(\frac{p^{(n+1)f}-1}{(p^f-1)d}\right). \tag{6.3}$$

Suppose there is a large Zsigmondy prime for $(p, (n+1)f)$. By Lemma 2.3,

$$r\{2(n+1)f+1\} = \frac{p^{(n+1)f}-1}{(p^f-1)d} \tag{6.4}$$

where $r = 1$ or 2, and $p \neq 2$ if $r = 2$. Thus

(6.5)
$$r\{2(n+1)f+1\} \geq \frac{p^{(n+1)f}-1}{(p^f-1)^2} > \frac{p^{nf}+p^{(n-1)f}}{(p^f+1)} \geq p^{(n-1)f} \geq 2^{(n-1)f}.$$

Therefore $n \leq 4$ and $n \leq 3$ if $r = 2$.

Suppose $r = 2$. If $n = 3$ then (6.5) implies $f = 1$ and $p = 3$, contrary to (6.4). If $n = 2$, then the right side of (6.4) is odd, again a contradiction. Now suppose $r = 1$.

If $n = 4$, (6.5) implies that $10f + 1 > p^{3f} \geq 2^{3f}$ and so $f = 1$. Thus $11 > p^3$ and $p = 2$. This contradicts (6.4).

If $n = 3$, (6.5) implies that $8f + 1 > p^{2f} \geq 2^{2f}$ and so $f \neq 2$. Thus $17 > p^4$ or $9 > p^2$ and so $p = 2$ in either case. This contradicts (6.4).

If $n = 2$, (6.5) implies that $6f > p^f \geq 2^f$. Thus $f = 1$, $p < 7$ or $f = 2$, $p \leq 3$ or, $f = 3$ or 4 and $p = 2$. Thus (6.4) implies that $p^f = 2$ and $G = A_2(2) \approx PSL_2(7)$.

Thus it may be assumed that there is no large Zsigmondy prime for $(p, (n+1)f)$. By Theorem 2.1 one of the following must occur:

$$\begin{aligned} &p = 2, \quad (n+1)f = 4, 6, 10, 12 \text{ or } 18;\\ &p = 3, \quad (n+1)f = 4 \text{ or } 6;\\ &p = 5, \quad (n+1)f = 6. \end{aligned}$$

Now (6.3) implies that the only possibilities are $n = 3$, $p^f = 2, 3$ or $n = 2$, $p^f = 4$. Since $A_3(2) \approx A_8$ it follows that $G = A_3(3)$ or $A_2(4)$.

$G = {}^2A_n(p^f)$ *with* $n \geq 2$. By (6.1),

(6.6)
$$2(n+1)f \geq \varphi\left[\frac{p^{(n+1)f}+(-1)^n}{(p^f+1)d}\right].$$

Suppose first that n is even. By Lemma 2.3 there is no large Zsigmondy prime for $(p, 2(n+1)f)$. As $2(n+1)f \geq 6$, Theorem 2.1 implies that one of the following must occur:

$$\begin{aligned} &p = 2, \quad (n+1)f = 3, 5, 6 \text{ or } 9;\\ &p = 3, \quad (n+1)f = 3;\\ &p = 5, \quad (n+1)f = 3. \end{aligned}$$

The group ${}^2A_2(2)$ is solvable. The remaining groups which satisfy (6.6) are ${}^2A_4(2)$ and ${}^2A_2(q)$ with $q = 3, 4, 5$ or 8.

Suppose that n is odd. Hence $n \geq 3$. If there exists a large Zsigmondy prime for $(p, (n+1)f)$ then (6.6) and Lemma 2.3 imply that

$$(6.7) \qquad rl = r(2(n+1)+1) = (p^{(n+1)f} - 1)/(p^f + 1)d,$$

where l is a prime, $r = 1$ or 2, and if $r = 2$, then p is odd. Set $n + 1 = 2m$ and $y = mf$. Then

$$rl = (p^{mf} - 1)(p^{mf} + 1)/(p^f + 1)d.$$

Hence

$$(6.8) \quad p^{mf} - 1 \leq rd(p^f + 1) = r(2m, p^f + 1)(p^f + 1) \leq r(p^f + 1)^2.$$

The inequality

$$p^{mf} - 1 \leq r(p^f + 1)^2$$

is impossible for $m \geq 4$. For $m = 3$, $p^{3f} - 1 \leq r6(p^f + 1)$ implies $p^f \leq 3$. If $p^f = 2$, then $G = PSU_6(2)$ and if $p^f = 3$, (6.7) fails to hold. Suppose $m = 2$. Then $p^{2f} - 1 \leq 2(4, p^f + 1)(p^f + 1)$, and so $p^f \leq 9$. The cases $p^f = 2, 3$ are out by hypothesis and none of the remaining cases satisfy (6.7).

Thus it may be assumed that there is no large Zsigmondy prime for $(p, (n+1)f)$. Theorem 2.1 implies that one of the following must occur:

$$p = 2, \quad (n+1)f = 4, 6, 10, 12 \text{ or } 18.$$
$$p = 3, \quad (n+1)f = 4 \text{ or } 6.$$
$$p = 5, \quad (n+1)f = 6.$$

The only cases where (6.6) is satisfied are $G = {}^2A_3(2) \approx PSp_4(3)$, ${}^2A_3(3)$ or ${}^2A_5(2)$.

$G = B_n(p^f)$ or $C_n(p^f)$ with $n \geq 3$. By (6.1),

$$(6.9) \qquad 2nf \geq \varphi\left[\frac{p^{nf} + 1}{d}\right].$$

By Lemma 2.3 there is no large Zsigmondy prime for $(p, 2nf)$. Hence Theorem 2.1 implies that one of the following must hold:

$$p = 2, \; nf = 3, 5, 6 \text{ or } 9;$$
$$p = 3 \text{ or } 5, \; nf = 3.$$

Thus (6.9) implies that $G = B_3(2) \approx C_3(2) \approx Sp_6(2)$, or $G \approx B_3(3)$ or $C_3(3)$.

$G = C_2(p^f)$ with $p \neq 2$. By (6.1),

$$4f \geq \varphi\left[\frac{p^{2f}+1}{2}\right].$$

By Lemma 2.3 there is no large Zsigmondy prime for $(p, 4f)$. By Theorem 2.1, $p = 3$ and $f = 1$. Hence $G = C_2(3) \approx Sp_4(3)$.

$G = C_2(2^f)$. By (6.1),

$$8f \geq \varphi(2^{2f}+1). \tag{6.10}$$

If there is a large Zsigmondy prime for $(2, 4f)$ then Lemma 2.3 implies that $8f + 1 = 2^{2f} + 1$. Hence $f = 2$ and so $G = C_2(4)$. If there is no large Zsigmondy prime for $(2, 4f)$ then $f = 1$ or 3 by Theorem 2.1. By (6.10), $f \neq 3$. Hence $G = C_2(2)$ and so $G' \approx A_6$.

$G = D_n(p^f)$ with $n \geq 5$. By (6.1),

$$4nf \geq (2, n)2nf \geq \varphi\left[\frac{p^{nf}-1}{d}\right]. \tag{6.11}$$

By Lemma 2.4 one of the following holds:

$$4nf \geq \frac{1}{2}\sqrt{\frac{p^{nf}-1}{d}} \geq \frac{1}{4}\sqrt{p^{nf}-1}, \quad p \neq 2;$$
$$4nf \geq \sqrt{2^{nf}-1}, \quad p = 2.$$

Thus either

$$256n^2f^2 \geq p^{nf} - 1 \geq 3^{nf} - 1, \quad p \neq 2,$$

or

$$16n^2f^2 \geq 2^{nf} - 1, \quad p = 2.$$

Therefore one of the following occurs:

$$p = 2, \quad nf \leq 10;$$
$$p = 3, \quad nf \leq 9;$$
$$p = 5, \quad nf = 5.$$

None of these satisfy (6.11).

$G = D_4(p^f)$. By (6.1),

$$24f \geq \varphi\left[\frac{p^{4f}-1}{d}\right]. \tag{6.12}$$

By Lemma 2.4 one of the following holds

$$24f \geq \frac{1}{2}\sqrt{\frac{p^{4f}-1}{d}} \geq \frac{1}{4}\sqrt{p^{4f}-1}, \quad p \neq 2;$$
$$24f \geq \sqrt{2^{4f}-1}, \quad p = 2.$$

Thus either

$$96^2 f^2 \geq p^{4f} - 1 \geq 3^{4f} - 1, \quad p \neq 2,$$

or

$$576 f^2 \geq 2^{4f} - 1, \quad p = 2.$$

Therefore one of the following must occur:

$$\begin{aligned} &p = 2, \quad f \leq 3;\\ &p = 3, \quad f \leq 2;\\ &p = 5 \text{ or } 7, \quad f = 1. \end{aligned}$$

Since (6.12) holds it follows that $G = D_4(p)$ with $p = 2$ or 3.

$G = {}^2D_n(p^f)$ with $n \geq 4$. By (6.1),

$$2nf \geq \varphi\left[\frac{p^{nf}+1}{d}\right]. \tag{6.13}$$

By Lemma 2.3 there is no large Zsigmondy prime for $(p, 2nf)$. Hence by Theorem 2.1, $p = 2$ and $nf = 5$, 6 or 9. In none of these cases is (6.13) satisfied.

$G = {}^3D_4(p^f)$. By (6.1),

$$12f \geq \varphi\left((p^{3f}-1)(p^f+1)\right). \tag{6.14}$$

Thus Lemma 2.4 implies that

$$12f \geq \tfrac{1}{2}\sqrt{(p^{3f}-1)(p^f+1)} \geq \tfrac{1}{2}\sqrt{p^{4f}} = \tfrac{1}{2}p^{2f}.$$

Therefore one of the following occurs:

$$p = 2, \qquad f \leq 3.$$
$$p .= 3, \qquad f = 1.$$

Thus $G = {}^3D_4(2)$ by (6.14).

$G = E_6(p^f)$. By (6.1),

$$24f \geq \varphi\left[\frac{\Phi_{12}(p^f)\Phi_3(p^f)}{d}\right].$$

For $p = 2$ and $f = 1$ this is impossible. If $p \neq 2$ or $f \neq 1$ then by Theorem 2.1 there is a large Zsigmondy prime for $(p, 12f)$. Hence Lemma 2.3 implies that

$$\frac{\Phi_{12}(p^f)\Phi_3(p^f)}{d} = l \quad \text{or} \quad 2l$$

with l a prime. Thus $\Phi_{12}(p^f) \leq 6$ or $\Phi_3(p^f) \leq 6$ which is not the case.

$G = {}^2E_6(p^f)$. By (6.1),

$$24f \geq \varphi\left[\frac{\Phi_{12}(p^f)\Phi_6(p^f)}{d}\right].$$

If $p = 2$ and $f = 1$ then $G = {}^2E_6(2)$. If $p \neq 2$ or $f \neq 1$ there is a large Zsigmondy prime for $(p, 12f)$ by Theorem 2.1. Hence Lemma 2.3 implies that

$$\frac{\Phi_{12}(p^f)\Phi_6(p^f)}{d} = l \quad \text{or} \quad 2l$$

with l a prime. Thus $\Phi_{12}(p^f) \leq 6$ or $\Phi_6(p^f) \leq 6$. This is not the case as $p^f > 2$.

$G = E_7(p^f)$. By (6.1),

$$24f \geq \varphi\left[\frac{\Phi_{12}(p^f)(p^{3f} + 1)}{d}\right].$$

If $p = 2$ and $f = 1$ this implies that $24 \geq \varphi(117)$ which is not the case. If $p \neq 2$ or $f \neq 1$ then there is a large Zsigmondy prime for $(p, 12f)$ by Theorem 2.1. Hence Lemma 2.3 implies that

$$\frac{\Phi_{12}(p^f)(p^{3f} + 1)}{d} = l \quad \text{or} \quad 2l$$

with l a prime. Thus $\Phi_{12}(p^f) \le 4$ or $p^{3f} + 1 \le 4$ which is not the case.

$G = E_8(p^f)$. By (6.1),

$$30f \ge \varphi\big(\Phi_{30}(p^f)\big). \tag{6.15}$$

By Theorem 2.1 there exists a large Zsigmondy prime for $(p, 30f)$. Hence (6.15) contradicts Lemma 2.3.

$G = F_4(p^f)$ *with p odd.* By (6.1),

$$8f \ge \varphi\big(p^{4f} + 1\big). \tag{6.16}$$

By Theorem 2.1 there exists a large Zsigmondy prime for $(p, 8f)$. Hence (6.16) contradicts Lemma 2.3.

$G = F_4(2^f)$. By (6.1), $16f \ge \varphi(2^{4f} + 1)$. By Theorem 2.1 there exists a large Zsigmondy prime for $(2, 8f)$. Hence Lemma 2.3 implies that $16f + 1 = 2^{4f} + 1$. Thus $f = 1$. Hence $G = F_4(2)$.

$G = G_2(p^f)$ *with* $p \neq 3$. By (6.1),

$$6f \ge \varphi\big(p^{2f} + p^f + 1\big). \tag{6.17}$$

If $(p, 3f)$ has a large Zsigmondy prime, Lemma 2.3 implies that

$$r(6f + 1) = p^{2f} + p^f + 1 \quad \text{for} \quad r = 1 \text{ or } 2.$$

This is impossible for $p^f \ge 4$. If $(p, 3f)$ has no large Zsigmondy prime then Theorem 2.1 implies $p = 2$ and $f = 2$, 4 or 6, or $p = 3$ or 5 and $f = 2$. Thus (6.17) implies that $G = G_2(4)$.

$G = G_2(3^f)$. By (6.1),

$$12f \ge \varphi\big(3^{2f} + 3^f + 1\big). \tag{6.18}$$

Lemma 2.4 implies that $12f \ge \sqrt{3^{2f} + 3^f + 1}$. Hence $144f^2 \ge 9^f + 3^f + 1$. Thus $f \le 3$ and so $f = 1$ by (6.18) and $G = G_2(3)$.

$G = {}^2C_2(2^{2a+1})$ *with* $a \ge 1$. By (6.1),

$$4(2a + 1) \ge \varphi\big(2^{2a+1} + 2^{a+1} + 1\big). \tag{6.19}$$

By Lemma 2.4 this implies that

$$4(2a + 1) \ge \sqrt{2^{2a+1} + 2^{a+1} + 1} > 2^a\sqrt{2}.$$

Thus $a < 5$. Hence $a = 1$ by (6.19) and $G = {}^2C_2(2^3) = Sz(8)$.

$G = {}^2F_4(2^{2a+1})$ *with* $a \geq 1$. By (6.1),

$$12(2a+1) \geq \varphi(2^{4a+2} + 2^{3a+2} + 2^{2a+1} + 2^{a+1} + 1). \tag{6.20}$$

By Lemma 2.4 this implies that

$$12(2a+1) > \sqrt{2^{4a+2}} = 2^{2a+1}.$$

Hence $a < 3$. This contradicts (6.20).

$G = {}^2G_2(3^{2a+1})$ *with* $a \geq 1$. By (6.1),

$$6(2a+1) \geq \varphi(3^{2a+1} + 3^{a+1} + 1). \tag{6.21}$$

By Lemma 2.4 this implies that $6(2a+1) \geq \sqrt{3^{2a+1}} = 3^a\sqrt{3}$. Hence $a \leq 2$ which contradicts (6.21). □

7. Theorem B and its corollaries

LEMMA 7.1. *Let $G = PSL_3(4)$ and let x be the automorphism of G which is the product of the graph automorphism and the field automorphism. Let $H = G\langle x\rangle$. Then H is a rational group.*

Proof. See [6]. □

Let y be an element in $PU_4(3)$ which is the image of an element in $U_4(3)$ whose determinant is a primitive 4th root of unity in $\mathbf{F}_9$. Let z be the field automorphism of $PU_4(3)$. If $G = PSU_4(3)$ then $\mathrm{Aut}(G) = G\langle y, z\rangle$ and $\mathrm{Aut}(G)/G$ is dihedral of order 8.

Let $x_1 = y^2, x_2 = yz., \ x_3 = x_1x_2$. Let $H = G\langle x_1, x_2, x_3\rangle$. Then H/G is noncyclic of order 4. In the notation of [6], x_1 is of type 2_1, x_2 and x_3 are of type 2_3.

LEMMA 7.2. *Let $G = PSU_4(3)$. Let $H = G\langle x_1, x_2, x_3\rangle$, where x_i is defined above for $i = 1, 2, 3$. Then H is a rational group.*

Proof. If χ is an irreducible character of G let $T(\chi)$ denote the inertia group of χ in H.

It will suffice to show that for each irreducible character χ of G, the constituents of χ^H are rational. Set $G_i = G\langle x_i\rangle$ for $1 = 1, 2, 3$.

Assume χ is rational. If $T(\chi) = G$, then χ^H is irreducible and clearly rational (since χ^H vanishes of G). Suppose $G_i \subseteq T(\chi)$ and γ_i is any extension of χ to G_i. If γ_i is not H-invariant, then $\theta = \gamma_i^H$ is irreducible, $\chi^H = \theta + \omega\theta$ for ω a linear character of H/G. If $\omega = 1$, the assertion holds. Otherwise, $T(\chi) = G_i$, so by [6], γ_i is rational valued, as is θ. Again the assertion holds. Note that this case necessarily holds if $T(\chi) = G_i$. We may thus suppose that $T(\chi) = H$ and that each such γ_i is H-invariant for each i.

Fix i and let θ be any extension of γ_i to H. Then θ_{G_j} is an extension of χ for $j = 1, 2, 3$. If each θ_{G_i} is rational, then θ is rational, and as $\chi^G = \Sigma\omega_j\theta$, and ω_j runs over the linear characters of H/G, the result holds. Thus, we may assume some θ_{G_i} is not rational for some i. In the notation of [6] this only occurs for $\chi = \chi_{16}$ and here θ_{G_j} is not real for any j. For φ a character let $v(\varphi)$ denote the Frobenius-Schur indicator of φ. Thus

$$v(\theta) = \tfrac{1}{2}\big(v(\theta_{G_1}) + v(\theta_{G_2}) + v(\theta_{G_3}) - v(\chi)\big) = \tfrac{1}{2}(-v(\chi)) = \pm\tfrac{1}{2},$$

a contradiction.

Finally, assume χ is not rational. From [6] we conclude that $\chi = \chi_i$ for $9 \leq i \leq 12$ or $i = 17, 18$. In the former case $T(\chi) = G$, χ^H is irreducible, it vanishes off G, and $\chi^H_G = \chi_9 + \chi_{10} + \chi_{11} + \chi_{12}$ is rational.

Suppose $\chi = \chi_i$ with $i = 17$ or 18. Then χ extends to a character γ of G_1. Now γ is irrational only on 7-singular elements, but in H any two 7-singular elements of the same order are conjugate. □

Proof of Theorem B. Since Weyl groups are rational, Lemmas 7.1 and 7.2 imply that the groups listed in the statement are isomorphic to composition factors of rational groups.

Let G be a noncyclic simple group which is a composition factor of a rational group. Assume that G is not an alternating group and is not isomorphic to $PSp_4(3)$, $Sp_6(2)$, $O_8^+(2)'$, $PSL_3(4)$ or $PSU_4(3)$. We will derive a contradiction from the assumed existence of G.

If G is a group of Lie type other than ${}^2F_4(2)'$, then Theorem 3.1 and Lemma 4.2 imply that (6.1) is satisfied. Thus by lemma 6.1 it may be assumed that G is sporadic, $G \approx {}^2F_4(2)'$ or G is one of the groups listed in the conclusion of Lemma 6.1. In each of these cases it will be shown that if $G \subseteq H \subseteq \operatorname{Aut}(G)$ then H has a faithful irreducible irrational character. Thus by Lemma 4.1, G cannot be a composition factor of a rational group.

All explicit references to characters are in the notation of the ATLAS.

Suppose that G is sporadic, $G \approx {}^2F_4(2)'$ or G is one of the groups listed in Lemma 6.1(i). By [6], $|\operatorname{Aut}(G){:}\ G| \leq 2$ and both G and $\operatorname{Aut}(G)$ have a faithful irrational character.

Suppose that G is one of the groups listed in Lemma 6.1(ii). By inspection G has an irrational character. The Steinberg character is invariant under every automorphism of G. Thus Aut(G) has a faithful irrational irreducible character by Lemma 4.3.

Suppose that G is one of the groups listed in Lemma 6.1 (iii). In each case the hypotheses of Lemma 4.4 are satisfied for the following values. Thus G is not a composition factor of a rational group.

G	P	e	$\chi(1)$
$PSL_2(27)$	13	2	28
$PSU_3(4)$	13	3	75
$PSU_3(5)$	7	3	144
$Sp_4(4)$	17	4	225
$PSU_3(8)$	19	3	567
$PSU_6(2)$	11	5	25,515
$PSO_8^+(3)$	13	6	716,800
${}^2E_6(2)$	11	5	33,748,307,775

Suppose finally that $G = PSL_4(3)$. Let $\langle y \rangle = P$ be a S_{13}-group of G. Then

$$|\mathbf{N}_G(P) \colon \mathbf{C}_G(P)| = 3.$$

If y is a rational element of H, then $\mathbf{N}_H(P)/\mathbf{C}_H(P)$ is cyclic of order 12. Since $G \subseteq H \subseteq$ Aut(G) and Aut$(G)/G$ is noncyclic of order 4 this is impossible. Hence y is not rational in H and so H has an irrational character which is necessarily faithful. □

Proof of Corollary B.1. This is immediate from Theorem B, Theorem 3.4 and [6]. □

LEMMA 7.3. *Let G be a finite group in which any two elements of the same order are conjugate. Then every homomorphic image of G has the same property.*

Proof. Let $G^* = G/K$. Let $x^*, y^* \in G^*$ have the same order. Choose coset representatives x, y for x^*, y^* respectively of minimum order. If x and y have the same order then x is conjugate to y in G by assumption and so x^* is conjugate to y^*. Suppose x and y have distinct orders. Then there exists a prime p so that $|\langle x \rangle| = p^a m$, $|\langle y \rangle| = p^b n$ with $p \nmid mn$ and $a \neq b$, say $a < b$. Let $x_1 = x^{mn}$, $y_1 = y^{mn}$. Then x_1^* and y_1^* have the same order in G^*. Since x_1 and $y_1^{p^{b-a}}$ both have order p^a they are conjugate in G. Hence x_1^* and $y_1^{*p^{b-a}}$ are conjugate in G^*, contrary to the fact that x_1^* and $y_1^{*p^{b-a}}$ have different orders. □

Proof of Corollary B.2. Let G be a counter example of minimum order. Then G is a rational group. Let K be a minimal normal subgroup of G. By Lemma 7.3, $|G/K| = 1$ or 2 or $G/K \approx \Sigma_3$.

Suppose first that K is solvable. Then K is an elementary abelian p-group for some prime p. If $|G/K| = 1$ then $|K| = |G| = 2$. If $|G/K| = 2$ then $|K| \leq 3$. If $|K| = 3$ then $G \approx \Sigma_3$. If $|K| = 2$ then $|G| = 4$ which is impossible. Thus $G/K \approx \Sigma_3$ and the hypothesis implies that $|K| \leq 7$.

If $|K| = 5$ or 7 then $|G\colon \mathbf{C}_G(K)| \leq 2$ and so there are at least 2 conjugacy classes of elements of order $|K|$ in G. If $|K| = 4$. Then a S_3-group of G acts faithfully on K and so $G \approx \Sigma_4$ which is impossible as there are 2 conjugacy classes of involutions in Σ_4.

If $|K| = 3$ then a S_3-group Q has order 9 and $|G\colon Q| = 2$. This is impossible as there are either 8 elements of order 3 or 6 elements of order 9 in Q, and these cannot all be conjugate. If $|K| = 2$ then G has a homomorphic image of order 4. This has either 3 pairwise nonconjugate involutions or 2 nonconjugate elements of order 4 contrary to Lemma 7.3.

Suppose now that K is not solvable. Then $K = K_1 \times \cdots \times K_s$, where $K_i \approx K_1$ for $i = 1, \ldots, s$ is simple. An involution in K_1 cannot be conjugate in G to an involution in K which is not in some K_i. Thus $K = K_1$ is simple. If $G = K$ then K is a rational group and so $K \approx Sp_6(2)$ or $O_8^+(2)'$ by Corollary B.1. However, both of these groups have more than one class of involutions. Suppose that $|G\colon K| > 1$.

As $\mathbf{C}_G(K) \lhd G$ and $K\mathbf{C}_G(K) = K \times Z$ it follows that $Z \lhd G$. If $Z \neq 1$ then Lemma 7.3 and induction imply that G/Z is solvable. Thus $Z = 1$ and $\mathbf{C}_G(K) = \langle 1 \rangle$. Hence $G \subseteq \mathrm{Aut}(K)$.

Suppose that $K \approx A_n$ for some $n \geq 5$. Then either $G \approx \Sigma_n$ or $n = 6$, and $|G\colon A_6| = 2$. If $G \approx \Sigma_n$ then G has more than one class of involutions. If $n = 6$ then by inspection G has either 2 conjugacy classes of order 8 or more than one class of involutions.

$K \not\approx Sp_6(2)$ as $\mathrm{Aut}(Sp_6(2)) = Sp_6(2)$.

If $K \approx PSp_4(3)$, $O_8^+(2)'$, $PSL_3(4)$ or $PSU_4(3)$ then by [6], G has involutions in K and involutions not in K. These cannot be conjugate. □

8. Automorphisms of simple groups

Proof of Theorem C. Let G be a noncyclic simple group. Let α be an outer automorphism of G which fixes every conjugacy class of G. We will reach a contradiction from the assumed existence of α.

By [6], $G \neq A_6$, $PSU_4(2)$, ${}^2F_4(2)'$ or a sporadic group.

If $G = A_n$ for $n \geq 5, n \neq 6$, then $\alpha \in \mathrm{Aut}(G) = \Sigma_n$. However, Σ_n is a rational group, while A_n is not, by Corollary B.1.

Suppose that G is a group of Lie type other than $PSU_4(2)$, or ${}^2F_4(2)'$. Let T be as in Theorem 3.1 and let $\langle y \rangle = T \cap G$. Assume first that $G \neq D_4(q)$. Since α fixes the conjugacy class which contains y it follows that $\mathbf{C}_A(y)$ contains an element of the coset $G\alpha$. Thus $\alpha \in G_1$ by Theorem 3.1.

Suppose that $G = D_4(q) = PO_8^+(q)'$. Choose $x \in G$ so that x is unipotent and if V is the underlying vector space for $O_8^+(q)$, then $[V, x]$ is a totally isotropic 4 dimensional space (x is the product of elements from two commuting root subgroups.) Then $\mathbf{C}_G(x)$ is contained in a unique maximal parabolic subgroup P (with Weyl group of type A_3). For $p = 2$ see [1], for $p \neq 2$ see [16], Theorem A. However P^A consists of three G_2 orbits, where G_2 is the group generated by G_1 and all field automorphisms, such that $A/G_2 \approx \Sigma_3$ acts faithfully on these orbits. Hence, if $\alpha \in A - G_2$ then α must move the class which contains x^β for some $\beta \in A$. Thus $\alpha \in G_2$. Since α does not move the class containing y, $\mathbf{C}_{G_2}(y)$ contains an element of the coset $G\alpha$. Thus $\alpha \in G_1$ by Theorem 3.1 in this case also.

Let u be a regular unipotent element of G. Then $\mathbf{C}_{G_1}(u)$ is a unipotent group. See [18]. Hence $\mathbf{C}_{G_1}(u) = \mathbf{C}_G(u)$ and so $\mathbf{C}_{G_1}(u)$ contains no element of $G\alpha$. Thus α does not fix the class containing u. □

9. Automorphism of group algebras

If χ is an irreducible character of G let $m(\chi)$ denote the Schur index of χ. If m is a natural number let $\mathbf{Q}_m$ denote the field generated by a primitive mth root of 1. By [2], Theorem 1′, $\mathbf{Q}_{m(\chi)} \subseteq \mathbf{Q}(\chi)$.

For the following result see [12], Corollary 1.

THEOREM 9.1. *Let $\sigma \in \mathrm{Gal}(\mathbf{Q}(\chi)/\mathbf{Q})$. Let M be the simple component of the group algebra $\mathbf{Q}[G]$ corresponding to χ. Thus $\mathbf{Q}(\chi)$ is the center of M. Furthermore, the following are equivalent.*

(i) *σ extends to an automorphism of M.*

(ii) *$\mathbf{Q}_{m(\chi)}$ is in the fixed field of σ.*

In particular, if $m(\chi) \leq 2$ then σ extends to an automorphism of M.

In this paper we will only need the case $m(\chi) \leq 2$.

COROLLARY 9.2. *If G has an irrational irreducible character with Schur index at most 2, then $\mathbf{Q}[G]$ has an outer automorphism.*

Proof. Clear by Theorem 9.1. □

COROLLARY 9.3. *Suppose that G has an irrational irreducible character χ such that ± 1 are the only roots of unity in $\mathbf{Q}(\chi)$. Then $\mathbf{Q}[G]$ has an outer automorphism.*

Proof. By Theorem 1′ of [2], the Schur index of χ is at most 2. The result follows from Corollary 9.2. □

COROLLARY 9.4. *Suppose that G is a noncyclic simple group which has a cyclic S_p-group $P \neq \langle 1 \rangle$ for some prime p and that*

$$e = |\mathbf{N}_G(P) : \mathbf{C}_G(P)| < p - 1.$$

Then $\mathbf{Q}[G]$ *has an outer automorphism.*

Proof. Since G is simple $e > 1$. Let χ be an exceptional character in the principle p-block. Thus $\mathbf{Q} \neq \mathbf{Q}(\chi) \subseteq F$ where F is the field of $|P|$th roots of unity. Furthermore, $\mathbf{Q}(\chi)$ does not contain a primitive Pth root of 1 as $e > 1$. Thus ± 1 are the only roots of unity in $\mathbf{Q}(\chi)$. The result follows from Corollary 9.3. □

Proof of Theorem D. If $K \lhd G$ then $\mathbf{Q}[G/K]$ is a direct summand of $\mathbf{Q}[G]$. Thus it suffices to prove the result for G simple.

Suppose that $|G| = p$ is a prime. If $p = 2$ then $\mathbf{Q}[G] \approx \mathbf{Q} \oplus \mathbf{Q}$ and there is an automorphism which exchanges the factors. If $p > 2$ then $\mathbf{Q}[G] \approx \mathbf{Q} \oplus F$, where F is the field of pth roots of 1. This has an automorphism, which is necessarily outer.

Thus it may be assumed that G is a noncyclic simple group. If G has an outer automorphism then this induces an automorphism on $\mathbf{Q}[G]$. By Theorem C it does not fix the center and so is not inner. Thus it may be assumed that $G = \mathrm{Aut}(G)$. Hence G is isomorphic to one of the following groups:

(9.1) A sporadic group;
(9.2) $E_7(2)$;
(9.3) $E_8(p)$;
(9.4) $F_4(p)$, $p \neq 2$;
(9.5) $Sp_{2n}(2)$;
(9.6) $G_2(p)$, $p > 3$.

If G is a sporadic group it is known that all Schur indices are at most 2; see [8]. By Corollary B.1, G has an irrational character. Thus $\mathbf{Q}[G]$ has an outer automorphism by Corollary 9.2. Alternatively, it may be observed that every sporadic group except J_2 satisfies the hypotheses of Corollary 9.4 for some prime, while J_2 has an outer automorphism.

If $G = E_7(2)$ then G has a S_{127}-group R of order 127. Since G has a faithful representation of degree 56 over $\mathbf{F}_2$ it follows that

$$|\mathbf{N}_G(R) : \mathbf{C}_G(R)| < 126.$$

By Corollary 9.4, $\mathbf{Q}[G]$ has an outer automorphism.

If G is one of the groups in (9.3)–(9.6) let T be the torus defined in Section 3. In each of the following cases let r be a large Zsigmondy prime for (p, m):

$$\begin{array}{lll} G = E_8(p), & m = 30; & \\ G = F_4(p), & m = 8, & p \neq 2; \\ G = Sp_{2n}(2), & p = 2, & m = 2n > 4; \\ G = G_2(p), & p > 3, & m = 6; \end{array}$$

Let R be a S_r-group of T. Then R is cyclic and R is a S_r-group of G. Furthermore, $|\mathbf{N}_G(R)\colon \mathbf{C}_G(R)| = |\mathbf{N}_G(T)\colon \mathbf{C}_G(T)| < r$. Thus $\mathbf{Q}[G]$ has an outer automorphism by Corollary 9.4.

By Theorem 2.1 such a large Zsigmondy prime exists except if $G = Sp_{2n}(2)$ and $m = 6$, 10, 12 or 18. In these cases define a prime r as follows:

If $m = 18$, $r = 257$.

If $m = 10$ or 12, $r = 17$.

Then a S_r-group R of G has order r and $|\mathbf{N}_G(R)\colon \mathbf{C}_G(R)| < r - 1$ as G has a faithful m dimensional representation over $\mathbf{F}_2$.

If $G = Sp_6(2)$ then all Schur indices are 1 by a Theorem of Benard. For example, see [8]. By [6], G has two irreducible rational characters of degree 21, and so $\mathbf{Q}[G]$ has two isomorphic simple components. Thus, there is an outer automorphism of $\mathbf{Q}[G]$ which interchanges these. □

References

1. M. Aschbacher and G. Seitz, *Involutions in Chevalley groups over fields of even order*, Nagoya Math. J., vol. 63 (1976), pp. 1–91.
2. M. Benard and M.M. Schacher, *The Schur subgroup II*, J. Algebra, vol. 22 (1972), pp. 378–385.
3. A. Borel and J. Tits, *Elements unipotents et sousgroupes paraboliques de groupes reductifs, I*, Invent. Math., vol. 12 (1971), pp. 95–104.
4. R. Carter, *Conjugacy classes in the Weyl group*, Compositio Math., vol. 25 (1972), pp. 1–59.
5. ______, *Simple groups of Lie type*, Wiley, New York, 1972.
6. J.H. Conway, R.T. Curtis, S.P. Norton, R.A. Parker and R.A. Wilson, *Atlas of finite groups*, Clarendon Press, Oxford, 1986.
7. E. Farias e Soares, *Big primes and character values for solvable groups*, J. Algebra, vol. 100 (1986), pp. 305–324.
8. W. Feit, *The computations of some Schur indices*, Israel J. Math., vol. 46 (1983), pp. 274–300.
9. ______, *Possible Brauer trees*, Illinois J. Math., vol. 28 (1984), pp. 43–56.
10. ______, *On large Zsigmondy primes*, Proc. Amer. Math. Soc., vol. 102 (1988), pp. 29–36.
11. R. Gow, *Groups whose characters are rational valued*, J. Algebra, vol. 40 (1976), pp. 280–299.
12. G. Janusz, *Automorphisms of simple algebras and group algebras*, Proc. Philadelphia Conference, Dekker Lecture Notes, no. 37 (1976), pp. 381–388.
13. The Kourovka Notebook, Amer. Math. Soc. Translations, Series 2, vol. 121.
14. G. Seitz, *On the subgroup structure of classical groups*, Comm. Algebra, vol. 10 (1982), pp. 875–885.
15. ______, *The root subgroups for maximal tori in finite groups of Lie type*, Pacific J. Math., vol. 106 (1983), pp. 153–244.

16. ______, *Parabolic subgroups containing the centralizer of a unipotent element*, J. Algebra, vol. 84 (1983), pp. 240–252.

17. T. Springer and R. Steinberg, *Conjugacy classes*, Springer Lecture Notes 131, Springer-Verlag, New York, 1970.

18. R. Steinberg, *Regular elements of semi-simple algebraic groups*, Publications I.H.E.S., France, no. 25 (1965), pp. 281–312.

Yale University
New Haven, Connecticut
University of Oregon
Eugene, Oregon