PRODUCTS OF CONJUGACY CLASSES IN FINITE AND ALGEBRAIC SIMPLE GROUPS

ROBERT GURALNICK, GUNTER MALLE, AND PHAM HUU TIEP

Dedicated to Robert Steinberg on the occasion of his 90th birthday

Abstract. We prove the Arad–Herzog conjecture for various families of finite simple groups — if A and B are nontrivial conjugacy classes, then AB is not a conjugacy class. We also prove that if G is a finite simple group of Lie type and A and B are nontrivial conjugacy classes, either both semisimple or both unipotent, then AB is not a conjugacy class. We also prove a strong version of the Arad–Herzog conjecture for simple algebraic groups and in particular show that almost always the product of two conjugacy classes in a simple algebraic group consists of infinitely many conjugacy classes. As a consequence we obtain a complete classification of pairs of centralizers in a simple algebraic group which have dense product. A special case of this has been used by Prasad to prove a uniqueness result for Tits systems in pseudo-reductive groups. Our final result is a generalization of the Baer-Suzuki theorem for p-elements with $p \geq 5$.

1. Introduction

In [2, p. 3], Arad and Herzog made the following conjecture:

Conjecture A (Arad–Herzog)**.** *If S is a finite non-abelian simple group and A and B are nontrivial conjugacy classes of S, then AB is not a conjugacy class.*

In this paper, we prove this conjecture in various cases. We also consider the analogous problem for simple algebraic groups. Note that the results do not depend on the isogeny class of the group (allowing the possibility of multiplying a class by a central element) and so we work with whatever form is more convenient. Moreover, in characteristic 2, we ignore the groups of type B (the result can be read off from the groups of type C).

Here one can prove much more:

Theorem 1.1. *Let $\mathbf{G}$ be a simple algebraic group over an algebraically closed field of characteristic $p \geq 0$. Let A and B be non-central conjugacy classes of $\mathbf{G}$. Then AB can never constitute a single conjugacy class. In fact, either AB is the union of infinitely many conjugacy classes, or (up to interchanging A and B and up to an isogeny for $\mathbf{G}$) one of the following holds:*

Date: October 29, 2012.

1991 *Mathematics Subject Classification.* Primary 20G15, 20G40, 20D06; Secondary 20C15, 20D05.

Key words and phrases. products of conjugacy classes, products of centralizers, algebraic groups, finite simple groups, Szep's conjecture, characters, Baer–Suzuki theorem.

The first and third authors were partially supported by the NSF (grants DMS-1001962, DMS-0901241, and DMS-1201374).

(1) $\mathbf{G} = G_2$, *A consists of long root elements and B consists of elements of order* 3. *If $p = 3$, B consists of short root elements and if $p \neq 3$, B consists of elements with centralizer isomorphic to* SL_3.
(2) $\mathbf{G} = F_4$, *A consists of long root elements and B consists of involutions. If $p = 2$, B consists of short root elements and if $p \neq 2$, B consists of involutions with centralizer isomorphic to B_4.*
(3) $\mathbf{G} = \mathrm{Sp}_{2n} = \mathrm{Sp}(V)$, *$n \geq 2$, $\pm A$ consists of long root elements and B consists of involutions; when $p = 2$ then the involutions $b \in B$ moreover satisfy $(bv, v) = 0$ for all $v \in V$.*
(4) $\mathbf{G} = \mathrm{SO}_{2n+1}$, *$n \geq 2$, $p \neq 2$, A consists of elements which are the negative of a reflection and B consists of unipotent elements with all Jordan blocks of size at most* 2.

The methods rely heavily on closure of unipotent classes. In particular, this gives a short proof for simple algebraic groups of what is referred to as Szep's conjecture for the finite simple groups (proved in [8]) — a finite simple group is not the product of two subgroups with nontrivial centers.

Corollary 1.2. *Let $\mathbf{G}$ be a simple algebraic group over an algebraically closed field of characteristic $p \geq 0$. Let a, b be non-central elements of $\mathbf{G}$. Then $\mathbf{G} \neq C_{\mathbf{G}}(a)C_{\mathbf{G}}(b)$.*

Indeed, we see that $C_{\mathbf{G}}(a)C_{\mathbf{G}}(b)$ is rarely dense in $\mathbf{G}$ (it only happens in the exceptional cases in Theorem 1.1) — see Corollary 5.13. In particular, we give a very short proof of:

Corollary 1.3. *If $\mathbf{G}$ is a simple algebraic group and x is a non-central element of G, then for any $g \in G$, $C_{\mathbf{G}}(x)gC_{\mathbf{G}}(x)$ is not dense in G. In particular, $|C_{\mathbf{G}}(x)\backslash\mathbf{G}/C_{\mathbf{G}}(x)|$ is infinite.*

This was proved independently for unipotent elements by Liebeck and Seitz [25, Chapter 1]. The previous result was used by Prasad [35, Thm. B] to show that any Tits system for a pseudo-reductive group satisfying some natural conditions is a standard Tits system (see [35] for more details).

Conjecture A is open only for the simple groups of Lie type, where it was known to be true for certain families (cf. [34]), but not for any family of arbitrary rank and field size. Our idea is to show that we can find a small set of irreducible characters Γ of S so that for any pair of nontrivial classes $A, B \subset S$ there is $\chi \in \Gamma$ which is not constant on AB (and so obviously AB is not a conjugacy class).

For $\mathfrak{A}_n$ and $\mathfrak{S}_n$, the conjecture was proved by Fisman and Arad [8, 3.1]; see also Adan-Bante and Verrill [1]. In Section 2 we give a very short proof of the slightly stronger result:

Theorem 1.4. *Let $H := \mathfrak{A}_n$ and $G := \mathfrak{S}_n$ with $n \geq 5$. For nontrivial elements $a, b \in G$, set $A := a^H$ and $B := b^H$. For $g \in G$, let $f(g)$ denote the number of fixed points of g in the natural permutation representation of G. Then f is not constant on AB.*

Similarly, we show:

Theorem 1.5. *Let $S = \mathrm{L}_d(q) = \mathrm{L}(V)$ be simple. Let $f(g)$ be the number of fixed one-spaces of $g \in S$ on V. If A and B are nontrivial conjugacy classes of S, then f is not constant on AB (in particular, AB is not a conjugacy class).*

As noted above this is the first family of groups of Lie type including both unbounded rank and field size for which the conjecture is now established.

For arbitrary groups of Lie type using Lemma 2.2, the fact that the Steinberg character is nonzero on semisimple elements only and the result that the product of centralizers of two non-central semisimple elements in a simple algebraic group is not dense (cf. Corollary 5.13), we can show:

Theorem 1.6. *Let G be a finite simple group of Lie type, and let* St *denote the Steinberg character of G. If $a, b \in G \setminus \{1\}$ are semisimple elements, then* St *is not constant on $a^G b^G$.*

This implies immediately:

Corollary 1.7. *Let G be a finite simple group of Lie type and $a, b, c \in G \setminus \{1\}$ such that $a^G b^G = c^G$. Then neither c is semisimple, nor are both a, b.*

Using Deligne–Lusztig theory, we can similarly show:

Theorem 1.8. *Let G be a finite simple group of Lie type and $a, b, c \in G \setminus \{1\}$ such that $a^G b^G = c^G$. Then c is not unipotent and so neither are both a and b.*

Recall that the Baer–Suzuki theorem states that if G is a finite group, p a prime and $x \in G$ is such that $\langle x, x^g \rangle$ is a p-group for all $g \in G$, then the normal closure of x in G is a p-group. One step in the proof of Theorem 1.8 is an analog of Theorem 1.1 for pairs of p-elements of finite groups. This leads to a generalization of the Baer–Suzuki theorem (for primes at least 5) by considering two possibly distinct conjugacy classes of p-elements.

Theorem 1.9. *Let G be a finite group, $p \geq 5$ prime, and let C and D be normal subsets of G with $H := \langle C \rangle = \langle D \rangle$. Suppose that for every pair $(c, d) \in C \times D$, $\langle c, d \rangle$ is a p-group. Then H is a p-group.*

The Baer–Suzuki theorem (for p-elements with $p \geq 5$) is the special case $C = D$. Example 7.3 shows that we cannot drop the assumption that $\langle C \rangle = \langle D \rangle$. The examples in Section 6 show that we must also require that $p \geq 5$.

See Theorems 8.4 and 8.8 for other variants.

This paper is organized as follows. In Section 2 we write down a variant of the character-theoretic condition for a product of conjugacy classes to be a conjugacy class in a finite group, and then use it to give short proofs of Conjecture A for $\mathfrak{A}_n$ and $\mathrm{L}_d(q)$. In Sections 3 and 4, we show that the conjecture holds for low rank classical and exceptional groups, and prove Theorems 1.6 and 1.8.

In Section 5, we consider algebraic groups and prove Theorem 1.1. We also establish Corollary 1.2, and classify in Corollary 5.13 the cases when products of centralizers in a simple algebraic group over an algebraically closed field are dense. We then discuss in Section 6 the special cases listed in Theorem 1.1 in detail. These two sections are essentially independent of the rest of the paper (only Corollary 5.13 is used to prove Theorem 1.6 for the finite groups of Lie type).

In the next section, we use our results on semisimple elements to give a relatively quick proof of Szep's conjecture and also provide some examples which show that the simplicity hypothesis in both Conjecture A and Szep's conjecture cannot be weakened much.

In the last section, we prove variants of Theorem 1.9.

In order to prove Conjecture A for the remaining open cases, one will have to work much harder. The short proofs for the alternating groups and linear groups used the fact that the groups had doubly transitive permutation representations (however, the proof does not work for all doubly transitive simple groups). There are a few other special cases where the existence of a special character makes the proofs relatively straightforward. The conjecture can be checked easily for the finite groups of Lie type of small rank using Chevie. In a sequel, employing more sophisticated tools from the representation theory of finite groups of Lie type, we hope to establish Conjecture A. We have proved the result for several families of classical groups – in particular the conjecture holds for symplectic groups (at this point the proof of this case is roughly 40 pages long). The methods here depend upon proving some new results about character values for these groups.

Remark 1.10. A dual problem to considering products of conjugacy classes would be to consider tensor products of irreducible representations. See [3, 4, 28, 29, 41] for some partial results.

Acknowledgements: It is a pleasure to thank Ross Lawther for writing his interesting paper [23] at our request and also for allowing us to include his result, Lemma 4.5. We also thank Tim Burness and Gopal Prasad for some helpful comments.

2. $\mathfrak{S}_n$, $\mathfrak{A}_n$, and Projective Linear Groups

We start by proving Theorem 1.4 which we restate below:

Theorem 2.1. *Let $a, b \in \mathfrak{S}_n \backslash \{1\}$ with $n \geq 5$ and set $A := a^{\mathfrak{A}_n}$ and $B := b^{\mathfrak{A}_n}$. For $g \in \mathfrak{S}_n$, let $f(g)$ be the number of fixed points of g in the natural permutation representation. Then f is not constant on AB.*

The proof uses the following easy lemma.

Lemma 2.2. *Let G be a finite group with H a subgroup of G. Let $a, b \in G$ and set $c = ab$, $A = a^H$ and $B = b^H$. Let V be an irreducible $\mathbb{C}G$-module that remains irreducible for H. If χ is the character of V and χ is constant on AB, then $\chi(a)\chi(b) = \chi(c)\chi(1)$.*

Proof. For $X \subseteq G$, let $\theta(X) = \sum_{x \in X} x \in \mathbb{Z}G$. Write $\theta(A)\theta(B) = \sum e_i \theta(C_i)$ where C_i are the H-orbits of elements in AB. Let $\rho : G \to \mathrm{GL}(V)$ denote the representation of G on V. Since H acts irreducibly on V, it follows that if $D = d^H$ for some $d \in G$, then $\rho(\theta(D))$ acts as a scalar on V. Computing traces, we see that the scalar is given by

$$\frac{|D|\,\chi(d)}{\chi(1)}.$$

Thus,

$$\frac{|A||B|\chi(a)\chi(b)}{\chi(1)^2} = (\sum_i e_i |C_i|)\frac{\chi(c)}{\chi(1)}.$$

Since $|A||B| = \sum e_i |C_i|$, the result follows. □

Proof of Theorem 1.4. For $n = 5$, one checks directly. So assume the theorem is false for some $n > 5$. Let $a \in A$, $b \in B$ and $c \in AB$. Note that $\chi := f - 1$ is an irreducible

character of both $\mathfrak{S}_n$ and $\mathfrak{A}_n$. If a and b each have a fixed point, then the result follows by induction.

So we may assume that $f(a) = 0$, i.e., $\chi(a) = -1$. Since $\chi(a)\chi(b) = (n-1)\chi(c)$ by Lemma 2.2, $\chi(c) \neq 0$ implies that $b = 1$, a contradiction. So $\chi(b) = 0 = \chi(c)$. In particular, c has a unique fixed point.

Suppose that neither a nor b is an involution. Then a and b both contain cycles of length at least $r \geq 3$. We can then replace b by a conjugate so that ab has at least $r - 1 \geq 2$ fixed points, a contradiction.

Suppose that either b has a cycle of length 4 or at least 2 nontrivial cycles. Thus, arguing as above, if a is not an involution (in the first case) or of order 2 or 3 (in the second case), we can arrange for ab to have at least 2 fixed points, a contradiction.

If a is a a fixed point free involution, we can reduce to the case that b is an $n-1$-cycle on n points. Then ab can be an n-cycle or can have fixed points, a contradiction. Similarly if a is fixed point free of order three, we can reduce to the case b is an $n-1$-cycle on n points. Again, we can arrange for ab either to have fixed points or not, a contradiction. □

We next consider $\mathrm{L}_d(q)$. We first note a much stronger result for $d = 2$.

Lemma 2.3. *Let $a, b \in \mathrm{GL}_2(q)$, $q > 3$ with a, b both non-central. Set $A = a^H$ and $B = b^H$ where $H = \mathrm{SL}_2(q)$.*

(a) *There exist $(u_i, v_i) \in A \times B$, $i = 1, 2$ such that u_1v_1 fixes a line and u_2v_2 does not.*
(b) *If a and b are semisimple elements with an eigenvalue in $\mathbb{F}_q$, then $|\{\mathrm{tr}(uv) \mid (u, v) \in A \times B\}| = q$.*

Proof. This is a straightforward computation. See also Macbeath [27]. □

For the rest of this section, we fix a prime power q. Let $S = \mathrm{L}_d(q) \leq H \leq G = \mathrm{PGL}_d(q)$ with $d \geq 3$. Let V be the natural module for the lift of G to $\mathrm{GL}_d(q)$. Let $f(g)$ denote the number of fixed 1-spaces of an element $g \in G$. Let $\chi = f - 1$ and note that χ is an irreducible character of G (and S).

Lemma 2.4. *Let a, b be nontrivial elements of G and set $A = a^H$, $B = b^H$ and $c = ab$. If f is constant on AB, then $f(a)$, $f(b)$, and $f(c)$ are each at least 2.*

Proof. Lift a and b to elements in $\mathrm{GL}_d(q) = \mathrm{GL}(V)$ (we abuse notation and still denote them by a and b). Note that $|\chi(g)| \geq 1$ if $\chi(g) \neq 0$.

If $f(a) = 0$, then $-\chi(b) = \chi(1)\chi(c)$ by Lemma 2.2, whence $\chi(c) = \chi(b) = 0$ and so each of b and c fixes a unique line. Similarly, if $f(a) = 1$, then $\chi(a) = 0$, whence $\chi(c) = 0$ and so a and c each fix a unique line. So we may assume that a and c each fix a unique line (interchanging a and b if necessary).

By scaling we may assume that the unique eigenvalue of a in $\mathbb{F}_q$ is 1. Note that if both a and b have cyclic submodules of dimension at least 3, then there are $u \in A$ and $v \in B$ with uv fixing at least two lines. (Indeed, let e_1, e_2, e_3 be part of a basis. Then we can choose u sending e_i to e_{i+1} for $i = 1, 2$ and v sending $\langle e_i \rangle_{\mathbb{F}_q}$ to $\langle e_{i-1} \rangle_{\mathbb{F}_q}$ for $i = 2, 3$.) Then $f(uv) > 1 = f(c)$, a contradiction.

So one of a or b has a quadratic minimal polynomial. Note that a cannot have a quadratic minimal polynomial, since its minimal polynomial has a linear factor and it fixes a unique line. So b has a quadratic minimal polynomial. Note that as long as

$d > 3$, a will either contain a 4-dimensional cyclic submodule or a direct sum of two cyclic submodules of dimension at least 2. Thus, if b has a 4-dimensional submodule that is a direct sum of two 2-dimensional cyclic modules, as above we can arrange that there are conjugates u, v with $f(uv) > 1$. So b has no submodule that is the direct sum of two cyclic submodules of dimension 2. This forces b to be (up to scaling) either a transvection or a pseudoreflection for $d > 3$. The same is true for $d = 3$.

So assume that this is the case. Suppose that a is not unipotent. Write $a = a_1 \oplus a_2$ where a_1 is a single Jordan block and a_2 fixes no lines. Conjugate b so that we may write $b = b_1 \oplus b_2$ where b_2 is not a scalar and b_1 is 1 (and a_i has the same size as b_i). Then since b_2 has a 2 dimensional cyclic submodule as does a_2, we can arrange that a_2b_2 fixes a line. Thus, $f(ab) > 1$, a contradiction.

So we may assume that a is a single Jordan block. If b is a transvection, then we can conjugate such that ab is a unipotent element with 2 blocks, a contradiction.

The remaining case is where a is a single Jordan block and b is a pseudoreflection. So we may assume that a is upper triangular and b is diagonal. Then ab will have two distinct eigenvalues in $\mathbb{F}_q$, whence $f(ab) > 1$, a contradiction. □

We now prove the main result of this section.

Theorem 2.5. *Let $H = \mathrm{L}_d(q) \leq G = \mathrm{PGL}_d(q)$ with $d \geq 3$. If a, b are nontrivial elements of G, then f is not constant on $a^H b^H$.*

Proof. Let $m(a)$ and $m(b)$ denote the dimensions of the largest eigenspaces (with eigenvalue in $\mathbb{F}_q$) for a and b, respectively. Assume that $m(a) \geq m(b)$, and set $c := ab$.

If f is constant on $a^H b^H$, then $\chi(a)\chi(b) = \chi(1)\chi(c)$. We know that $\chi(a), \chi(b)$ and $\chi(c)$ are all positive by the previous lemma.

Note that $m(c) \geq m(b)$ (since we can conjugate and assume that the largest eigenspace of b is contained in that of a). Note also that $\chi(a) \leq q^{d-2} + \ldots + 1$ (with equality precisely when a is essentially a pseudoreflection). Thus, $\chi(a) \leq \chi(1)/q$.

First assume that $m(b) > 1$. Then $\chi(b) < q^{m(b)} - 1$ and $\chi(c) \geq q^{m(b)-1} + \ldots + q > \chi(b)/q$, whence $\chi(a)\chi(b) < \chi(1)\chi(c)$, a contradiction. If $m(b) = 1$, then $\chi(b) \leq q - 1$ and $\chi(c) \geq 1$ (by the previous lemma) and we have the same contradiction. □

3. Classical and low rank exceptional type groups

We first prove the Arad–Herzog conjecture for some low rank classical groups.

Proposition 3.1. *Conjecture A holds for $\mathrm{U}_n(q)$ with $3 \leq n \leq 6$, $(n, q) \neq (3, 2)$.*

Proof. The values of the unipotent characters of $\mathrm{GU}_n(q)$, $3 \leq n \leq 6$, are contained in Chevie [9]. Now unipotent characters restrict irreducibly to the derived group $\mathrm{SU}_n(q)$, and are trivial on the center, so can be regarded as characters of the simple group $\mathrm{U}_n(q)$. It turns out that for $a, b, c \in \mathrm{GU}_n(q)$ non-central the equation $\chi(a)\chi(b) = \chi(1)\chi(c)$ is only satisfied for all unipotent $\chi \in \mathrm{Irr}(\mathrm{GU}_n(q))$ when either c is regular unipotent, or a is unipotent with one Jordan block of size $n - 1$, b is semisimple with centralizer $\mathrm{GU}_{n-1}(q)$ (in $\mathrm{U}_n(q)$) and $c = xy$ is a commuting product with x conjugate to a and y conjugate to b. In particular, in the latter case all three classes have representatives in $\mathrm{GU}_{n-1}(q)$, and it is straightforward to see that the product hits more than one class. The situation of the former case is ruled out by Theorem 1.8 (which does not rely on this result). □

Proposition 3.2. *Conjecture A holds for* $\mathrm{S}_4(q)$, $\mathrm{S}_6(q)$, $\mathrm{O}_8^+(q)$ *and* $\mathrm{O}_8^-(q)$.

Proof. The values of the unipotent characters of the conformal symplectic group $\mathrm{CSp}_{2n}(q)$, $n = 2, 3$, of the conformal spin group $\mathrm{CSpin}_8^+(q)$ and of a group of type ${}^2D_4(q)$ are available in [9]. As before, unipotent characters restrict irreducibly to the derived group and are trivial on the center, so can be regarded as characters of the simple group $\mathrm{S}_{2n}(q)$ respectively $\mathrm{O}_8^\pm(q)$. Again, for given non-central elements a, b, c the equation $\chi(a)\chi(b) = \chi(1)\chi(c)$ fails for at least one unipotent character χ, unless either c is regular unipotent, which by Theorem 1.8 does not give rise to an example, or $n = 2$, q is odd and one of a, b is an element with centralizer $\mathrm{SL}_2(q^2)$. But $\mathrm{Sp}_4(q)$ does not contain such elements. □

Unfortunately, Chevie does not contain the unipotent characters of any group related to $\mathrm{O}_7(q)$.

Next we prove the Arad-Herzog conjecture for the low rank exceptional type groups.

Proposition 3.3. *Conjecture A holds for the groups*

$$ {}^2B_2(2^{2f+1})\ (f \geq 1),\ {}^2G_2(3^{2f+1})\ (f \geq 1),\ G_2(q)\ (q \geq 3),\ {}^3D_4(q),\ {}^2F_4(2^{2f+1})\ (f \geq 1). $$

Proof. The generic character tables of all of the above groups G are available in the Chevie system [9], respectively, the values of all unipotent characters in the case of ${}^2F_4(2^{2f+1})$. It can be checked easily that the equation $\chi(a)\chi(b) = \chi(c)\chi(1)$ is not satisfied simultaneously for all unipotent characters χ of G, for any choice of $a, b, c \neq 1$; except when

(1) $G = {}^2G_2(q^2)$ with b, c of order dividing $q^2 - 1$;
(2) $G = G_2(q)$, $\gcd(q, 6) = 1$, with b, c regular unipotent; or
(3) $G = {}^3D_4(q)$, q odd, with b, c regular unipotent.

In the latter three cases, the required equality fails on some of the two, respectively four, irreducible characters lying in Lusztig series parametrized by an involution in the dual group. □

In fact, one does not even need all the characters mentioned in the above proof: in all cases just four of them will do. We also note that the cases of $\mathrm{L}_3(q)$, $\mathrm{U}_3(q)$, ${}^2G_2(q)$ and $\mathrm{S}_4(q)$ are handled in [34] using available character tables but somewhat more elaborate arguments.

In the next three results, by *a finite classical group* we mean any non-solvable group of the form $\mathrm{SL}(V)$, $\mathrm{SU}(V)$, $\mathrm{Sp}(V)$, or $\mathrm{SO}(V)$, where V is a finite vector space. First we note (see also [23]):

Lemma 3.4. *Let G be a finite classical group with natural module V of dimension d over the finite field $\mathbb{F}_q$. Assume that G has rank at least 2 and that $\dim V \geq 6$ if G is an orthogonal group. Let $x \in G$ be a nontrivial unipotent element of G.*

(a) *Let P be the stabilizer of a singular 1-space with Q the unipotent radical of P. If $x^G \cap P \subseteq Q$, then either $G = \mathrm{Sp}_4(q)$ with q even and x is a short root element, or $G = \mathrm{SU}_4(q)$.*
(b) *If $d = 2m$ and either $G = \mathrm{Sp}_d(q)$ with q even or $G = \mathrm{SU}_d(q)$, and P is the stabilizer of a maximal totally isotropic subspace with Q the unipotent radical of P and $x^G \cap P \subseteq Q$, then x is a long root element.*

Proof. Consider (a). By assumption x is conjugate to an element of Q. If $G = \mathrm{SL}_d(q)$, this forces x to be a transvection and the result is clear. Otherwise, we have $\dim(x-1)V \leq 2$.

If $d \leq 4$, this is a straightforward computation (in particular, for q even, all short root elements in P are contained in Q).

If $d > 4$, then x will act trivially on a nondegenerate space. Thus, if $G = \mathrm{SU}_d(q)$, it suffices to show the claim for $d = 5, 6$ and this is a straightforward computation. In all other cases, it follows by the results for $d \leq 4$ noting that if x is a short root element, then clearly x is conjugate to an element in a Levi subgroup of P.

Now consider (b) with $G = \mathrm{Sp}_d(q)$. Again, we may assume that $x \in Q$ and x is not a transvection. We can identify Q with the set of symmetric matrices of size m. Since x is not a transvection, x corresponds to a symmetric matrix of rank at least 2. If x corresponds to a skew symmetric matrix, then we see that $V = V_1 \perp V_2$ where V_1 is 4-dimensional and x is a short root element on V_1 and the result follows by induction. If x does not correspond to a skew symmetric matrix, we may conjugate x so that it corresponds to a diagonal matrix of rank at least 2, whence we see that $V = V_1 \perp V_2$ where V_1 is 4-dimensional and x has two Jordan blocks on V_1 each nondegenerate. A straightforward computation shows that x stabilizes and acts nontrivially on a 2-dimensional totally singular subspace of V_1 and so also on V.

If $G = \mathrm{SU}_d(q)$, we can identify Q with Hermitian $m \times m$ matrices and every element of Q is conjugate to a diagonal element. Since $g \in Q$ is nontrivial and not a transvection, it corresponds to an element of rank at least 2 in Q and a straightforward computation in SU_4 gives the result. □

We can use this to prove the following result about pairs of unipotent elements in classical groups.

Theorem 3.5. *Let G be a finite classical group with natural module V of dimension $d \geq 2$ over the finite field $\mathbb{F}_q$. Let $x, y \in G$ be nontrivial unipotent elements of G. Then one of the following holds:*

(1) *$x^G y^G$ does not consist of unipotent elements; or*
(2) *$G = \mathrm{Sp}_d(q) = \mathrm{Sp}(V)$, $d \geq 4$, with q even and (up to order) x is a long root element and y is an involution such that $(yv, v) = 0$ for all $v \in V$.*

Proof. For the moment exclude the case that $G = \mathrm{Sp}_d(q)$, $d \geq 4$, with q even or $G = \mathrm{SU}_d(q)$ with $d \geq 4$ even. Let P be the stabilizer of a singular 1-space. By (a) of the previous result and induction, we are reduced to considering $G = \mathrm{SL}_2(q)$ and $G = \mathrm{SU}_3(q)$. We can then apply Lemma 2.3 (and just compute to see that this is still true for $q \leq 3$) and similarly for $\mathrm{SU}_3(q)$.

Next consider $G = \mathrm{Sp}_d(q)$ with q even. Suppose that neither x nor y is a long root element. By applying (b) of the previous lemma, we are reduced to the case of $\mathrm{SL}_m(q)$ where $d = 2m$. If x and y are both long root elements, the result is clear (even for $q = 2$) by reducing to the case of SL_2. So we may assume that x is a long root element and that y is either not an involution or $(yv, v) \neq 0$ for some $v \in V$. Indeed, in either case there exists $v \in V$ with $(yv, v) \neq 0$. By replacing x by a conjugate, we may assume that x leaves $W := \langle v, yv \rangle$ invariant and acts nontrivially. Writing $V = W \oplus W^\perp$ and conjugating x on W as necessary, it is an easy linear algebra computation to see that we can arrange for $\mathrm{tr}(xy) \neq d$, whence xy is not unipotent.

Finally, consider $G = \mathrm{SU}_d(q)$ with d even. If $d = 2$, then the result follows by the case of $\mathrm{SL}_2(q)$. By applying (b) of the previous lemma, we see that we may assume that x is a long root element. By applying (a) of the previous lemma, we are reduced to the case of $\mathrm{SU}_4(q)$ and a straightforward computation completes the proof. □

Note that, by choosing x, y in the same Sylow subgroup of G, we see that $x^G y^G$ always contains unipotent elements. Furthermore, in (2) above, $x^G y^G$ will in fact consist of unipotent elements (since y acts trivially on a maximal totally singular space, we see that x and y always act trivially on a common totally singular space U of dimension $d/2 - 1$ and y will act trivially on the two-dimensional space $U^\perp/U$, whence xy is unipotent). On the other hand, it is also straightforward to compute that xy can be an involution or an element of order 4, whence $x^G y^G$ is not a single conjugacy class. Thus:

Corollary 3.6. *Let G be a finite classical group with natural module V of dimension $d \geq 2$ over the finite field $\mathbb{F}_q$. Let H be the derived subgroup of $G/Z(G)$. Let $x, y \in H$ be nontrivial unipotent elements of H. Then $x^H y^H$ is not a single conjugacy class of H.*

4. Semisimple and unipotent classes

In this section we prove Theorem 1.6 (assuming a result on algebraic groups, Corollary 5.13, which is independent of this section), and complete the proof of Theorem 1.8.

First we set up some notation. Throughout this section, let $\mathbf{G}$ be a connected reductive algebraic group in characteristic $p > 0$ and $F : \mathbf{G} \to \mathbf{G}$ a Steinberg endomorphism of $\mathbf{G}$, with (finite) group of fixed points $G := \mathbf{G}^F$. Note that if $\mathbf{G}$ is simple of adjoint type then $S = O^{p'}(G)$ is almost always simple. We may abuse notation and write $G = \mathbf{G}(q)$ where q is the power of p (always integral unless G is a Suzuki or Ree group; in the latter case we write $\mathbf{G}(q^2)$ instead) such that F acts as $q\phi$ on the character group of an F-stable maximal torus of $\mathbf{G}$, with ϕ of finite order. Note that if $a \in G$ is semisimple, then $a^G = a^S$ (see [36, 2.12]).

4.1. **Proof of Theorem 1.6.** Theorem 1.6 follows from the following, slightly more general result:

Proposition 4.1. *Let $S \leq H \leq G$. Let $a, b \in H$ be nontrivial semisimple elements. Then the Steinberg character is not constant on $a^S b^S$. In particular, $a^H b^H \neq c^H$ for any $c \in H$.*

Proof. Let St denote the Steinberg character of G. Note that St restricts irreducibly to S unless $G = {}^2G_2(3), G_2(2), \mathrm{Sp}_4(2)$ or ${}^2F_4(2)$. In those cases, one can verify the result directly (in the last case, we could use the two "half-Steinberg" representations). Note that if $g \in G$, then

$$\mathrm{St}(g) = \begin{cases} \pm|C_G(g)|_p = \pm q^{m(g)} & \text{if } g \text{ is semisimple,} \\ 0 & \text{else,} \end{cases}$$

where $m(g)$ is the dimension of a maximal unipotent subgroup of $C_{\mathbf{G}}(g)$ (see for example [7, Thm. 6.4.7]). In particular, $\mathrm{St}(1) = q^N$ where N is the number of positive roots of $\mathbf{G}$.

Suppose that a and b are nontrivial semisimple elements and St is constant on $a^H b^H$. Then $\mathrm{St}(a)\mathrm{St}(b) = \mathrm{St}(c)\mathrm{St}(1)$ for $c := ab$, by Lemma 2.2. In particular, $\mathrm{St}(c) \neq 0$, whence c is also semisimple. This in turn implies that $m(a) + m(b) = m(c) + N$.

Since $C_{\mathbf{G}}(a)$ is reductive and contains a maximal torus of $\mathbf{G}$, we see that $\dim C_{\mathbf{G}}(a) = 2m(a) + r$ where r is the rank of $\mathbf{G}$ (and similarly for b and c). Thus,

$$\begin{aligned}\dim C_{\mathbf{G}}(a) + \dim C_{\mathbf{G}}(b) &= 2(m(a) + m(b)) + 2r = 2r + 2m(c) + 2N \\ &= (r + 2N) + (r + 2m(c)) = \dim \mathbf{G} + \dim C_{\mathbf{G}}(c).\end{aligned}$$

Let $f : C_{\mathbf{G}}(a) \times C_{\mathbf{G}}(b) \to \mathbf{G}$ be the multiplication map. Note that each fiber has dimension equal to $\dim(C_{\mathbf{G}}(a) \cap C_{\mathbf{G}}(b))$ which is at most $\dim C_{\mathbf{G}}(c)$ as $c = ab$. It follows that

$$\begin{aligned}\dim C_{\mathbf{G}}(a)C_{\mathbf{G}}(b) &= \dim C_{\mathbf{G}}(a) + \dim C_{\mathbf{G}}(b) - \dim(C_{\mathbf{G}}(a) \cap C_{\mathbf{G}}(b)) \\ &\geq \dim C_{\mathbf{G}}(a) + \dim C_{\mathbf{G}}(b) - \dim C_{\mathbf{G}}(c) = \dim \mathbf{G}.\end{aligned}$$

Thus, $C_{\mathbf{G}}(a)C_{\mathbf{G}}(b)$ is dense in $\mathbf{G}$. By Corollary 5.13 (below) this cannot occur, so St cannot be constant on $a^S b^S$. □

4.2. **Proof of Theorem 1.8.** For any F-stable maximal torus $\mathbf{T}$ of $\mathbf{G}$ and any $\theta \in \mathrm{Irr}(\mathbf{T}^F)$, Deligne and Lusztig defined a generalized character $R_{\mathbf{T},\theta}^{\mathbf{G}}$ of $G = \mathbf{G}^F$. Its restriction $Q_{\mathbf{T}}^{\mathbf{G}} := R_{\mathbf{T},\theta}^{\mathbf{G}}|_{G_u}$ to the set G_u of unipotent elements of G is independent of θ, rational valued, and called the Green function corresponding to $\mathbf{T}$ (see for instance [7, §§7.2, 7.6]).

The following is an easy consequence of Deligne–Lusztig's character formula for $R_{\mathbf{T},\theta}^{\mathbf{G}}$:

Proposition 4.2. *Let $\mathbf{G}, F$ be as above. Let $x \in G$, with Jordan decomposition $x = su$, where $s \in G$ is semisimple, u is unipotent. Let $\mathbf{T} \leq \mathbf{G}$ be an F-stable maximal torus with $s \notin \mathbf{T}^g$ for all $g \in G$. Then $R_{\mathbf{T},\theta}^{\mathbf{G}}(x) = 0$ for any $\theta \in \mathrm{Irr}(\mathbf{T}^F)$.*

Proof. By [7, Thm. 7.2.8] we have

$$R_{\mathbf{T},\theta}^{\mathbf{G}}(x) = \frac{1}{|\mathbf{C}^F|} \sum_{g \in G\,:\, s^g \in \mathbf{T}^F} \theta(s^g)\, Q_{{}^g\mathbf{T}}^{\mathbf{C}}(u),$$

where $\mathbf{C} = C_{\mathbf{G}}^{\circ}(s)$. Clearly, this shows that $R_{\mathbf{T},\theta}^{\mathbf{G}}(x) = 0$ unless $s \in {}^g\mathbf{T}^F$ for some $g \in G$. □

Now assume that $S = G/Z(G)$ is a finite simple group (which usually happens when $\mathbf{G}$ is simple of simply connected type).

Proposition 4.3. *In the above setting, let $c \in S$ be unipotent and suppose that there are $a, b \in S$ with $a^S b^S = c^S$. Then for any F-stable maximal torus $\mathbf{T} \leq \mathbf{G}$ such that $T = \mathbf{T}^F$ has a character θ in general position with $\theta|_{Z(G)} = 1$ we have:*

(a) *the semisimple parts a_s, b_s of a, b are conjugate to elements of T, and*
(b) $|C_G(a)|\,|C_G(b)| \geq |G : T|_{p'}^2$.

Proof. As θ is in general position, $R_{\mathbf{T},\theta}^{\mathbf{G}}$ is an irreducible character of G up to sign, say χ, by [7, Cor. 7.3.5]. Since $\theta|_{Z(G)} = 1$ we also have $\chi|_{Z(G)} = 1$ by the character formula [7, Thm. 7.2.8], so χ can be considered as an irreducible character of $S = G/Z(G)$. Moreover, since $Q_{\mathbf{T}}^{\mathbf{G}}$ is rational valued we have

$$R_{\mathbf{T},\theta}^{\mathbf{G}}(c) = Q_{\mathbf{T}}^{\mathbf{G}}(c) \equiv Q_{\mathbf{T}}^{\mathbf{G}}(1) = R_{\mathbf{T},\theta}^{\mathbf{G}}(1) = \pm|G : T|_{p'} \equiv \pm 1 \pmod{p}.$$

(Here, the first congruence holds for any generalized character of the cyclic p-group $\langle c\rangle$, and the second congruence holds since it is true for cyclotomic polynomials in q.) In particular, $\chi(c)$ is a nonzero integer. Thus, by Lemma 2.2, we also have $\chi(a)\chi(b) = \chi(1)\chi(c) \neq 0$. By Proposition 4.2 this gives (a), and moreover

$$|C_G(a)| \cdot |C_G(b)| \geq |\chi(a)|^2 \cdot |\chi(b)|^2 \geq \chi(1)^2 = |G : T|_{p'}^2.$$

□

Proposition 4.4. *Let S be a simple group of Lie type, and $a, b, c \in S \setminus \{1\}$ such that $a^S b^S = c^S$. Then c is unipotent if and only if both a and b are.*

Proof. Let $\mathbf{G}$ be a simple, simply connected algebraic group over an algebraic closure of $\mathbb{F}_p$ and $F : \mathbf{G} \to \mathbf{G}$ a Steinberg endomorphism whose group of fixed points $G = \mathbf{G}^F$ satisfies $S = G/Z(G)$. This is possible unless $S = {}^2F_4(2)'$, for which the claim is easily checked directly. If S is of exceptional type and twisted Lie rank at most 2, the claim has already been proved in Proposition 3.3. For all other types we have given in Tables 1 and 2 two maximal tori of G (see [31, Tables 5.2 and 5.8]), with the following properties: in the exceptional types always, and in the classical types whenever the corresponding Zsigmondy primes ℓ_i exist, the dual tori contain regular elements of order this Zsigmondy prime (by [31, Lemmas 5.3 and 5.9]) and with connected centralizer in the dual group. Note that ℓ_i is coprime to $|Z(G)|$, so both tori have characters θ_i in general position with the center in their kernel.

Now let $\tilde{a}, \tilde{b}$ be preimages of a, b respectively in G. Assume that $\tilde{c} \in G$ is unipotent, with image c in S. Then Proposition 4.3 applies to say that $\tilde{a}_s$ is conjugate to elements of both T_1, T_2. But in all cases the intersection of T_1 with any conjugate of T_2 lies in $Z(G)$, so a is unipotent, and similarly for b.

We now consider the classical groups for which not both Zsigmondy primes exist. The groups $\mathrm{L}_2(q)$, $\mathrm{L}_3(q)$, $\mathrm{L}_6(2)$, $\mathrm{L}_7(2)$ are handled in Lemma 2.3 and Theorem 2.5. For the unitary groups $\mathrm{U}_3(q)$ and the symplectic groups $\mathrm{S}_4(q)$ as well as for the groups $\mathrm{U}_6(2)$, $\mathrm{S}_6(2)$, $\mathrm{O}_8^+(2)$, $\mathrm{O}_8^-(2)$, the claim follows by Propositions 3.1 and 3.2 while for the groups $\mathrm{U}_7(2)$, $\mathrm{S}_8(2)$ it can be checked directly using the character tables in GAP.

Conversely, if a, b are unipotent then without loss they lie in a common Sylow p-subgroup of S, and hence so does c, whence it is unipotent. □

Table 1. Two tori and Zsigmondy primes in exceptional groups

G	$\lvert T_1\rvert$	$\lvert T_2\rvert$	ℓ_1	ℓ_2
$F_4(q)$	Φ_8	Φ_{12}	$l(8)$	$l(12)$
$E_6(q)$	Φ_9	$\Phi_1\Phi_2\Phi_8$	$l(9)$	$l(8)$
${}^2E_6(q)$	Φ_{18}	$\Phi_1\Phi_2\Phi_8$	$l(18)$	$l(8)$
$E_7(q)$	$\Phi_2\Phi_{18}$	$\Phi_1\Phi_7$	$l(18)$	$l(7)$
$E_8(q)$	Φ_{30}	Φ_{24}	$l(30)$	$l(24)$

Together with Corollary 3.6 this establishes Theorem 1.8 for classical groups. To complete the proof of Theorem 1.8 for exceptional groups, we need the following result of Lawther:

TABLE 2. Two tori and Zsigmondy primes in classical groups

G	$\lvert T_1\rvert$	$\lvert T_2\rvert$	ℓ_1	ℓ_2
A_n	$(q^{n+1}-1)/(q-1)$	q^n-1	$l(n+1)$	$l(n)$
${}^2A_n$ $(n\geq 2$ even$)$	$(q^{n+1}+1)/(q+1)$	q^n-1	$l(2n+2)$	$l(n)$
${}^2A_n$ $(n\geq 3$ odd$)$	$(q^{n+1}-1)/(q+1)$	q^n+1	$l(n+1)$	$l(2n)$
B_n, C_n $(n\geq 2$ even$)$	q^n+1	$(q^{n-1}+1)(q+1)$	$l(2n)$	$l(2n-2)$
B_n, C_n $(n\geq 3$ odd$)$	q^n+1	q^n-1	$l(2n)$	$l(n)$
D_n $(n\geq 4$ even$)$	$(q^{n-1}-1)(q-1)$	$(q^{n-1}+1)(q+1)$	$l(n-1)$	$l(2n-2)$
D_n $(n\geq 5$ odd$)$	q^n-1	$(q^{n-1}+1)(q+1)$	$l(n)$	$l(2n-2)$
${}^2D_n$ $(n\geq 4)$	q^n+1	$(q^{n-1}+1)(q-1)$	$l(2n)$	$l(2n-2)$

Lemma 4.5 (Lawther)**.** *Let $G = F_4(q)$ with q even. Let $P = QL$ be a maximal end node parabolic with unipotent radical Q and Levi subgroup $L \cong C_3(q)T_1$. If $u \in G$ is a nontrivial unipotent element such that $u^G \cap P \subset sQ \cup Q$ where s is a long root element in L, then u is a long root element.*

Proof. The proof is a case by case analysis. Write roots in F_4 as linear combinations of simple roots, so that for example the highest root is denoted 2342. Write w_i for the Weyl group reflection corresponding to the ith simple root.

Let us say that if x is a product of positive root elements, at least one of whose roots is in $\{0010, 0001, 0011\}$, then x has property (*). Observe that if x has property (*), then x mod Q is neither the identity nor a long root element of L. Now note that Shinoda [37, p. 130] has listed unipotent class representatives $x_0, x_1, \ldots, x_{34}$ of G. Recall that $x_0 = 1$ and x_2 is a long root element. Thus it suffices to observe that for $i = 1, 3, 4, \ldots, 34$ there is a $g_i \in G$ so that $g_i^{-1}x_ig_i \in P$ has property (*).

If $i = 1, 3, 4$, take $g_i = w_4w_3w_2w_1w_3w_2$. If $5 \leq i \leq 16$, take $g_i = w_1w_2$. If $19 \leq i \leq 21$, take $g_i = w_2$. In the remaining cases, x_iQ is neither trivial nor a long root element. The result follows. □

Now we can use our methods together with another result of Lawther [23] to obtain the following:

Theorem 4.6. *Let G be a finite simple group of Lie type in characteristic p. Let u, w be nontrivial unipotent elements of G. Then u^Gw^G is not a single conjugacy class. If uw^g is unipotent for all $g \in G$, then $p \leq 3$ and (up to order) one the following holds:*

(1) *$G = \mathrm{Sp}_{2n}(q)$, $p = 2$, u is a long root element and w is an involution (which satisfies $(wv, v) = 0$ for all $v \in V$, the natural module);*
(2) *$G = F_4(q)$, $p = 2$, u is a long root element and w is a short root element; or*
(3) *$G = G_2(q)$, $p = 3$, u is a long root element and w is a short root element.*

Proof. If G is classical, this follows by Theorem 3.5. If $G = {}^2G_2(q^2)$, ${}^2B_2(q^2)$, ${}^2F_4(q^2)'$ or ${}^3D_4(q)$, the result follows by a computation using Chevie. If $G = E_n(q)$, then by [19, §2], we can assume that u, w are in an end node parabolic subgroup and not in its radical. The result now follows by induction (since none of the exceptions occur in the inductive step). If $G = {}^2E_6(q)$, then by Lawther [23], the same argument applies.

Suppose that $G = G_2(q)$. If $q = 2$, one computes directly. Let P_i, $i = 1, 2$ denote the two maximal parabolic subgroups containing a fixed Borel subgroup. Let Q_i be the unipotent radical of P_i. If $p \neq 3$ and $q > 2$, it follows by [23] that any unipotent element is conjugate to an element of $P_1 \setminus Q_1$ and so the result follows by the result for A_1. If $p = 3$, then also by [23] unless u is a long root element and w is a short root element (or vice versa), u, w are conjugate to elements in $P_i \setminus Q_i$ for $i = 1$ or 2 and the result follows by the case of A_1. Alternatively, one can compute using Chevie.

It remains to consider $G = F_4(q)$. Let P be a maximal parabolic subgroup with Levi subgroup of type $B_3(q)$. By [23], we may assume that u, w are in P and not in the radical Q of P. Arguing as above, we may reduce to the case of $B_3(q)$, whence the result for q odd. If q is even, the same argument shows that the result holds unless (up to order), $u^G \cap P \subset Q \cup xQ$ where x is a long root element and $w^G \cap P \subset Q \cup yQ$ where y is a short root element. Now Lemma 4.5 forces u to be a long root element. Now replace u and w by their images u' and w' under the graph automorphism. So u' is a short root element. As above, this forces w' to be a long root element, whence w is a short root element.

We now show that $u^G w^G$ is not a single conjugacy class. If so, then uw^g is conjugate to uw for all g. Of course, uw^g may be unipotent. So the result is clear aside from the three special cases above. In (1), it is straightforward to observe that uw^g may have order either 2 or 4. Consider (2). Since we can choose $u, w^g \in H \leq F_4$ with $H \cong \mathrm{Sp}_4(q)$, the result holds. Finally, in (3), it is straightforward to see that uw^g can be a regular unipotent element (and so of order 9). On the other hand, u and w are both conjugate to central elements in a Sylow 3-subgroup, whence uw^g can also be a 3-central element (of order 3). This completes the proof. □

In fact, we will see (in Examples 6.1, 6.3, and 6.6) that in all the exceptional cases in the previous result, $\langle u, w^g \rangle$ is unipotent for all g (even in the corresponding algebraic group).

Lawther [23] proves much more than we require for the proof of Theorem 4.6. He determines all pairs of conjugacy classes C of unipotent elements and maximal parabolic subgroups P of a finite simple group of Lie type such that $C \cap P$ is contained in the unipotent radical of P.

Now Theorem 1.8 immediately follows from Proposition 4.4 and Theorem 4.6.

4.3. **Some permutation characters.** We now prove some results on certain permutation characters for $G_2(q)$ and $F_4(q)$ that we will need for our results on algebraic groups.

Lemma 4.7. *Let $G = G_2(q)$ with $(q, 3) = 1$. Let a be a long root element and b an element of order 3 with centralizer $\mathrm{SL}_3(q)$ or $\mathrm{SU}_3(q)$ (depending upon whether $q \equiv 1 \pmod 3$ or not). Let $C = C_G(a)$ and $D = C_G(b)$. Then the scalar product $[1_C^G, 1_D^G]$ equals 2. Moreover, if $q \equiv 1 \pmod 3$, then $\langle a, b \rangle$ is contained in a Borel subgroup of G.*

Proof. We give the proof for $q \equiv 1 \pmod 3$. Essentially the identical proof works in the other case. Moreover, for our application to algebraic groups, this case is sufficient.

Note that $[1_C^G, 1_D^G] = |C \backslash G / D|$ or equivalently the number of orbits of G on $\Gamma := a^G \times b^G$ (acting by simultaneous conjugation).

We will produce two distinct G-orbits on Γ and show that the number of elements in the union of these orbits is $|\Gamma|$, whence the result.

The first orbit consists of the commuting pairs in Γ. We can conjugate and assume that the second element is b and so a must be a long root elements in D. We thus see that this is a single orbit of size $q^3(q^3+1)(q+1)(q^3-1)$.

Using Chevie, we see that we may choose $(c,d) \in \Gamma$ such that cd is conjugate to bu with u a regular unipotent element in D. Thus, $C_G(c) \cap C_G(d)$ is isomorphic to a subgroup of $C_D(u)$ which has order $3q^2$. We claim that $C_G(c) \cap C_G(d)$ contains no elements of order 3. This is because the only elements of order 3 in D which are conjugate to b in G are b and b^{-1}. Since c does not commute with d, it follows that no element of order 3 is in $C_G(c) \cap C_G(d)$. Thus, $|C_G(c) \cap C_G(d)| \leq q^2$ (in fact, we have equality but this will come out).

Thus, the size of the G-orbit containing (c,d) is $[G : (C_G(c) \cap C_G(d))] \geq q^4(q^2-1)(q^6-1)$. It follows that the size of the union of these two orbits is at least $|\Gamma|$ (and so exactly).

Since we are assuming that $q \equiv 1 \pmod 3$, b is contained in some Borel subgroup B of G containing the Borel subgroup of $C_G(b)$. Let T be a maximal torus of $C_B(b)$ (and so also of G). Let a_1 be a long root element of $C_B(b)$. Let J be the subgroup of B generated by T and all long root elements of B. Since J is normal in B and $C_B(b)$ is not normal in B, we can choose a long root element a_2 of B not in $C_B(g)$. Thus, (a_1, b) and (a_2, b) are in different G-orbits on $a^G \times b^G$. It follows that each pair in Γ is contained in some Borel subgroup of G. □

Lemma 4.8. *Let $G = F_4(q)$ with q odd. Let a be a long root element of G and b an involution in G with centralizer $H := C_G(b)$ of type $B_4(q)$. Let P be the normalizer of the long root subgroup of G containing a, so that $P' = C_G(a)$. Then $[1_H^G, 1_{P'}^G] = 2$. Moreover, if $(c,d) \in a^G \times b^G$, then $\langle c, d\rangle$ is contained in a Borel subgroup of G.*

Proof. Certainly, $1_{P'}^G = \sum_{\lambda \in \mathrm{Irr}(P/P')} \lambda^G$, with $P/P' \cong C_{q-1}$.

Let $\mathbf{P} \leq \mathbf{G}$ be an F-stable parabolic subgroup with $\mathbf{P}^F = P$, and $\mathbf{L}$ an F-stable Levi subgroup of $\mathbf{P}$. Any nontrivial linear character λ of P/P' can be viewed as a linear character of $L = \mathbf{L}^F$, and then λ^G is the Harish-Chandra induction $R_{\mathbf{L}}^{\mathbf{G}}(\lambda)$ of λ. Thus λ belongs to the Lusztig series $\mathcal{E}(L,s)$, where s is a nontrivial central (semisimple) element of $L^* \leq G^* = \mathbf{G}^{*F^*}$, the dual of L, where $\mathbf{G}^*$ denotes the dual group (which is isomorphic to G). Now $\mathbf{L}$ has type C_3T_1, with T_1 a 1-dimensional torus. So the underlying algebraic group $\mathbf{L}^*$ with $L^* = \mathbf{L}^{*F^*}$ has type B_3T_1. By [7, Prop. 3.6.8] we have $Z(\mathbf{L}^*)^{F^*} = Z(L^*)$, whence $C_{\mathbf{G}^*}(s)$ contains the reductive subgroup $\mathbf{L}^*$ of type B_3T_1. Note that Lusztig induction $R_{\mathbf{L}}^{\mathbf{G}}$ sends any irreducible character in $\mathcal{E}(L,s)$ to a linear combination of irreducible characters in $\mathcal{E}(G,s)$, cf. for instance [26, Lemma 8.2]. So all the irreducible constituents φ of λ^G belongs to $\mathcal{E}(G,s)$.

On the other hand, since q is odd, by [22, p. 110] we have

$$1_H^G = \chi_{\phi_{1,0}} + \chi_{\phi''_{8,3}} + \chi_{\phi_{4,1}} + \chi_{\phi''_{2,4}} + \chi_{\kappa_1}^{1,St} + \sum_{j=1}^{(q-3)/2} \chi_{\kappa_7,j}^1 + \sum_{j=1}^{(q-1)/2} \chi_{\kappa_{8,j}}^1,$$

where the first four constituents are unipotent characters (and χ_ψ is the unipotent character labeled by the Weyl group character ψ listed in [7, §13.9]). Furthermore, the fifth constituent belongs to $\mathcal{E}(G,\kappa_1)$, where $\kappa_1 = (t_1)^{G^*}$ is the conjugacy class of an involution $t_1 \in G^*$ with $C_{\mathbf{G}^*}(t_1)$ of type C_3A_1. Each of the summands in the next two summations belongs to $\mathcal{E}(G,\kappa_{7,j})$ or $\mathcal{E}(G,\kappa_{8,j})$, where $\kappa_{a,j} = (t_{a,j})^{G^*}$ is the conjugacy class of a

semisimple element $t_{a,j} \in G^*$, with the semisimple part of $C_{\mathbf{G}^*}(t_{a,j})$ being of type C_3 for $a = 7, 8$. Since $C_{\mathbf{G}^*}(s)$ contains a reductive subgroup of type B_3T_1, s cannot be conjugate to any of the elements 1, t_1, or $t_{a,j}$, $a = 7, 8$. It follows that $[1_H^G, \lambda^G] = 0$ for $\lambda \neq 1$.

Thus $[1_H^G, 1_{P'}^G] = [1_H^G, 1_P^G]$, and it remains to consider the case $\lambda = 1_P$. It is well known that the decomposition of 1_P^G into irreducible constituents is given by the corresponding decomposition for the permutation character of the Weyl group $W(F_4)$ acting on the cosets of the parabolic subgroup $W(C_3)$, the Weyl group of L. The irreducible constituents in the latter decomposition are $\chi_{\phi_{1,0}}$, $\chi_{\phi'_{2,4}}$, $\chi_{\phi_{9,2}}$, $\chi_{\phi_{4,1}}$, and $\chi_{\phi'_{8,3}}$. Thus, the scalar product of the two permutation characters is 2 as claimed.

It follows that G has two orbits on $a^G \times b^G$. Let B be a Borel subgroup of G containing a Borel subgroup of $C_G(b) \cong B_4(q)$. Arguing as in the previous case, we can choose long root elements $a_1, a_2 \in B$ with $a_1b = ba_1$ and $a_2b \neq ba_2$. Certainly, (a_1, b) and (a_2, b) belong to different G-orbits on $a^G \times b^G$. It follows that each pair in $a^G \times b^G$ is contained in some Borel subgroup of G. □

5. Algebraic Groups

We first recall some facts about conjugacy classes in algebraic groups. Throughout the section we fix an algebraically closed field k of characteristic $p \geq 0$.

By a fundamental result of Lusztig there are only finitely many conjugacy classes of unipotent elements in a connected reductive group. This is easily seen to imply that if A and B are conjugacy classes of a simple algebraic group, then AB is an infinite union of conjugacy classes if and only if the closure of AB contains infinitely many semisimple conjugacy classes. We will not use this result in what follows.

We will use the following elementary result. Note that if a is an element of a connected reductive algebraic group $\mathbf{G}$ and $a = su = us$ where s is semisimple and u is unipotent, then $s \in \overline{a^{\mathbf{G}}}$.

Lemma 5.1. *Let $\mathbf{G}$ be a connected reductive algebraic group over k, $\mathbf{T}$ a maximal torus of $\mathbf{G}$, and let A and B be non-central conjugacy classes of $\mathbf{G}$. Then the following statements hold.*

(a) *$\overline{AB}$ either contains a unique semisimple conjugacy class of $\mathbf{G}$ or contains infinitely many semisimple classes.*
(b) *$\overline{AB}$ contains a unique semisimple conjugacy class if and only if $\overline{AB} \cap \mathbf{T}$ is finite.*

Proof. Suppose that $\overline{AB}$ contains finitely many semisimple classes $C_1, \ldots, C_m$. Let X_i be the set of elements in $\mathbf{G}$ whose semisimple parts are in C_i. Note that X_i is closed (since if $s \in X_i$ is a semisimple element, then X_i consists of all elements $g \in \mathbf{G}$ with $\chi(g) = \chi(s)$ for all the characters of rational finite-dimensional $\mathbf{G}$-modules). Since A and B are irreducible varieties, so is $\overline{AB}$, whence $\overline{AB} \subset \cup_i X_i$ implies that $\overline{AB} \subset X_i$ for some i. This proves (a).

Now (b) follows by (a) and the facts that every semisimple class of $\mathbf{G}$ intersects $\mathbf{T}$ nontrivially and this intersection is finite (since it is an orbit of the Weyl group on $\mathbf{T}$, see [7, Prop. 3.7.1]). □

We need some results about closures of unipotent classes. These can be deduced from the results in [38]. We give elementary proofs for what we need (but quote [38] for G_2

and also for F_4 in characteristic 2). We also do not consider the groups of type B in characteristic 2. The results in this case can be read off from the results for the groups of type C. The first such result we need has a very short proof, see [15, Cor. 3.3].

Lemma 5.2. *Let $\mathbf{G}$ be a simple algebraic group over an algebraically closed field k of characteristic $p \geq 0$ and $g \in \mathbf{G}$ a nontrivial unipotent element. Then the closure of $g^{\mathbf{G}}$ contains root elements.*

We next note the following fact:

Lemma 5.3. *Let $\mathbf{G}$ be a semisimple algebraic group with $a, b \in \mathbf{G}$. If $C_{\mathbf{G}}(a)C_{\mathbf{G}}(b)$ is dense in $\mathbf{G}$, then $a^{\mathbf{G}}b^{\mathbf{G}}$ is contained in the closure of $(ab)^{\mathbf{G}}$. In particular, the semisimple parts of elements of $a^{\mathbf{G}}b^{\mathbf{G}}$ form a single semisimple conjugacy class of $\mathbf{G}$.*

Proof. Let $\Gamma = \{(g, h) \in \mathbf{G} \times \mathbf{G} \mid gh^{-1} \in C_{\mathbf{G}}(a)C_{\mathbf{G}}(b)\}$. Note that by assumption Γ contains a dense open subset of $\mathbf{G} \times \mathbf{G}$. Suppose that $(g, h) \in \Gamma$. Then

$$(a^g, b^h) = (a^{gh^{-1}}, b)^h = (a^{xy}, b)^h = (a, b)^{yh},$$

where $gh^{-1} = xy$ with $x \in C_{\mathbf{G}}(a)$ and $y \in C_{\mathbf{G}}(b)$. Consider $f : \mathbf{G} \times \mathbf{G} \to \mathbf{G}$ given by $f(g, h) = a^g b^h$. If $c = ab$, then $f(\Gamma) \subseteq c^{\mathbf{G}}$, whence $f(\mathbf{G} \times \mathbf{G})$ is contained in the closure of $c^{\mathbf{G}}$, and the first part of the lemma follows.

Let s be the semisimple part of c. Let $\mathbf{G}_s$ be the set of elements in $\mathbf{G}$ whose semisimple part is conjugate to s. As previously noted, $\mathbf{G}_s$ is a closed subvariety of $\mathbf{G}$. Thus, $a^{\mathbf{G}}b^{\mathbf{G}} \subseteq \overline{c^{\mathbf{G}}} \subseteq \mathbf{G}_s$. □

We record the following trivial observation. Let H and K be subgroups of a group G and set $\Gamma := G/H \times G/K$. Then G acts naturally on Γ and the orbits of G on Γ are in bijection with the orbits of H on G/K and so in bijection with $H\backslash G/K$. In particular, this implies:

Lemma 5.4. *Let G be a group with $a, b \in G$. The number of conjugacy classes in $a^G b^G$ is at most $|C_G(a)\backslash G/C_G(b)|$.*

We record the following easy result.

Lemma 5.5. *Let $\mathbf{G}$ be a connected reductive algebraic group with $\mathbf{H}$ a connected reductive subgroup. If $a, b \in \mathbf{H}$ and the semisimple parts of $a^{\mathbf{H}}b^{\mathbf{H}}$ are not a single $\mathbf{H}$-class, then the semisimple parts of $a^{\mathbf{G}}b^{\mathbf{G}}$ are a union of an infinite number of $\mathbf{G}$-conjugacy classes.*

Proof. Let $\mathbf{S}$ be a maximal torus of $\mathbf{H}$ and $\mathbf{T}$ a maximal torus of $\mathbf{G}$ containing $\mathbf{S}$. By Lemma 5.1, $\overline{a^{\mathbf{H}}b^{\mathbf{H}}} \cap \mathbf{S}$ is infinite. In particular, $\overline{a^{\mathbf{G}}b^{\mathbf{G}}} \cap \mathbf{T}$ is infinite and the result follows by another application of Lemma 5.1. □

We next point out the following short proof about products of centralizers. For unipotent elements, this was proved independently by Liebeck and Seitz [25, Chapter 1]. We will obtain stronger results below.

Corollary 5.6. *Let $\mathbf{G}$ be a semisimple algebraic group. If $a \in \mathbf{G}$ is not central and $g \in \mathbf{G}$, then $C_{\mathbf{G}}(a)C_{\mathbf{G}}(a^g)$ is not dense in $\mathbf{G}$.*

Proof. Clearly, we can reduce to the case that $\mathbf{G}$ is simple. Write $a = su$ where $su = us$, s is semisimple and u is unipotent. If $u \neq 1$, then u is not central and since $C_{\mathbf{G}}(u) \geq C_{\mathbf{G}}(a)$, we may assume $a = u$. If $u = 1$, then a is semisimple. In particular, we may assume that a is either semisimple or unipotent.

As we have noted in Lemma 5.3, if $C_{\mathbf{G}}(a)C_{\mathbf{G}}(a^g)$ is dense in $\mathbf{G}$, then the semisimple parts of elements of $a^{\mathbf{G}}a^{\mathbf{G}}$ form a single conjugacy class. If a is semisimple, then we may assume that a lies in a maximal torus $\mathbf{T}$ and does not commute with some root subgroup $\mathbf{U}_\alpha$. However, by Lemma 2.3 applied to any large enough field $\mathbb{F}_q$ that contains an eigenvalue of a, $a^{\mathbf{H}}a^{\mathbf{H}}$ contains more than one semisimple class in $\mathbf{H} := \langle \mathbf{U}_{\pm\alpha}, \mathbf{T}\rangle$, whence the result follows by Lemma 5.5.

If $a \neq 1$ is unipotent, then by Lemma 5.2, there is a positive root α and a nontrivial element $b \in \mathbf{U}_\alpha$ in the closure of $a^{\mathbf{G}}$. Set $\mathbf{H} := \langle \mathbf{U}_\alpha, \mathbf{U}_{-\alpha}\rangle$, a rank 1 group. By a direct computation in SL_2, we see that $b^{\mathbf{H}}b^{\mathbf{H}}$ contains both non-central semisimple and unipotent elements. The result now follows by Lemma 5.3. □

Note that Corollary 1.3 now follows since $C_{\mathbf{G}}(a)g^{-1}C_{\mathbf{G}}(a) = C_{\mathbf{G}}(a)C_{\mathbf{G}}(a^g)g^{-1}$.

Lemma 5.7. *Let $\mathbf{G} = \mathrm{Sp}_{2n}(k) = \mathrm{Sp}(V)$ where k is an algebraically closed field of characteristic 2. Let $g \in \mathbf{G}$ be a nontrivial unipotent element that is not a transvection. Let $h \in \mathbf{G}$ be a unipotent element such that $V = V_1 \perp V_2 \perp V_3$ with $\dim V_1 = \dim V_2 = 2$ such that h induces a transvection on V_1 and V_2 and is trivial on V_3.*

(a) *Suppose that $(gv, v) = 0$ for all $v \in V$. Then $g^2 = 1$, and the closure of $g^{\mathbf{G}}$ contains short root elements but not long root elements.*
(b) *The closure of $h^{\mathbf{G}}$ contains both short and long root elements.*
(c) *Suppose that $(gv, v) \neq 0$ for some $v \in V$. Then the closure of $g^{\mathbf{G}}$ contains h and so also both long and short root elements.*

Proof. In (a) write $g = I + N$ where N is nilpotent. Note that $(Nv, v) = (gv - v, v) = 0$ for all $v \in V$. Note also that $0 = (N(v + w), v + w) = (Nv, w) + (Nw, v)$ and so $(Nv, w) = (Nw, v)$ for all $v, w \in V$. It follows that $NV \subseteq (\ker N)^\perp$, whence we see that N (and g) act trivially on a maximal totally singular subspace W of V. Let $\mathbf{P}$ be the stabilizer of W and $\mathbf{Q}$ its unipotent radical. We may view $\mathbf{Q}$ as the space of symmetric $n \times n$ matrices. Let $\mathbf{Q}_0$ be the subspace of skew symmetric matrices. Thus, $g \in \mathbf{Q}$, whence $g^2 = 1$. Moreover the condition that $(gv, v) = 0$ is exactly equivalent to $g \in \mathbf{Q}_0$.

Since $(gv, v) = 0$ for all $v \in V$ is a closed condition, any element in the closure of $g^{\mathbf{G}}$ also satisfies this, whence long root elements are not in the closure of $g^{\mathbf{G}}$ (and so necessarily short root elements are — this is also obvious from the proof above). This proves (a).

To prove (b) it suffices to work in Sp_4. Note that we can conjugate h and assume that it is in the unipotent radical $\mathbf{Q}$ of the stabilizer of a maximal totally singular space. Note that $h^{\mathbf{G}} \cap \mathbf{Q}$ is dense in $\mathbf{Q}$ and since $\mathbf{Q}$ contains both long and short root elements, the result follows.

Now assume that $(gv, v) \neq 0$ for some $v \in V$. Recall that g is not a transvection.

Choose $0 \neq w \in V$ with $gw = w$. Let $\mathbf{P}$ be the subgroup of $\mathbf{G}$ stabilizing the line containing w and let $\mathbf{Q}$ be its unipotent radical. Note that $(gu, u) \neq 0$ for some u with $(u, w) \neq 0$ (if $(gu, u) = 0$ for all u outside $w^\perp$, then $(gu, u) = 0$ for all u by density). Let $X = ku + kw$ which is a nondegenerate 2-dimensional space and set $Y = X^\perp$.

Let $\mathbf{L}$ be the Levi subgroup of $\mathbf{P}$ that stabilizes ku and kw (and so also X and Y). Let $\mathbf{T}$ be the 1-dimensional central torus of $\mathbf{L}$.

With respect to the decomposition $V = kw \oplus Y \oplus ku$, g acts as

$$\begin{pmatrix} 1 & s & c \\ 0 & r & s^\top \\ 0 & 0 & 1 \end{pmatrix}$$

where $r \in \mathrm{Sp}(Y)$ is a unipotent element and $c \neq 0$. First suppose that r is nontrivial. Thus, we see that the closure of g^T contains an element of the same form but with $s = 0$. Since the closure of r in $\mathrm{Sp}(Y)$ contains a root element, we see that we may assume that $V = X \perp Y$, g induces a transvection on X and $\dim Y = 2$ or 4 and g induces either a transvection on Y or a short root element. If g induces a transvection on Y, then g is conjugate to h and there is nothing more to prove. So assume that $\dim Y = 4$ and g acts as a short root element on Y. This implies that the fixed space of g is a 3-dimensional totally singular subspace Z. The hypotheses imply that the closure of $g^{\mathbf{G}}$ contains the unipotent radical of the stabilizer of Z, whence it contains h. Finally suppose that r is trivial. Since g is not a transvection, s is nontrivial. Since Sp is transitive on nonzero vectors, we can then assume that $s = (1, 0, \ldots, 0)$ and so reduce to the case of Sp_4. In that case, g is already conjugate to h. This completes the proof. □

Lemma 5.8. *Let $\mathbf{G}$ be a simple algebraic group over an algebraically closed field k of characteristic $p \geq 0$. Let g be a nontrivial unipotent element of $\mathbf{G}$. The closure of $g^{\mathbf{G}}$ contains long root elements unless one of the following occurs:*

(1) $(\mathbf{G}, p) = (G_2, 3)$ *or* $(F_4, 2)$ *and g is a short root element; or*
(2) $\mathbf{G} = \mathrm{Sp}_{2n} = \mathrm{Sp}(V)$, $p = 2$, $n \geq 2$ *and* $(gv, v) = 0$ *for all* $v \in V$.

Moreover, if $(\mathbf{G}, p) = (G_2, 3)$ *or* $(F_4, 2)$ *and g is not a root element, then the closure of $g^{\mathbf{G}}$ contains both short and long root elements.*

Proof. By Lemma 5.2, the result follows unless $\mathbf{G}$ has two root lengths.

If $\mathbf{G} = G_2$, see [38, II.10.4]. Similarly if $\mathbf{G} = F_4$ with $p = 2$, see [38, p. 250].

Now assume that $p \neq 2$ and $\mathbf{G} = B_n$, C_n or F_4. It suffices to show that for g a short root element, the closure of $g^{\mathbf{G}}$ contains long root elements. By passing to a rank 2 subgroup containing both long and short root subgroups, it suffices to consider $\mathbf{G} = \mathrm{Sp}_4 = \mathrm{Sp}(V)$. In this case, we can write $V = V_1 \perp V_2$ where g acts as a transvection on each V_i and so clearly the closure of $g^{\mathbf{G}}$ contains long root elements (for $\mathbf{U}$ a maximal unipotent subgroup of $\mathrm{Sp}(V_1) \times \mathrm{Sp}(V_2)$, $g^{\mathbf{G}} \cap \mathbf{U}$ is dense in $\mathbf{U}$ and $\mathbf{U}$ contains long root elements).

Finally, when $p = 2$ and $\mathbf{G} = \mathrm{Sp}_{2n} = \mathrm{Sp}(V)$ we may apply Lemma 5.7. □

Lemma 5.9. *Let $\mathbf{G} = \mathrm{SO}_{2n+1}(k) = \mathrm{SO}(V)$, $n \geq 2$, with k an algebraically closed field of characteristic $p \neq 2$. Let $g \in \mathbf{G}$ be unipotent. Then the closure of $g^{\mathbf{G}}$ contains a short root element if and only if g has a Jordan block of size at least* 3.

Proof. Clearly, the condition is necessary since having all Jordan blocks of size at most 2 is a closed condition and a short root element has a Jordan block of size 3. Conversely, suppose that g has a Jordan block of size $d \geq 3$. It is well known that V can be written as an orthogonal direct sum of g-invariant subspaces on each of which either g has a single Jordan block of odd size or it has two Jordan blocks of (the same) even size of g.

Thus, we can write $V = V_1 \perp V_2$ where either $\dim V_1 = d \geq 3$ is odd and g acting on V_1 is a regular unipotent element of $\mathrm{SO}(V_1)$ or $\dim V_1 = 2d \geq 6$ and g acts on V_1 with two Jordan blocks of size d. By taking closures, we may assume that g is trivial on V_2. In the first case, the closure of $g^{\mathbf{G}}$ contains all unipotent elements of $\mathrm{SO}(V_1)$ (in particular a short root element). In the second case, we see that g is contained in some GL_d Levi subgroup of $\mathrm{SO}(V_1)$ and so g is a regular unipotent element of GL_d. Thus, its closure contains all unipotent elements of GL_d, whence in particular an element with two Jordan blocks of size 3. Now argue as in the first case. □

We next need a result about subgroups generated by root subgroups of a given length.

Lemma 5.10. *Let $\mathbf{G}$ be a simply connected algebraic group over an algebraically closed field k of characteristic $p \geq 0$. Let $\mathbf{T}$ be a maximal torus of $\mathbf{G}$ and let Φ denote the set of roots of $\mathbf{G}$ with respect to $\mathbf{T}$. Assume that Φ contains roots of two distinct lengths. Let Φ_ℓ denote the long roots in Φ and $\Phi_s = \Phi \setminus \Phi_\ell$ the short roots. Let $X_\ell = \langle \mathbf{U}_\alpha \mid \alpha \in \Phi_\ell \rangle$, and $\mathbf{X}_s = \langle \mathbf{U}_\alpha \mid \alpha \in \Phi_s \rangle$. The following hold:*

(a) $C_{\mathbf{G}}(\mathbf{X}_s) = Z(\mathbf{G})$.
(b) *If $\mathbf{G} = G_2$, then $C_{\mathbf{G}}(\mathbf{X}_\ell)$ has order 3 if $p \neq 3$ and is trivial otherwise.*
(c) *If $p = 2$ and $\mathbf{G} \neq G_2$, then $C_{\mathbf{G}}(\mathbf{X}_\ell) = Z(\mathbf{G})$.*
(d) *If $p \neq 2$ and $\mathbf{G} \neq G_2$, then $C_{\mathbf{G}}(\mathbf{X}_\ell)$ is an elementary abelian 2-group and intersects a unique non-central conjugacy class of involutions unless $\mathbf{G} = \mathrm{Sp}_{2n}$ in which case it intersects every conjugacy class of involutions (in Sp_{2n}).*

Proof. This is a straightforward observation. In fact if $p \neq 2$, then $\mathbf{X}_s = \mathbf{G}$ unless $\mathbf{G} = G_2$ with $p = 3$. In all those cases, the centralizer is just the center. So we only need to consider $\mathbf{X}_\ell$. If $\mathbf{G} = F_4$, then $\mathbf{X}_\ell \cong D_4$ while if $\mathbf{G} = \mathrm{Sp}_{2n}$, $\mathbf{X}_\ell \cong \mathrm{SL}_2 \times \ldots \times \mathrm{SL}_2$. Finally if $\mathbf{G} = B_n$ with $p \neq 2$, then $\mathbf{X}_\ell \cong D_n$. The result follows. □

We can now prove Theorem 1.1 which we restate. As we have already remarked, the result is essentially independent of the isogeny type of the simple algebraic group. We will work with the most convenient form for each group (in particular, we work with Sp_{2n} and SO_{2n+1}).

Theorem 5.11. *Let $\mathbf{G}$ be a simple algebraic group over an algebraically closed field k of characteristic $p \geq 0$. Let a, b be non-central elements of $\mathbf{G}$. Then one of the following holds (up to interchanging a and b and up to an isogeny for $\mathbf{G}$):*

(1) *There are infinitely many semisimple conjugacy classes which occur as the semisimple part of elements of $a^{\mathbf{G}} b^{\mathbf{G}}$.*
(2) $\mathbf{G} = \mathrm{Sp}_{2n}(k) = \mathrm{Sp}(V)$, *$n \geq 2$, $\pm b$ is a long root element, and either*
   (a) *$p \neq 2$ and a is an involution; or*
   (b) *$p = 2$ and a is an involution with $(av, v) = 0$ for all v in V.*
(3) $\mathbf{G} = \mathrm{SO}_{2n+1}(k) = \mathrm{SO}(V)$, *$n \geq 2$, $p \neq 2$ and $-a$ is a reflection and b is a unipotent element with all Jordan blocks of size at most 2.*
(4) $\mathbf{G} = G_2$, *$p \neq 3$, a is of order 3 with centralizer SL_3 and b is a long root element.*
(5) $\mathbf{G} = F_4$, *$p \neq 2$, a is an involution with centralizer of type B_4 and b is a long root element.*
(6) $(\mathbf{G}, p) = (F_4, 2)$ *or* $(G_2, 3)$, *a is a long root element and b is a short root element.*

Proof. Let A be the closure of $a^{\mathbf{G}}$ and B the closure of $b^{\mathbf{G}}$. Note that if the closure of $a^{\mathbf{G}}b^{\mathbf{G}}$ contains only finitely many semisimple classes, the same is true for AB (take closures). Thus, the same is true for $A'B'$ where $A' \subset A$ and $B' \subset B$ are conjugacy classes.

Also recall (Lemma 5.5) that if $a, b \in \mathbf{H}$ a connected reductive subgroup of $\mathbf{G}$ and there are infinitely many semisimple classes occurring as the semisimple part of elements of $a^{\mathbf{H}}b^{\mathbf{H}}$, then the same is true in $\mathbf{G}$.

A) We give a very quick proof in the case that $\mathbf{G}$ has only one root length where we show that it is always the case that $a^{\mathbf{G}}b^{\mathbf{G}}$ contains infinitely many classes with distinct semisimple parts.

If the semisimple part s of a is noncentral, then s is in the closure of $a^{\mathbf{G}}$ and so we may assume that a is semisimple. If not, then modifying a by a central element, we may assume that a is unipotent. Similarly, we may assume that b is either semisimple or unipotent.

If a and b are both semisimple, choose a maximal torus $\mathbf{T}$ containing conjugates a', b' of a and b. By conjugating by Weyl group elements, we may assume that a', b' do not commute with $\mathbf{U}_\alpha$ for some root α. Thus, $\langle \mathbf{T}, \mathbf{U}_{\pm\alpha}\rangle$ is reductive with semisimple part A_1. Moreover, a', b' are not central, whence the result follows from the result for A_1 (see Lemma 2.3). Similarly if a and b are both unipotent, then by replacing a and b by elements in the closures of the classes, we may assume that a and b are both long root elements, whence as above we reduce to the case of A_1. If a is unipotent and b is semisimple, then as above, we may assume that $a \in \mathbf{U}_\alpha$ and $b \in \mathbf{T}$ does not centralize a, whence again the result follows by the case of A_1.

B) So for the rest of the proof we assume that $\mathbf{G}$ has two root lengths. In particular $\mathrm{rank}(\mathbf{G}) > 1$. The proof is similar to that above but more complicated (and there are always exceptions).

Case 1. a, b are both semisimple.

Let $\mathbf{T}$ be a maximal torus containing both a and b. We apply Lemma 5.10. In particular, we can choose a (short) root subgroup $\mathbf{U}_\alpha$ and conjugates of a, b by elements of the Weyl group that do not centralize $\mathbf{U}_\alpha$. Now the result follows by considering the subgroup $\langle \mathbf{T}, \mathbf{U}_{\pm\alpha}\rangle$.

Case 2. a and b are both unipotent and are not among the excluded cases.

If the closures of A and B both contain long root elements, then the result follows from the case of A_1. If $p \neq 2$, this is always the case by Lemma 5.8 unless $(\mathbf{G}, p) = (G_2, 3)$. If $\mathbf{G} = G_2$ with $p = 3$ or $\mathbf{G} = F_4$ with $p = 2$, aside from the excluded cases, the closures of A and B will either contain both long root elements or short root elements and again the result follows.

It remains only to consider $\mathbf{G} = \mathrm{Sp}_{2n}$ with $p = 2$. It follows by Lemma 5.8 that unless a or b is a long root element, the closures of A and B will contain short root elements and the result follows as above. So we may assume that b is a long root element and that the closure of A does not contain long root elements. Again by Lemma 5.8 this implies that a is an involution with $(av, v) = 0$ for $v \in V$.

Case 3. a is semisimple and b is unipotent.

Let $a \in \mathbf{T}$ be a maximal torus. If $\operatorname{char} k = 2$ with $\mathbf{G} \neq G_2$, we can choose a root subgroup $\mathbf{U}_\alpha$ with a not centralizing $\mathbf{U}_\alpha$ and reduce to $\langle \mathbf{T}, \mathbf{U}_{\pm\alpha} \rangle$. If $\mathbf{G} = G_2$ with $p = 3$, the same argument suffices.

Indeed, if the closure of $b^{\mathbf{G}}$ contains a short root element, then it suffices to assume that b is contained in a short root subgroup $\mathbf{U}_\alpha$ and as above, we can conjugate a by an element of the Weyl group and assume that a does not centralize $\mathbf{U}_\alpha$. Now argue as before.

The same argument suffices if a is not an involution conjugate to an element of the centralizer of the subgroup of $\mathbf{G}$ generated by the long root subgroups (with respect to $\mathbf{T}$). So we have reduced to the case that a is such an involution and the closure of $b^{\mathbf{G}}$ contains long root elements and not short root elements. By Lemma 5.8, these are precisely the exceptions allowed in the theorem.

Case 4. The general case.

We may assume (by interchanging a and b if necessary and using the previous cases) that $a = su = us$ where s is a noncentral semisimple element and $u \neq 1$ is unipotent.

If the semisimple part of b is not central, we can take closures and so assume that b is semismple. If the semisimple part of b is central, we can replace b by a central element times b and assume that b is unipotent.

If b is unipotent, then we can take closures and assume that b is a root element. By working in the closure of a^G (which contains s), we see that by previous cases, it must be that $s^{\mathbf{G}} b^{\mathbf{G}}$ must have constant semisimple part. This implies that either $p \neq 2$, $\mathbf{G} \neq G_2$ and s is an involution with b a long root element or $\mathbf{G} = G_2$, $p \neq 3$, s is an element of order 3 and b is a long root element.

Let $\mathbf{T}$ be a maximal torus. We may assume that $b \in \mathbf{U}_\alpha$, a root subgroup with respect to $\mathbf{T}$. By taking closures in $D := C_{\mathbf{G}}(s)$, we may also assume that u is in a root subgroup $\mathbf{U}_\beta$ with respect to $\mathbf{T}$. Thus, by considering $\langle \mathbf{T}, \mathbf{U}_{\pm\alpha}, \mathbf{U}_{\pm\beta} \rangle$, it suffices to assume that $\mathbf{G}$ has rank 2.

Now suppose that $p \neq 2$ and $\mathbf{G} = \mathrm{Sp}_4$. As noted above, s must be an involution. Note that D contains both long and short root elements and moreover the centralizer of s is an A_1A_1, whence we see that there are conjugates of b and a in D with $a^D b^D$ having infinitely many different semisimple parts.

The remaining case is $p \neq 3$ and $\mathbf{G} = G_2$. It follows that s is an element of order 3 with centralizer D isomorphic to A_2. So u is a long root element. As we noted, b is also a long root element and so conjugate to an element of D. The result follows since it holds for A_2. □

We will discuss the examples listed above in the next section. In particular, we will see that in all cases $a^{\mathbf{G}} b^{\mathbf{G}}$ is a finite union of classes but always more than one. Indeed, we will see that $a^{\mathbf{G}} \times b^{\mathbf{G}}$ is the union of a very small number of $\mathbf{G}$-orbits (but always at least 2). In particular, this implies the following result which includes Szep's conjecture for algebraic groups. See [8] for the finite case and [5, 6] for related results on factorizations.

Corollary 5.12. *Let $\mathbf{G}$ be a simple algebraic group. If a, b are non-central elements of $\mathbf{G}$, then $a^{\mathbf{G}} b^{\mathbf{G}}$ is not a single conjugacy class and $\mathbf{G} \neq C_{\mathbf{G}}(a) C_{\mathbf{G}}(b)$.*

Another immediate consequence is:

Corollary 5.13. *Suppose that* $\mathbf{G}$ *is a simple algebraic group over an algebraically closed field* k *with* $\operatorname{char} k = p \geq 0$*, and that* a, b *are non-central elements of* $\mathbf{G}$*. If* $C_{\mathbf{G}}(a)C_{\mathbf{G}}(b)$ *is dense, then* $\mathbf{G}, a, b$ *are as described in Theorem 5.11. In particular,* $C_{\mathbf{G}}(a)C_{\mathbf{G}}(b)$ *is not dense if any of the following hold (modulo the center):*

(1) *a and b are conjugate;*
(2) *neither a nor b is unipotent; or*
(3) *a is semisimple and has order greater than* 3.

Indeed, if a is semisimple and is not an involution then $\mathbf{G} = G_2$ and a has order 3.

We point out one further corollary which also comes from analyzing the exceptions in the theorem above.

Corollary 5.14. *Let* $\mathbf{G}$ *be a semisimple algebraic group. Let* $a, b \in \mathbf{G}$*. The following are equivalent.*

(i) *$a^{\mathbf{G}}b^{\mathbf{G}}$ is a finite union of conjugacy classes.*
(ii) *The closure of $a^{\mathbf{G}}b^{\mathbf{G}}$ contains only one semisimple conjugacy class.*
(iii) *$|C_{\mathbf{G}}(a)\backslash\mathbf{G}/C_{\mathbf{G}}(b)|$ is finite.*
(iv) *$\mathbf{G}$ has finitely many orbits on $a^{\mathbf{G}} \times b^{\mathbf{G}}$.*
(v) *$C_{\mathbf{G}}(a)C_{\mathbf{G}}(b^g)$ is dense in $\mathbf{G}$ for some $g \in \mathbf{G}$.*
(vi) *$\langle a, b^g\rangle$ is contained in some Borel subgroup of $\mathbf{G}$ for every $g \in \mathbf{G}$.*

Proof. Statements (i) and (ii) are equivalent by Lemma 5.1, and clearly (iii) and (iv) are equivalent. Furthermore, (iii) implies (v). By Lemma 5.3 we have that (v) implies (ii).

Assume that (vi) holds. The conjugates of x_1, x_2 inside the normalizer of a fixed Borel subgroup have only finitely many distinct semisimple parts, so the same is true for their possible products, whence we get (ii) by Lemma 5.1.

Thus it remains to show that (i) implies (iii) and (vi), which we do in the next section by going through the cases in Theorem 5.11. Note that by passing to the adjoint quotient of $\mathbf{G}$ we may assume that $\mathbf{G}$ is a direct product of its simple factors, and finiteness of the product of two classes in that direct product is equivalent to finiteness in each simple component (and similarly for the properties in (iii) and (vi)). □

In fact, we will see that in all the cases where $a^{\mathbf{G}}b^{\mathbf{G}}$ is a finite union of conjugacy classes, it is a union of at most 4 classes.

6. Examples with dense centralizer products

We now consider the examples for the exceptions in Theorem 1.1 and show that $a^{\mathbf{G}}b^{\mathbf{G}}$ is a finite union of conjugacy classes in all cases. However, it always consists of at least two classes and so $\mathbf{G} \neq C_{\mathbf{G}}(a)C_{\mathbf{G}}(b)$. We also show that there is a dense (and so open) element in $C_{\mathbf{G}}(a)\backslash\mathbf{G}/C_{\mathbf{G}}(b)$, whence $C_{\mathbf{G}}(a)C_{\mathbf{G}}(b^g)$ is dense for some $g \in \mathbf{G}$. Indeed we will see that $|C_{\mathbf{G}}(a)\backslash\mathbf{G}/C_{\mathbf{G}}(b)| \leq 4$ in all cases.

Throughout the section, fix k to be an algebraically closed field of characteristic $p \geq 0$.

Example 6.1. Let $\mathbf{G} = G_2$ with $p = 3$. Let a be a long root element and b a short root element. Choose conjugates so that ab is a regular unipotent element. Then $\dim a^{\mathbf{G}} = \dim b^{\mathbf{G}} = 6$ and $\dim(ab)^{\mathbf{G}} = 12$. Since $\dim a^{\mathbf{G}} + \dim b^{\mathbf{G}} = 12$, we see that $\dim a^{\mathbf{G}}b^{\mathbf{G}} \leq 12$ and so $(ab)^{\mathbf{G}}$ is the dense orbit in $a^{\mathbf{G}}b^{\mathbf{G}}$. In particular, $\overline{a^{\mathbf{G}}b^{\mathbf{G}}}$ is the set of unipotent

elements in $\mathbf{G}$. Moreover, for such a pair (a,b) we see that $\dim(C_{\mathbf{G}}(a)\cap C_{\mathbf{G}}(b))\geq 2$ because $\dim C_{\mathbf{G}}(a)=\dim C_{\mathbf{G}}(b)=8$. However, since $C_{\mathbf{G}}(a)\cap C_{\mathbf{G}}(b)\leq C_{\mathbf{G}}(ab)$ and $\dim C_{\mathbf{G}}(ab)=2$, we have equality, whence $C_{\mathbf{G}}(a)C_{\mathbf{G}}(b)$ is dense in $\mathbf{G}$. Note that there are at least two classes in $a^{\mathbf{G}}b^{\mathbf{G}}$. As noted, $a^{\mathbf{G}}b^{\mathbf{G}}$ contains the regular unipotent elements. On the other hand, we can find conjugates which commute and so the product will have order 3 and so is not a regular unipotent element (and so $\mathbf{G}\neq C_{\mathbf{G}}(a)C_{\mathbf{G}}(b)$). Since $(a,b)^{\mathbf{G}}$ is dense in $a^{\mathbf{G}}\times b^{\mathbf{G}}$, it follows that any pair in $a^{\mathbf{G}}\times b^{\mathbf{G}}$ is contained in some Borel subgroup.

We next show that in fact $|C_{\mathbf{G}}(a)\backslash\mathbf{G}/C_{\mathbf{G}}(b)|=2$. This can be seen as follows. Fix a maximal torus $\mathbf{T}$ and a Borel subgroup $\mathbf{B}$ containing $\mathbf{T}$. Note that we may take $C_{\mathbf{G}}(a)=\mathbf{P}_1'$ and $C_{\mathbf{G}}(b)=\mathbf{P}_2'$ where $\mathbf{P}_1$ and $\mathbf{P}_2$ are the maximal parabolics containing $\mathbf{B}$. Let $\mathbf{T}_i=\mathbf{T}\cap\mathbf{P}_i'$. Since the $\mathbf{P}_1,\mathbf{P}_2$ double cosets are in bijection with the corresponding double cosets in the Weyl group, we see that there are 2 such double cosets. Note that if w is in the Weyl group, then $\mathbf{P}_1'w\mathbf{P}_2'=\mathbf{P}_1'\mathbf{T}_1(\mathbf{T}_2)^w w\mathbf{P}_2'$. Note that $\mathbf{T}=\mathbf{T}_1(\mathbf{T}_2)^w$ for any w in the Weyl group. It follows that $\mathbf{P}_1'w\mathbf{P}_2'=\mathbf{P}_1'\mathbf{T}w\mathbf{T}\mathbf{P}_2'=\mathbf{P}_1w\mathbf{P}_2$ and so $|\mathbf{P}_1'\backslash\mathbf{G}/\mathbf{P}_2'|=2$.

Example 6.2. Let $\mathbf{G}=G_2$ with $p\neq 3$. Let a be a long root element and b an element of order 3 with centralizer SL_3. First take k to be the algebraic closure of a finite field. By Lemma 4.7, we see that $\mathbf{G}$ has two orbits on $a^{\mathbf{G}}\times b^{\mathbf{G}}$ and for any $(c,d)\in a^{\mathbf{G}}\times b^{\mathbf{G}}$, $\langle c,d\rangle$ is contained in some Borel subgroup. As noted in the proof of Lemma 4.7, $a^{\mathbf{G}}b^{\mathbf{G}}$ consists of two conjugacy classes (the classes have representatives bx and by where x is a long root element of $C_{\mathbf{G}}(b)$ and y is a regular unipotent element of $C_{\mathbf{G}}(b)$).

By taking ultraproducts, we see that the same is true for some algebraically closed field of characteristic 0. By a well known argument (cf. [14, 1.1]), it follows that the same is true for any algebraically closed field of characteristic not 3.

Example 6.3. Let $\mathbf{G}=F_4$ with $p=2$. Let a be a long root element and b be a short root element. We will show that $\langle a,b\rangle$ is always unipotent. Let $\mathbf{T}$ be a maximal torus of $\mathbf{G}$ with $\mathbf{T}\leq\mathbf{B}$, a Borel subgroup of $\mathbf{G}$. Let $\mathbf{P}_1$ and $\mathbf{P}_4$ be the two end node maximal parabolic subgroups containing $\mathbf{B}$. Note that there are only finitely many $\mathbf{P}_1,\mathbf{P}_4$ double cosets in $\mathbf{G}$ each of the form $\mathbf{P}_1w\mathbf{P}_4$ where w is in the Weyl group. We may assume that $\mathbf{P}_1'=C_{\mathbf{G}}(a)$ and $\mathbf{P}_4'=C_{\mathbf{G}}(b)$. Arguing precisely as for G_2 with $p=3$, we see that $\mathbf{P}_1'w\mathbf{P}_4'=\mathbf{P}_1w\mathbf{P}_4$. Thus there are only finitely many $C_{\mathbf{G}}(a),C_{\mathbf{G}}(b)$ double cosets in $\mathbf{G}$. In fact, by computing in the Weyl group, we see that there are precisely 2 double cosets. In particular, $\mathbf{G}$ has only two orbits on $a^{\mathbf{G}}\times b^{\mathbf{G}}$, whence the semisimple part of any element in $a^{\mathbf{G}}b^{\mathbf{G}}$ is the same up to conjugacy and so is contained in the set of unipotent elements. The dense double coset corresponds to w being the element which acts as inversion on $\mathbf{T}$. One computes that the group generated by a and b^w is unipotent, whence this is true for all pairs in $a^{\mathbf{G}}\times b^{\mathbf{G}}$ (by density).

If a and b^g commute, then ab^g has order 2 while if a and b^g do not commute, we see that ab^g has order 4 (already in C_2). Thus $a^{\mathbf{G}}b^{\mathbf{G}}$ consists of two conjugacy classes.

Example 6.4. Let $\mathbf{G}=F_4$ with $p\neq 2$. Let a be a long root element and let b be an involution with centralizer of type B_4. If k is the algebraic closure of a finite field of odd characteristic, it follows by Lemma 4.8 that $|C_{\mathbf{G}}(a)\backslash\mathbf{G}/C_{\mathbf{G}}(b)|=2$ and every pair $(c,d)\in a^{\mathbf{G}}\times b^{\mathbf{G}}$ has the property that $\langle c,d\rangle$ is contained in a Borel subgroup. Arguing as for G_2 with $p\neq 3$, the same is true for k any algebraically closed field of characteristic

not 2. Thus, $\mathbf{G}$ has two orbits on $a^{\mathbf{G}} \times b^{\mathbf{G}}$. Clearly, one orbit is the set of commuting pairs. If a and b^g commute, then $(ab^g)^2$ is a long root element. It is straightforward to compute that if a and b^g do not commute, then $(ab^g)^2$ is a short root element and so there are exactly two conjugacy classes in $a^{\mathbf{G}}b^{\mathbf{G}}$.

Example 6.5. Let $\mathbf{G} = \mathrm{Sp}_{2n} = \mathrm{Sp}(V)$, $n \geq 2$, with $p \neq 2$. Let a be a transvection and let b be an involution (i.e., all eigenvalues are ± 1). We claim that $\langle a, b\rangle$ is contained in a Borel subgroup, whence $a^{\mathbf{G}}b^{\mathbf{G}}$ contains only elements with the semisimple part conjugate to b. Let W be the intersection of the fixed spaces of a and b. If W contains a nondegenerate subspace, we pass to the orthogonal complement and use induction. If W is totally singular, then $\dim W = n-1$ or n. Let $\mathbf{P}$ be the stabilizer of W with unipotent radical $\mathbf{Q}$. If $\dim W = n$, a is in $\mathbf{Q}$, whence the result. If $\dim W = n-1$, then b is central in $\mathbf{P}/\mathbf{Q}$, whence the result follows in this case as well.

Since $C_{\mathbf{G}}(b) = \mathrm{Sp}_{2m} \times \mathrm{Sp}_{2n-2m}$, we see that $C_{\mathbf{G}}(b)$ has three orbits on $V \setminus \{0\}$ whence $|C_{\mathbf{G}}(a)\backslash\mathbf{G}/C_{\mathbf{G}}(b)| = 3$. It is straightforward to see (already in Sp_4) that $a^{\mathbf{G}}b^{\mathbf{G}}$ contains elements whose square are long root elements or short root elements, whence $a^{\mathbf{G}}b^{\mathbf{G}}$ contains at least 2 conjugacy classes.

Example 6.6. Let $\mathbf{G} = \mathrm{Sp}_{2n} = \mathrm{Sp}(V)$, $n \geq 2$ with $p = 2$. Let a be a transvection and b an involution with $(bv, v) = 0$ for all $v \in V$. We claim that $\langle a, b\rangle$ is unipotent. Consider the intersection W of the fixed space of b and the fixed space of a. This has dimension at least $n-1 \geq 1$. If this space contains a nondegenerate space D, we can replace V by $D^{\perp}$ and use induction (note that if $n = 1$, $b = 1$). So we may assume that W is totally singular. Let $\mathbf{P}$ be the stabilizer of W and $\mathbf{Q}$ the unipotent radical of $\mathbf{P}$. If $\dim W = n$, then a, b are both in $\mathbf{Q}$ and so commute. If $\dim W = n-1$, then $\langle a, b\rangle \leq \mathbf{Q}\mathrm{Sp}_2$ whence $b \in \mathbf{Q}$. Thus $a^{\mathbf{G}}b^{\mathbf{G}}$ is contained in the set of unipotent elements (and any pair in $a^{\mathbf{G}} \times b^{\mathbf{G}}$ is contained in a common Borel subgroup). As we have seen a and b may commute and so ab is an involution but it is straightforward to see that the order of ab may be 4.

We can write $V = V_1 \perp V_2 \perp \ldots \perp V_m \perp W$ where $\dim V_i = 4$, and b acts as a short root element on V_i and b is trivial on W. If $n = 2$, we argue as for G_2 to see that $C_{\mathbf{G}}(a)C_{\mathbf{G}}(b)$ can be dense. Indeed, it follows that in general $C_{\mathbf{G}}(b)$ has only finitely many orbits on V, whence there are only finitely many $C_{\mathbf{G}}(a), C_{\mathbf{G}}(b)$ double cosets in $\mathbf{G}$. Indeed, it is a fairly easy exercise in linear algebra to show that $C_{\mathbf{G}}(b)$ has at most 4 orbits on nonzero vectors in V, whence $|C_{\mathbf{G}}(a)\backslash\mathbf{G}/C_{\mathbf{G}}(b)| \leq 4$.

Example 6.7. Let $\mathbf{G} = \mathrm{SO}_{2n+1} = \mathrm{SO}(V)$, $n \geq 2$ with $p \neq 2$. Let $a \in \mathbf{G}$ be such that $-a$ is a reflection, and let b be a unipotent element with all Jordan blocks of size at most 2. We claim that $\langle a, b\rangle$ is contained in a Borel subgroup of $\mathbf{G}$, whence $a^{\mathbf{G}}b^{\mathbf{G}}$ consists of unipotent elements. If $n = 2$, then the result follows by the result for Sp_4. So assume that $n > 2$. Let W be the intersection of the -1 eigenspace of a and $[b, V]$. Note that $W \neq 0$ (since $\dim[b, V] \geq 2$) and is totally singular. By induction, ab has semisimple part the negative of a reflection on $W^{\perp}/W$, whence also in $\mathbf{G}$.

Note that $C_{\mathbf{G}}(a)$ is the stabilizer of a nonsingular 1-space. Note also that the number of Jordan blocks of b is even, whence by reducing to the 4-dimensional case we see that $C_{\mathbf{G}}(b)$ has only finitely many orbits on 1-dimensional spaces. Thus there are only finitely many $C_{\mathbf{G}}(a)\backslash\mathbf{G}/C_{\mathbf{G}}(b)$ double cosets. Indeed, it is a straightforward exercise to see that $|C_{\mathbf{G}}(a)\backslash\mathbf{G}/C_{\mathbf{G}}(b)| \leq 4$. By reducing to the case of $\mathrm{SO}_5 \cong C_2$, we see that the unipotent

parts of elements in $a^{\mathbf{G}}b^{\mathbf{G}}$ are in at least 2 different conjugacy classes, whence $a^{\mathbf{G}}b^{\mathbf{G}}$ is not a single conjugacy class.

7. A short proof of Szep's conjecture

We use our previous results to give a short proof of the conjecture of Szep's (a finite simple group cannot be the product of two centralizers); see [8] for the original proof. In particular, using Corollaries 1.7 and 5.13 (for semisimple elements), we can shorten the proof considerably.

Observe the following connection to the Arad–Herzog conjecture. Let G be a group with $a, b \in g$. As we have noted the number of orbits of G on $a^G \times b^G$ is precisely $C_G(a)\backslash G/C_G(b)$. In particular, if $G = C_G(a)C_G(b)$, then G acts transitively on $a^G \times b^G$ and $a^G b^G$ is a single conjugacy class of G. Indeed if $w(x, y)$ is any element of the free group on two generators, then $w(a', b')$ is conjugate to $w(a, b)$ for all $(a', b') \in a^G \times b^G$. In particular, if the Arad–Herzog conjecture holds for G, then no such factorization can exist.

Theorem 7.1 (Szep's conjecture; Fisman–Arad [8])**.** *Let G be a finite non-abelian simple group. If a, b are non-trivial elements of G, then $G \neq C_G(a)C_G(b)$.*

Proof. For alternating groups, the Arad–Herzog conjecture, proved in Theorem 1.4, gives the result. For the twenty six sporadic groups, it is straightforward to check the Arad–Herzog conjecture from the character tables.

So now assume that G is simple of Lie type. The basic idea is as follows. We find two primes r_1, r_2 for which the Sylow r_i-subgroups of G are cyclic and there exist regular semisimple elements $x_1, x_2 \in G$ of order r_i such that no nontrivial element of G centralizes conjugates of both of them.

Then assume that $G = C_G(a)C_G(b)$ for $a, b \in G$. If r_i divides $|C_G(a)|$, then some conjugate of x_i centralizes a, and similarly for $|C_G(b)|$. Thus by our assumption, a centralizes a conjugate of x_1, say, and b centralizes a conjugate of x_2. Since the x_i are regular, this implies that a, b are both semisimple. But then by Proposition 4.1, $a^G b^G$ consists of more than one class of G. As pointed out above this implies that $C_G(a)C_G(b) \neq G$, a contradiction.

For G of exceptional type and rank at least 4, we take for r_1, r_2 Zsigmondy primes as listed in Table 1. For the small rank cases the claim follows from Proposition 3.3.

For G of classical type, the claim for $\mathrm{L}_n(q)$ follows by Theorem 2.5, and for $\mathrm{U}_n(q)$ with $3 \leq n \leq 6$ by Proposition 3.1. For the types ${}^2A_n$, B_n, C_n, ${}^2D_n$ and D_{2n+1}, we take the two tori T_1, T_2 given in [32, Table 2.1], which contain Zsigmondy prime elements and are not contained in a common centralizer (by the arguments given in [32, §2]).

This leaves only the case of $\mathrm{O}^+_{4n}(q)$. If $n = 2$, we apply Proposition 3.2. So assume that $n > 2$. Here we take r_1 to be a Zsigmondy prime divisor of $q^{4n-2} - 1$, r_2 to be a Zsigmondy prime divisor of $q^{2n-1} - 1$. Let $x_i \in G$ be of order r_i. Note that the Sylow r_i-subgroups of G are cyclic, and x_1 and x_2 are regular semisimple. Abusing the notation, we will let x_i denote the inverse image of x_i of order r_i in $S := \mathrm{SO}^+_{4n}(q)$. Then $C_S(x_1) \cong C_{q^{2n-1}+1} \times C_{q+1}$ and $C_S(x_2) \cong C_{q^{2n-1}-1} \times C_{q-1}$. Suppose $s \in S$ centralizes conjugates of both x_1 and x_2. Then $|s|$ divides $\gcd(q^{2n+1} + 1, q^{2n-1} - 1) \leq 2$. In particular, $s = 1$ if $2|q$. Assume q is odd and $s \neq 1$. Since s centralizes a conjugate of x_1, we see that s acts as ± 1 on U_1 and as

± 1 on $U_1^\perp$, where U_1 is a nondegenerate subspace (of the natural $\mathbb{F}_q S$-module $V = \mathbb{F}_q^{4n}$) of type $-$ of codimension 2. Similarly, since s centralizes a conjugate of x_2, s acts as ± 1 on U_2 and as ± 1 on $U_2^\perp$, where U_2 is a nondegenerate subspace of V of type $+$ of codimension 2. This can happen only when $s = -1_V$. We have shown that no nontrivial element of G can centralize conjugates of both x_1 and x_2, and so we can finish as above. $\square$

We next give some examples to show that if the ambient group is not simple, there are many counterexamples to both Szep's conjecture and the Arad–Herzog conjecture. Of course, a trivial example is to take G a direct product and choose elements in different factors. There is a more interesting example for almost simple groups.

Example 7.2. Let $G := \mathrm{GL}_{2n}(q) = \mathrm{GL}(V)$, $n \geq 1$, $q > 2$, $(n, q) \neq (1, 3)$, and let τ be a graph automorphism of G with centralizer $C_G(\tau) \cong \mathrm{Sp}_{2n}(q)$. Also, let $x = \mathrm{diag}\,(a, 1, \ldots, 1)$ for some $1 \neq a \in \mathbb{F}_q^\times$, so that $C_G(x)$ is the stabilizer of a pair (L, H), where L is a line and H is a hyperplane not containing L in V.

First we show that $G = C_G(\tau)C_G(x)$; equivalently, $C_G(\tau)$ is transitive on such pairs (L, H). Since $\mathrm{Sp}_{2n}(q)$ is transitive on nonzero vectors, we just have to show that the stabilizer of L in $C_G(\tau)$ is transitive on the hyperplanes complementary to L. Let H_i, $i = 1, 2$, be fixed hyperplanes complementary to L. Let $0 \neq v \in L$. Choose $v_i \in L_i := H_i^\perp$ with $(v_i, v) = 1$. Set $M_i = \langle L, L_i \rangle$. Note that $V = M_i \perp H_i'$ where $H_i' = L_i^\perp \cap H_i$ is a hyperplane in $L^\perp$ not containing L. By Witt's theorem for alternating forms, there is an isometry $g \in G$ such that $gM_1 = M_2$ and $gH_1 = H_2$. So we may assume that $M_1 = M_2$. Applying another isometry, we may assume that $L_1 = L_2$ whence $H_1 = H_2$ as required.

It follows that $\tau^A x^A = (\tau x)^A$ with $A := \langle G, \tau \rangle$. The same also holds in the almost simple group $A/Z(G) \leq \mathrm{Aut}(\mathrm{L}_n(q))$.

Of course this also works for the algebraic group (or indeed over any field of size greater than 2).

Here is another example.

Example 7.3. Let L be a nontrivial finite group and H a cyclic group of order $n > 1$. Set $G = L \wr H$. Let $1 \neq a$ be an element of L^n with only one nontrivial coordinate. Let b be a generator for H. Note that $C_G(a) \geq L^{n-1}$ while $C_G(b) = D \times H$ where D is a diagonal subgroup of L^n. Thus $G = C_G(a)C_G(b)$ and $a^G b^G = (ab)^G$.

In particular, we can take $n = 2$, L simple non-abelian and choose a and b to be involutions or $n = p$ a prime and L simple of order divisible by p and choose a and b to have order p. Note that since G is transitive on $a^G \times b^G$, we see that $\langle a^x, b^y \rangle$ is always a p-group.

We give one more example to show that $a^G b^G = (ab)^G$ does not necessarily imply that $G = C_G(a)C_G(b)$.

Example 7.4. Let G be a group with a normal subgroup N. Suppose that $a, b \in G$ are such that all elements in abN are conjugate. Assume that G/N is abelian. Then clearly, $a^G b^G = (ab)^G = abN$ (the condition that G/N is abelian can be relaxed). Such examples include $\mathfrak{A}_4$ and non-abelian groups of order qp where $p < q$ are odd primes with a, b classes of p-elements with b not conjugate to a^{-1}.

8. Variations on Baer–Suzuki

Recall that the Baer–Suzuki theorem asserts that if G is a finite (or linear) group, $x \in G$, then $\langle x^G \rangle$ is nilpotent if and only if $\langle x, x^g \rangle$ is nilpotent for all $g \in G$. One might ask what happens if we assume that $\langle x, y^g \rangle$ is nilpotent (or solvable) for all $g \in G$ for x, y not necessarily conjugate elements. The examples in Section 7 show that this analog of the Baer–Suzuki theorem fails for nonconjugate elements (and indeed even the solvable version of Baer–Suzuki fails — see [13]). As we have seen for $p = 2, 3$, we even have counterexamples for simple algebraic groups (and so also for finite simple groups).

However, it turns out that one can extend the Baer–Suzuki theorem with appropriate hypotheses at least for p-elements with $p \geq 5$ (see Theorem 8.8 below).

8.1. **Some variations on Baer–Suzuki for simple groups.** First we note that in Theorem 4.6 there are no exceptions if $p > 3$. Moreover, the same proof (basically reducing to the case of rank 1 groups) gives the following:

Corollary 8.1. *Let G be a finite simple group of Lie type in characteristic $p \geq 5$. Let u, w be nontrivial unipotent elements of G. There exists $g \in G$ such that uw^g is not unipotent and $\langle u, w^g \rangle$ is not solvable.*

Guest [13] proved that if G is a finite group with $F(G) = 1$ and $x \in G$ has prime order $p \geq 5$, then $\langle x, x^g \rangle$ is not solvable for some $g \in G$. See also [10].

Next we record the following results for alternating and sporadic groups.

Lemma 8.2. *Let $G = \mathfrak{A}_n$, $n \geq 5$. Let p be a prime with $p \geq 3$. If $u, w \in G$ are nontrivial p-elements, then there exists $g \in G$ such that uw^g is not a p-element and $\langle u, w^g \rangle$ is nonsolvable.*

Proof. First take $p = 3$. By induction, it suffices to consider the case $n = 5$ or 6 where the result is clear. So assume that $p \geq 5$. Clearly, it suffices to consider the case $p = n$, where again the result is clear. □

Lemma 8.3. *Let G be a sporadic simple group. Let p be a prime. Let $u, w \in G$ be nontrivial p-elements. Then*

(a) *there exists $g \in G$ such that uw^g is not a p-element; and*
(b) *if $p \geq 5$, there exists $g \in G$ such that $\langle u, w^g \rangle$ is not solvable.*

Proof. These are straightforward computations using GAP. □

8.2. **A variation on Baer–Suzuki for almost simple groups.** Our next goal is to prove the following:

Theorem 8.4. *Let $p \geq 5$ be a prime and let S be a finite non-abelian simple group. Let $S \lhd G \leq \mathrm{Aut}(S)$, and $c, d \in G$ any two elements of order p. Then:*

(a) *There is some $g \in G$ such that $\langle c, d^g \rangle$ is not solvable.*
(b) *There is some $g \in G$ such that cd^g is not a p-element.*

If S is an alternating group or a sporadic group, we apply Lemmas 8.2 and 8.3. So assume that S is of Lie type in characteristic r. In what follows, we will call any element of G inducing a nontrivial field automorphism of S modulo $\mathrm{Inndiag}(S)$, the subgroup of inner-diagonal automorphisms of S, *a field automorphism*. Also, $\Phi_m(t)$ denotes the mth-cyclotomic polynomial in the variable t.

8.2.1. *The case $r = p$.* If c, d are both inner elements, then the result follows by Corollary 8.1. So assume that c induces a field automorphism of S. Suppose that S has rank at least 2. Let P be a maximal end node parabolic subgroup of S with d not in the radical Q of P. Note that $N_G(P)$ contains a Sylow p-subgroup of G and so we may assume that $c, d \in N_G(P)$. Since $p \geq 5$, it follows that P/Q has a unique simple section S_0 and that c, d each act nontrivially on S_0, whence the result follows by induction.

If S has rank 1, then either $S \cong \mathrm{L}_2(q)$ or $\mathrm{U}_3(q)$. Write $q = q_0^p$. Since $p \geq 5$, it follows [11, 7.2] that there is a unique conjugacy class of subgroups of field automorphisms of order p and that every unipotent element is conjugate to an element of the group defined over $\mathbb{F}_{q_0}$. Thus, we see conjugates of c, d in $H := \mathrm{L}_2(q_0) \times \langle c \rangle$ or $\mathrm{U}_3(q_0) \times \langle c \rangle$. Note that c is conjugate in G to a non-central element in H (again by [11, 7.2]) and so the result follows by induction.

For the rest of the section, we assume that $r \neq p$.

8.2.2. *Field automorphisms.* Here we handle the case when c is a field automorphism of order p of S. So we can view $S = S(q)$ as a group over the field of q elements with $q = q_0^p$. One can find a simple algebraic group $\mathbf{G}$ of adjoint type over $\overline{\mathbb{F}}_r$ and a Steinberg endomorphism $F : \mathbf{G} \to \mathbf{G}$ such that $X = X(q) := \mathbf{G}^{Fp}$ is the group of inner-diagonal automorphisms of S. By [11, 7.2], any two subgroups of G of order p of field automorphisms of S are conjugate via an element of $X(q)$. In particular, this implies that any field automorphism normalizes a parabolic subgroup of any given type. Thus, precisely as in the case $r = p$, if d is also a field automorphism, we can reduce to the case that S has rank 1 and complete the proof.

Thus, we may assume that d is semisimple. Moreover, since $d^S = d^X$, it suffices to work with X-classes and as noted there is a unique conjugacy class of subgroups of order p consisting of field automorphisms. We digress to mention two results about p-elements.

Lemma 8.5. *Let $\mathbf{H}$ be a connected reductive algebraic group over $\overline{\mathbb{F}}_r$, with a Steinberg endomorphism $F : \mathbf{H} \to \mathbf{H}$, and let $p \neq r$ be a prime not dividing the order of the Weyl group W of $\mathbf{H}$ nor the order of the automorphism of W induced by F. Then the Sylow p-subgroups of $\mathbf{H}^F$ and $\mathbf{H}^{Fp}$ are abelian of the same rank.*

Proof. Under our assumptions, by [33, Thm. 25.14] the Sylow p-subgroups of $\mathbf{H}^{F^i}$ are homocyclic abelian, of rank s_i say. Moreover, there is at most one cyclotomic polynomial Φ_{e_i} dividing the order polynomial of $(\mathbf{H}, F^i)$ such that $p | \Phi_{e_i}(q^i)$, where q denotes the absolute value of the eigenvalues of F on the character group of an F-stable maximal torus of $\mathbf{H}$, and s_i equals the Φ_{e_i}-valuation of the order polynomial. Now $p | \Phi_e(q)$ if and only if $p | \Phi_{ep}(q)$, and if Φ_e divides the order polynomial of $(\mathbf{H}, F)$ then Φ_{ep} divides the one of $(\mathbf{H}, F^p)$, to the same power. Thus, $e_p = pe_1$ and $s_p = s_1$, and the claim follows. □

Note that in our situation the previous result says that if $p \geq 5$ does not divide the order of the Weyl group W, then every element in S of order p is conjugate to an element centralized by F. We can extend this even to some primes dividing $|W|$.

Lemma 8.6. *Let $\mathbf{H}$ be a simple simply connected linear algebraic group over $\overline{\mathbb{F}}_r$, with a Steinberg endomorphism $F : \mathbf{H} \to \mathbf{H}$. Let $\mathbf{T}$ be an F-stable maximal torus of $\mathbf{H}$ and let $\delta > 0$ such that F^δ acts trivially on the Weyl group $N_{\mathbf{H}}(\mathbf{T})/\mathbf{T}$. If $x \in \mathbf{H}^{Fp}$ has order p, for some prime p with $\gcd(p, r\delta) = 1$, then x is conjugate in $\mathbf{H}^{Fp}$ to an element of $\mathbf{H}^F$.*

Proof. Since $\mathbf{H}$ is simply connected, centralizers of semisimple elements in $\mathbf{H}$ are connected. So it suffices to show that the $\mathbf{H}$-conjugacy class C of x is F-stable (see [33, Thm. 26.7]). Since $F^p(x) = x$, C is F^p invariant. Thus, it suffices to show that F^m fixes C for some m prime to p. By our assumption on δ, we may replace F by the standard Frobenius endomorphism F^δ. Let y be a conjugate of x in the maximal torus $\mathbf{T}$, so that $F(t) = t^q$ for all $t \in \mathbf{T}$. Thus, F fixes $\langle y \rangle$ and so F^{p-1} fixes y, whence C is F-stable. $\square$

Note that we may always choose $\mathbf{T}$ so that $\delta \leq 3$. Note also that the proof goes through verbatim if we only assume that $\mathbf{H}$ is reductive and that the derived group is simply connected with fewer than p simple factors.

Returning to the proof of Theorem 8.4 we see in particular, if p does not divide the order of the center of the simply connected algebraic group $\mathbf{H}$ in the same isogeny class with $\mathbf{G}$, this shows that d is conjugate to an element of $X(q_0)$ (and since the centralizer of d covers $X(q)/S(q)$, this conjugation is via an element of $S(q)$). Next we claim that some conjugate of c normalizes but does not centralize some conjugate of $X(q_0)$. Since any two subgroups of field automorphisms of order p are conjugate via an element of $X(q)$, it follows that $c^{X(q)} \cap X(q_0)$ consists of more than one conjugacy class. Therefore c has more than one fixed point on $X(q)/X(q_0)$, whence the result. Thus, choosing some subgroup Y of $X(q)$ with $Y \cong S(q_0)$, we may assume that each of c and d normalizes but does not centralize $S(q_0)$, whence the result follows by induction.

So we will only need to consider field automorphisms in the case that $S = \mathrm{U}_n(q)$ or $\mathrm{L}_n(q)$ with p dividing n, and these cases will be handled in the next subsection.

8.2.3. *Classical groups.* A) We first handle the case where $S = \mathrm{L}_p^\epsilon(q)$ with p dividing $q - \epsilon 1$ and c is an irreducible p-element. In particular, c is semisimple regular. First suppose that d is semisimple. By a minor variation of Gow's result [12], we see that cd^g can be any regular semisimple element of G in the coset cdS. In particular, cd^g need not be a p-element. By choosing cd^g to have order as large as possible in the torus acting irreducibly on a hyperplane, we see that $\langle c, d^g \rangle$ need not be solvable (for example, using the main result of [17]).

Suppose now that d is a field automorphism, and let T be a maximally split torus of S. Then $N_G(T)$ contains a Sylow p-subgroup of G. Note that $N_G(T)/C_G(T) \cong \mathfrak{S}_p$ and both c and d are conjugate to elements in $N_G(T) \setminus C_G(T)$ (this is obvious for c, and for d we can apply [11, 7.2]). Hence the result follows by applying Lemma 8.2 to $N_G(T)/C_G(T)$.

B) Now let S be any (simple) classical group with natural module V of dimension e defined over $\mathbb{F}_{q_1}$. By our earlier results, it suffices to assume that c is semisimple and d is either a field automorphism or a semisimple element. Moreover, since c^S is invariant under all diagonal automorphisms, by the remark above, we can work with any conjugacy class of field automorphisms of order p.

Let m be the dimension of an irreducible module for an element of order p. Then the case where $p = m$ and m is the order of q_1 modulo p has already been treated in A). Note that every semisimple element of order p stabilizes an m-dimensional subspace W that is either nondegenerate or totally singular (furthermore, the type is independent of the element).

Suppose that W is totally singular. Then we may assume that c, d both normalize the stabilizer of W. If $m = 1$, then c, d both normalize the stabilizer of a singular 1-space and

the result follows by induction. So assume that $m > 1$. As W is totally singular, then by construction, we see that c, d induce nontrivial automorphisms on $\mathrm{GL}(W)$ (and since $p \geq 5$, $\mathrm{SL}(W)$ is quasisimple), whence the result follows by induction.

Suppose that W is nondegenerate. The same argument applies unless the stabilizer of W is not essentially simple. This only happens if $m = 2$ and S is an orthogonal group (and so we may assume that $e \geq 7$). In this case, we see that c, d will each stabilize a nondegenerate space of the same type of either dimension 4 or 6 and we argue as above.

8.2.4. *Exceptional groups.* By the results above, we may assume that c, d are both semisimple elements in S of order p (with $p \geq 5$). We may also assume that P is not cyclic (since that case is handled by [18] and [13]). In particular, the result follows for $S = {}^2B_2(q^2)$ or ${}^2G_2(q^2)$ since there P is always cyclic.

If $S = {}^2F_4(2)'$, the result follows by a straightforward computation (the only prime to consider is $p = 5$). Suppose that $S = {}^2F_4(q^2)$, $q^2 > 2$. It follows by [30] that P will either be contained in a subgroup ${}^2B_2(q^2) \wr 2$ or $\mathrm{Sp}_4(q^2)$. In either case, we see that conjugates of c, d will normalize but not centralize a simple subgroup and the result follows by induction.

Suppose $S = G_2(q)$. Since $p \geq 5$ and P is non-cyclic, we see that $p|(q^2 - 1)$ and $q \geq 4$. Now we can embed P in a subgroup $R \cong \mathrm{SL}_3(q)$ or $\mathrm{SU}_3(q)$ of S and apply the previous results to R.

Next suppose that $S = {}^3D_4(q)$. If $p|(q^2 - 1)$, then we can argue as in the case of $G_2(q)$. The remaining cases are when p divides $\Phi_3(q)$ or $\Phi_6(q)$. One cannot find a good overgroup in these cases, but using Chevie, we see that $c^G d^G$ hits any regular element in a torus of order dividing $\Phi_{12}(q)$. In particular, cd^g need not be a p-element. By considering the maximal subgroups [21], it also follows that $S = \langle c, d^g \rangle$ for some g.

The standing hypothesis for the rest of this subsection is the following:

- S is a simple exceptional Lie-type group, of type F_4, E_6, ${}^2E_6$, E_7, or E_8, over $\mathbb{F}_q$;
- c and d are semisimple p-elements in S and the Sylow p-subgroups of S are not cyclic.

Slightly changing the notation, we will view $S = S(q)$ as $(\mathbf{G}^F)'$, where $\mathbf{G}$ is a simple algebraic group of adjoint type over $\overline{\mathbb{F}}_q$ with a Steinberg endomorphism $F : \mathbf{G} \to \mathbf{G}$, and W is the Weyl group of $\mathbf{G}$.

The basic idea to prove Theorem 8.4 for S is the following:

Lemma 8.7. *Assume Theorem 8.4 holds for all non-abelian simple groups of order less than $|S|$. To prove Theorem 8.4 for semisimple elements $c, d \in S$, it suffices to find a subgroup $D < S$ with the following properties:*

(a) *$D = D_1 \circ \ldots \circ D_t$ is a central product of $t \leq 3$ quasisimple subgroups D_i with p coprime to $|Z(D)|$;*
(b) *each S-conjugacy class of elements of order p intersects D; and*
(c) *either $N_S(D)$ acts transitively on $\{D_1, \ldots, D_t\}$, or $t = 2$ and an S-conjugate of D_1 is contained in D_2.*

Proof. 1) By (b), we may assume that $c, d \in D$. Suppose that there is some j such that neither c nor d centralizes D_j. Then we can embed c and d in the almost simple group $N_D(D_j)/C_D(D_j)$ with socle $D_j/Z(D_j)$. Since Theorem 8.4 holds for $D_j/Z(D_j)$, we are done.

2) Since $p \not| |Z(D)|$, we are done if $t = 1$. Suppose $t = 2$. In view of 1) we may assume that $c \in C_D(D_1) = Z(D)D_2$ (in particular, c does not centralize D_2 and $c \in D_2$ since $p \not| |Z(D)|$). Now if d does not centralize D_2, we are also done. So we may assume that $d \in C_D(D_2) = Z(D)D_1$, whence $d \in D_1$. By the assumptions, there is some $s \in S$ such that $d^s \in D_2$. Now we can apply Theorem 8.4 to the images of c and d^s in $D_2/Z(D_2)$.

Finally suppose that $t = 3$. As above, we may assume that $c \in E := D_2 \circ D_3$. If d does not centralize E, then we can embed both c and d in $N_D(E)/C_D(E)$ and repeat the $t = 2$ argument. On the other hand, if $d \in C_D(E) = Z(D)D_1$, then $d \in D_1$ and some S-conjugate d^s lies in $D_2 < E$, and so d^s does not centralize E. Hence we are again done. □

The rest of this subsection is to produce a subgroup D satisfying the conditions set in Lemma 8.7. In the following table we list such a subgroup D. In all cases but the lines with $D = F_4(q)$, D is taken from [24, Table 5.1], so that $N_S(D)$ is a subgroup of maximal rank. In all cases, we choose e smallest possible such that $p|\Phi_e(q)$, and list the largest power Φ_e^l that divides the order polynomial of $(\mathbf{G}, F)$. According to [33, Thm. 25.11], $\mathbf{G}^F$ has a unique conjugacy class of tori T of order $\Phi_e^l(q)$. Moreover, by [40, Lemma 4.5], every p-element of $\mathbf{G}^F$ of order at most the p-part of $\Phi_e(q)$ is conjugate to an element in T. In all cases, we choose D so that it contains a $\mathbf{G}^F$-conjugate of T and p is coprime to $|Z(D)|$. Also, all the Lie-type groups appearing in the third column are *simple* non-abelian (here we are slightly abusing the notation, using $E_6(q)$ and ${}^2E_6(q)$ to denote their non-abelian composition factors).

$\mathbf{G}^F$	Φ_e^l	D
$F_4(q)$	Φ_1^4, Φ_2^4, or Φ_4^2	$Z_{(2,q-1)} \cdot \mathrm{O}_9(q)$
	Φ_3^2 or Φ_6^2	${}^3D_4(q)$
$E_6(q)$	Φ_1^6	$Z_{(2,q-1)} \cdot (\mathrm{L}_2(q) \times \mathrm{L}_6(q))$
	Φ_2^4, Φ_4^2, or Φ_6^2	$F_4(q)$
	Φ_3^3	$Z_{(3,q-1)} \cdot (\mathrm{L}_3(q) \times \mathrm{L}_3(q) \times \mathrm{L}_3(q))$
${}^2E_6(q)$	Φ_1^4, Φ_3^2, or Φ_4^2	$F_4(q)$
	Φ_2^6	$Z_{(2,q-1)} \cdot (\mathrm{L}_2(q) \times \mathrm{U}_6(q))$
	Φ_6^3	$Z_{(3,q+1)} \cdot (\mathrm{U}_3(q) \times \mathrm{U}_3(q) \times \mathrm{U}_3(q))$
$E_7(q)$	Φ_1^7 or Φ_4^2	$Z_{(4,q-1)/(2,q-1)} \cdot \mathrm{L}_8(q)$
	Φ_2^7	$Z_{(4,q+1)/(2,q-1)} \cdot \mathrm{U}_8(q)$
	Φ_3^3	$Z_{(3,q-1)} \cdot E_6(q)$
	Φ_6^3	$Z_{(3,q+1)} \cdot {}^2E_6(q)$
$E_8(q)$	Φ_1^8, Φ_2^8, Φ_4^4, or Φ_8^2	$Z_{(2,q-1)} \cdot \mathrm{O}_{16}^+(q)$
	Φ_3^4	$Z_{(3,q-1)} \cdot (\mathrm{L}_3(q) \times E_6(q))$
	Φ_5^2	$Z_{(5,q-1)} \cdot (\mathrm{L}_5(q) \times \mathrm{L}_5(q))$
	Φ_6^4	$Z_{(3,q+1)} \cdot (\mathrm{U}_3(q) \times {}^2E_6(q))$
	Φ_{10}^2	$Z_{(5,q+1)} \cdot (\mathrm{U}_5(q) \times \mathrm{U}_5(q))$
	Φ_{12}^2	${}^3D_4(q^2)$

To check the condition (3) of Lemma 8.7, we need to work with the extended Dynkin diagram of $\mathbf{G}$. Fix an orthonormal basis $(e_1, \ldots, e_8)$ of the Euclidean space $\mathbb{R}^8$ and let

$$\alpha_1 = (e_1 + e_8 - \sum_{i=2}^{7} e_i)/2,\ \alpha_2 = e_2 + e_1,\ \alpha_i = e_{i-1} - e_{i-2}\ (3 \le i \le 8),\ \alpha_8' = -e_8 - e_7,$$

so that $\alpha_1, \ldots, \alpha_j$ are the simple roots of the root system of type E_j, $6 \le j \le 8$, and $(\alpha_1, \ldots, \alpha_8, \alpha_8')$ forms the extended Dynkin diagram $E_8^{(1)}$ of type E_8. Also, let α_6' be chosen such that $(\alpha_1, \ldots, \alpha_6, \alpha_6')$ forms the extended Dynkin diagram $E_6^{(1)}$ of type E_6.

Certainly, the condition (3) in Lemma 8.7 needs to be verified only when D is not quasisimple. These cases are considered below, where we will construct certain explicit automorphisms of the Dynkin diagram.

• $\mathbf{G}^F = E_6(q)$. Let ω denote a graph automorphism of order 3 of $E_6^{(1)}$. Observe that it is induced by an element of W, whence by some element $s \in S$. If D is of type $A_1 + A_5$, then ω sends α_6' to α_1 or α_5, and so it sends the A_1-subgroup D_1 to a subgroup of the A_5-subgroup D_2. If D is of type $3A_2$, then ω permutes the three A_2-subgroups D_i of D cyclically.

• $\mathbf{G}^F = {}^2E_6(q)$. Let τ denote the unique graph automorphism of order 2 of the Dynkin diagram E_6 (which also acts on $E_6^{(1)}$), so that $\mathbf{G}^F$ is constructed using τ. If D is of type $A_1 + {}^2A_5$, then certainly the A_1-subgroup D_1 (corresponding to α_6') is S-conjugate to the A_1-subgroup labeled by α_4 of the ${}^2A_5$-subgroup D_2. Assume now that D is of type $3({}^2A_2)$. Observe that τ is central in a Sylow 2-subgroup of the full automorphism group $Z_2 \times W$ of the root system of type E_6. Hence it commutes with a W-conjugate of γ, the automorphism that interchanges α_1 with α_3, α_5 with α_6, and α_2 with α_6'. So without loss we may assume D is constructed using this particular graph automorphism γ. In this case, the order 3 automorphism ω commutes with γ and permutes the three ${}^2A_2$-subgroups D_i of D cyclically.

• $\mathbf{G}^F = E_8(q)$. If D is of type $A_2 + E_6$, then certainly the A_2-subgroup D_1 (corresponding to α_8 and α_8') is S-conjugate to the A_2-subgroup labeled by α_1 and α_3 of the E_6-subgroup D_2. Assume now that D is of type ${}^2A_2 + {}^2E_6$. One can check that D can be constructed using the element

$$\beta\ :\ \alpha_1 \leftrightarrow \alpha_6,\ \alpha_2 \mapsto \alpha_2,\ \alpha_3 \leftrightarrow \alpha_5,\ \alpha_4 \mapsto \alpha_4,\ \alpha_7 \mapsto e_6 + e_7,\ \alpha_8 \leftrightarrow \alpha_8'$$

in W; in particular, β fixes α_6'. Applying the previous case to $D_2 \cong {}^2E_6(q)$, we see that D_2 contains a ${}^2A_2$-subgroup (labeled by α_5 and α_6). The latter is S-conjugate to D_1, the ${}^2A_2$-subgroup labeled by α_8 and α_8', via conjugation by the element

$$\delta\ :\ e_1 \mapsto e_1,\ e_2 \mapsto e_2,\ e_3 \leftrightarrow e_8,\ e_4 \leftrightarrow -e_7,\ e_5 \leftrightarrow -e_6$$

in W, and so we are done.

Next, observe that the element

$$\begin{aligned}\varphi\ :\ & \alpha_1 \mapsto \alpha_6 \mapsto \alpha_2 \mapsto \alpha_8' \mapsto \alpha_1,\ \alpha_3 \mapsto \alpha_7 \mapsto \alpha_4 \mapsto \alpha_8 \mapsto \alpha_3,\\ & \alpha_5 \mapsto (-e_1 - e_2 - e_3 + e_4 + e_5 + e_6 - e_7 + e_8)/2\end{aligned}$$

in W interchanges the two A_4-components of $E_8^{(1)}$, and φ^2 induces the graph automorphism of each of these A_4-component. Since F acts trivially on $E_8^{(1)}$, we now see that φ

interchanges the two A_4-subgroups D_i if D is of type $2A_4$, and φ interchanges the two ${}^2A_4$-subgroups D_i if D is of type $2({}^2A_4)$.

We have therefore completed the proof of Theorem 8.4.

8.3. **Further variations on Baer–Suzuki.** We can now prove:

Theorem 8.8. *Let $p \geq 5$ be prime. Let G be a finite group. Let C, D be conjugacy classes of G with $G = \langle C \rangle = \langle D \rangle$. If $c^i d^j$ is a p-element for all $(c, d) \in C \times D$ and all integers i, j, then G is a cyclic p-group.*

Proof. First note that a p-group generated by a single conjugacy class is cyclic (pass to the Frattini quotient to see that the Frattini quotient of G and so G are cyclic). Consider a minimal counterexample (G, C, D).

We claim that G has a unique minimal normal subgroup N. If N_1 and N_2 are distinct minimal normal subgroups, then by minimality, G/N_i is a p-group for each i, whence G is a p-group, whence the claim.

By induction, G/N is a cyclic p-group. If N is a p-group, then so is G and the result follows. Assume that N is an elementary abelian r-group for some prime $r \neq p$, and let P be a Sylow p-subgroup of G. Choose $c, d \in P$, whence $d = c^i$ for some i. Since N is the unique minimal normal subgroup of G and $G/N = \langle dN \rangle$, d acts irreducibly and nontrivially on N. It follows that $d^N = dN$. In particular, we can find $x, y \in N$ such that $d^x = dy \neq d$. Now $c^{-i} d^x = y$ is not a p-element, a contradiction.

So N is a direct product of copies of a non-abelian simple group L. Replacing C and D by C^q and D^q, we may assume that $|G/N| = p$. If N is simple, then G is almost simple and Theorem 8.4(b) applies. So we may assume that N is a direct product $L_1 \times \cdots \times L_p$ and that an element of C or D conjugates L_i to L_{i+1} for $1 \leq i < p$. Replacing the elements of D by a power prime to p, we may assume that $CD \subset N$. Choose $(c, d) \in C \times D$. Write $c = (x_1, \ldots, x_p)\rho$ where $x_i \in \mathrm{Aut}(L_i)$ and $\rho \in \mathrm{Aut}(N)$ permuting the L_i in a cycle. So $d = \rho^{-1}(y_1, \ldots, y_p)$ with $y_i \in \mathrm{Aut}(L_i)$. Choosing $h = (z, 1, \ldots, 1) \in N$ with z running over L, we see that $cd^h \in N$, whose first coordinate is equal to $x_1 y_1 z$ and so it also runs over L. In particular cd^h need not be a p-element for all $h \in N$. □

We now want to weaken the hypothesis that $G = \langle C \rangle = \langle D \rangle$ in Theorem 8.8. To do so, we have to weaken slightly the conclusion.

We first need the following result:

Lemma 8.9. *Let $p \geq 3$ be prime. Let G be a finite group with a Sylow p-subgroup P and a normal p-complement N. Assume that $P = \langle C \rangle = \langle D \rangle$ for $C, D \subset P$, and that $\langle c^x, d \rangle$ is a p-group for all $x \in N$ and $(c, d) \in C \times D$. Then $G = N \times P$.*

Proof. Observe that the hypotheses imply that $N = C_N(c)C_N(d)$ for all $(c, d) \in C \times D$. Indeed, for all $x \in N$ we have that $\langle c^x, d \rangle$ is a p-group. Thus, there exists $y \in N$ with $c^{xy}, d^y \in P$. Since $N \cap P = 1$, it follows that $y \in C_N(d)$ and $xy \in C_N(c)$, whence $x \in C_N(c)C_N(d)$.

By way of contradiction, assume that $[P, N] \neq 1$. Note that if R is a Sylow r-subgroup of N, then $G = N_G(R)N$, whence $N_G(R)$ contains a Sylow p-subgroup of G. Thus, P normalizes a Sylow r-subgroup R of G for each prime divisor r of $|N|$. So for some r, P does not centralize R. Thus, without loss we may assume that N is an r-group for some

prime r. By passing to a quotient, we may first assume that N is elementary abelian and then that P acts irreducibly and nontrivially on N.

Now view N as an absolutely irreducible $\mathbb{F}P$-module where $\mathbb{F} := \mathrm{End}_P(N)$. We can extend scalars and work over an algebraically closed field. So $N = \mathrm{Ind}_M^P(W)$ for some irreducible M-module W with M a maximal subgroup of P. Since P/M is cyclic and N is irreducible over P, we have that $N = W_1 \oplus \ldots \oplus W_p$ where the W_i are pairwise non-isomorphic irreducible M-modules. Choosing $c \in C \setminus M$, we see that c permutes the W_i transitively, whence $\dim C_N(c) \leq (\dim N)/p$.

Thus we have found $c \in C$ with $\dim_{\mathbb{F}_r} C_N(c) \leq (\dim_{\mathbb{F}_r} N)/p$ and similarly for some $d \in D$. For this choice of (c, d), $|C_N(c)C_N(d)| \leq |N|^{2/p} < |N|$, a contradiction. □

We can now prove another variation on Baer–Suzuki, which is Theorem 1.9 in the introduction. Note that this includes the usual Baer–Suzuki theorem (for $p \geq 5$) by taking $C = D$.

Theorem 8.10. *Let G be a finite group and $p \geq 5$ prime. Let C and D be normal subsets of G such that $H := \langle C \rangle = \langle D \rangle$. If $\langle c, d \rangle$ is a p-group for all $(c, d) \in C \times D$, then $H \leq O_p(G)$.*

Proof. 1) Let G be a counterexample of minimal order. By minimality, $G = H$. By the usual argument, we see that G must have a unique minimal normal subgroup N. Let P be a Sylow p-subgroup of G.

By induction, G/N is a p-group, whence $G = NP$ and N is not a p-group. For any $c \in C$, since $\langle c \rangle$ is a p-subgroup, we can find $x \in N$ such that $c' := c^x \in C \cap P$. It follows that $Nc' = Ncx = N(cxc^{-1})c = Nc$, and so $c \in N\langle C \cap P \rangle$. Thus $G = N\langle C \cap P \rangle$, and similarly, $G = N\langle D \cap P \rangle$.

2) Suppose that N is a p'-group. Then $N \cap P = 1$ and $NP = N\langle C \cap P \rangle$ by 1), whence $P = \langle C \cap P \rangle$ and similarly, $P = \langle D \cap P \rangle$. Applying Lemma 8.9, we see that $P \lhd G$, a contradiction.

Thus we may assume that $N = L_1 \times \cdots \times L_t$ where $L_i \cong L$, a non-abelian simple group (of order divisible by p). Let $Q := P \cap N = Q_1 \times \cdots \times Q_t$ with $Q_i \leq L_i$, and let $T := N_G(Q) = XP$, where $X = X_1 \times \cdots \times X_t$ with $X_i := N_{L_i}(Q_i)$. By a result of Glauberman–Thompson [20, Thm. X.8.13] (see also [16]), it follows that $X_i \neq Q_i$.

Now consider $T/Q = (X/Q)(P/Q)$. Then $P/Q \cong G/N$ is generated by the images of $C \cap P$ and also by the images of $D \cap P$ by 1), and X/Q is a p'-group. So by Lemma 8.9 applied to T/Q, P/Q must centralize $X/Q \cong (X_1/Q_1) \times \cdots \times (X_t/Q_t)$. But $X_i \neq Q_i$ and P permutes the L_i, hence P must normalize each L_i. Since N normalizes each L_i, this implies that L_i is normal in $G = NP$. Recall that N is the unique minimal normal subgroup of H. Thus, we have shown that $N = L_1$ is simple and so G is almost simple. Now we have a contradiction by Theorem 8.4(a). □

There is a version of the previous result for linear groups.

Corollary 8.11. *Let k be a field of characteristic p with $p = 0$ or $p > 3$. Let G be a subgroup of $\mathrm{GL}_n(k)$. If C and D are normal unipotent subsets of G with $H := \langle C \rangle = \langle D \rangle$ such that $\langle c, d \rangle$ is unipotent for all $(c, d) \in C \times D$, then H is a normal unipotent subgroup of G.*

Proof. There is no harm in assuming that k is algebraically closed and that $G = H$. Since the condition that $\langle c, d\rangle$ is unipotent is a closed condition, it suffices to prove the result in the case where G, C and D are replaced by their Zariski closures. So $G = \mathbf{G}$ is an algebraic group. We may furthermore assume that the unipotent radical of $\mathbf{G}$ is trivial. In particular, the connected component $\mathbf{G}^\circ$ of $\mathbf{G}$ is reductive. By the result for finite groups, $\mathbf{G}/\mathbf{G}^\circ$ is a p-group (in particular if $p = 0$, $\mathbf{G}$ is connected). If $\mathbf{G}^\circ$ is trivial, the result follows. Let $\mathbf{B}$ be a Borel subgroup of $\mathbf{G}^\circ$ with unipotent radical $\mathbf{U}$. Then $N_{\mathbf{G}}(\mathbf{B})$ covers $\mathbf{G}/\mathbf{G}^\circ$. Let $\mathbf{P}$ be a maximal (necessarily closed) unipotent subgroup of $N_{\mathbf{G}}(\mathbf{B})$ (so $\mathbf{U} \leq \mathbf{P}$), and let $\mathbf{T}$ be a maximal torus of $\mathbf{B}$. Then $N_{\mathbf{G}}(\mathbf{B})/\mathbf{U} = \mathbf{T}.(\mathbf{P}/\mathbf{U})$. Note that $\mathbf{P}/\mathbf{U}$ is generated by $C\mathbf{U}/\mathbf{U}$ (as in our earlier arguments). For any $m \geq 1$ let $\mathbf{T}[m]$ be the m-torsion subgroup of $\mathbf{T}$. Note that $\mathbf{T}[m]$ is a finite group. Applying Lemma 8.9, it follows that $[\mathbf{P}, \mathbf{T}[m]] \leq \mathbf{U}$. Since $\mathbf{T}$ is the closure of its torsion subgroup, $[\mathbf{P}, \mathbf{T}] \leq \mathbf{U}$. Thus, $\mathbf{G}$ normalizes each simple component of $\mathbf{G}^\circ$ and so we are reduced to the almost simple case. However a simple algebraic group in characteristic $p \neq 2, 3$ has no outer automorphisms of order p and so $\mathbf{G}$ is simple. Now the result follows by Theorem 5.11. □

References

[1] E. Adan-Bante, H. Verrill, Symmetric groups and conjugacy classes. J. Group Theory **11** (2008), 371–379.

[2] Z. Arad, M. Herzog, *Products of Conjugacy Classes in Groups.* Lecture Notes in Math., 1112, Springer-Verlag, Berlin, 1985.

[3] C. Bessenrodt, A. S. Kleshchev, On Kronecker products of complex representations of the symmetric and alternating groups. Pacific J. Math. **190** (1999), 201–223.

[4] C. Bessenrodt, A. S. Kleshchev, Irreducible tensor products over alternating groups. J. Algebra **228** (2000), 536–550.

[5] J. Brundan, Double coset density in exceptional algebraic groups. J. London Math. Soc. (2) **58** (1998), 63–83.

[6] J. Brundan, Double coset density in classical algebraic groups. Trans. Amer. Math. Soc. **352** (2000), 1405–1436.

[7] R. W. Carter, *Finite Groups of Lie Type. Conjugacy Classes and Complex Characters.* Wiley Classics Library. John Wiley & Sons, Chichester, 1993.

[8] E. Fisman, Z. Arad, A proof of Szep's conjecture on nonsimplicity of certain finite groups. J. Algebra **108** (1987), 340–354.

[9] M. Geck, G. Hiss, F. Lübeck, G. Malle, G. Pfeiffer, CHEVIE – A system for computing and processing generic character tables for finite groups of Lie type, Weyl groups and Hecke algebras. Appl. Algebra Engrg. Comm. Comput. **7** (1996), 175–210.

[10] N. Gordeev, F. Grunewald, B. Kunyavskii, E. Plotkin, From Thompson to Baer-Suzuki: a sharp characterization of the solvable radical. J. Algebra **323** (2010), 2888–2904.

[11] D. Gorenstein, R. Lyons, *The Local Structure of Finite Groups of Characteristic 2 Type.* Mem. Amer. Math. Soc. **42** (1983), no. 276.

[12] R. Gow, Commutators in finite simple groups of Lie type. Bull. London Math. Soc. **32** (2000), 311–315.

[13] S. Guest, A solvable version of the Baer-Suzuki theorem. Trans. Amer. Math. Soc. **362** (2010), 5909–5946.

[14] R. M. Guralnick, M. W. Liebeck, D. MacPherson, G.M. Seitz, Modules for algebraic groups with finitely many orbits on subspaces. J. Algebra **196** (1997), 211–250.

[15] R. M. Guralnick, G. Malle, Classification of 2F-modules, II. Pp. 117–183 in: *Finite Groups 2003*, Walter de Gruyter, Berlin, 2004.
[16] R. M. Guralnick, G. Malle, G. Navarro, Self-normalizing Sylow subgroups. Proc. Amer. Math. Soc. **132** (2004), 973–979.
[17] R. M. Guralnick, T. Penttila, C. Praeger, J. Saxl, Linear groups with orders having certain large prime divisors. Proc. London Math. Soc. (3) **78** (1999), 167–214.
[18] R. M. Guralnick, G. R. Robinson, On extensions of the Baer–Suzuki theorem. Israel J. Math. **82** (1993), 281–297.
[19] R. M. Guralnick, J. Saxl, Generation of finite almost simple groups by conjugates. J. Algebra **268** (2003), 519–571.
[20] B. Huppert, N. Blackburn, *Finite Groups III*. Springer-Verlag, Berlin, New York, 1982.
[21] P. B. Kleidman, The maximal subgroups of the Steinberg triality groups ${}^3D_4(q)$ and of their automorphism groups. J. Algebra **115** (1988), 182–199.
[22] R. Lawther, The action of $F_4(q)$ on cosets of $B_4(q)$. J. Algebra **212** (1999), 79–118.
[23] R. Lawther, P-radical classes in simple algebraic groups and finite groups of Lie type. Preprint.
[24] M. W. Liebeck, J. Saxl, G. Seitz, Subgroups of maximal rank in finite exceptional groups of Lie type. Proc. London Math. Soc. **65** (1992), 297–325.
[25] M. W. Liebeck, G. Seitz, *Nilpotent and Unipotent Classes in Simple Algebraic Groups and Lie Algebras*. Amer. Math. Soc., Providence, RI, 2012.
[26] F. Lübeck, Charaktertafeln für die Gruppen $\mathrm{CSp}_6(q)$ mit ungeradem q und $\mathrm{Sp}_6(q)$ mit geradem q. Preprint 93-61, IWR Heidelberg, 1993.
[27] A. M. Macbeath, Generators of the linear fractional groups. Pp. 14–32 in: *Proc. Sympos. Pure Math.*, Vol. XII, Houston, Tex., Amer. Math. Soc., Providence, RI, 1967.
[28] K. Magaard, G. Malle, P. H. Tiep, Irreducibility of tensor squares, symmetric squares, and alternating squares. Pacific J. Math. **202** (2002), 379–427.
[29] K. Magaard, P. H. Tiep, Irreducible tensor products of representations of quasi-simple finite groups of Lie type. Pp. 239–262 in: *Modular Representation Theory of Finite Groups*, Walter de Gruyter, Berlin, 2001.
[30] G. Malle, The maximal subgroups of ${}^2F_4(q^2)$. J. Algebra **139** (1991), 52–69.
[31] G. Malle, G. Navarro, J.B. Olsson, Zeros of characters of finite groups. J. Group Theory **3** (2000), 353–368.
[32] G. Malle, J. Saxl, Th. Weigel, Generation of classical groups. Geom. Dedicata **49** (1994), 85–116.
[33] G. Malle, D. Testerman, *Linear Algebraic Groups and Finite Groups of Lie Type*. Cambridge Studies in Advanced Mathematics, 133, Cambridge University Press, 2011.
[34] J. Moori, H. Tong-Viet, Products of conjugacy classes in simple groups. Quaest. Math. **34** (2011), 433–439.
[35] G. Prasad, Weakly-split spherical Tits systems in pseudo-reductive groups. Preprint. arXiv: 1103.5970
[36] G. Seitz, Generation of finite groups of Lie type. Trans. Amer. Math. Soc. **271** (1982), 351–407.
[37] K. Shinoda, The conjugacy classes of Chevalley groups of type $(F4)$ over finite fields of characteristic 2. J. Fac. Sci. Univ. Tokyo Sect. I A Math. **2** (1974), 133–159.
[38] N. Spaltenstein, *Classes Unipotentes et Sous-Groupes de Borel*. Lecture Notes in Math., 946. Springer-Verlag, Berlin, 1982.
[39] T. Springer, Conjugacy classes in algebraic groups. Pp. 175–209 in: *Group Theory*, Beijing 1984, Lecture Notes in Math., 1185, Springer-Verlag, Berlin, 1986.
[40] A. E. Zalesski, The number of distinct eigenvalues of elements in finite linear groups. J. London Math. Soc. (2) **74** (2006), 361–378.
[41] I. Zisser, Irreducible products of characters in A_n. Israel J. Math. **84** (1993), 147–151.

Department of Mathematics, University of Southern California, Los Angeles, CA 90089-2532, USA
E-mail address: guralnic@usc.edu

FB Mathematik, TU Kaiserslautern, Postfach 3049, 67653 Kaiserslautern, Germany
E-mail address: malle@mathematik.uni-kl.de

Department of Mathematics, University of Arizona, Tucson, AZ 85721-0089, USA
E-mail address: tiep@math.arizona.edu