COMPOSITIO MATHEMATICA

Rational rigidity for $E_8(p)$

Robert Guralnick and Gunter Malle

Compositio Math. **150** (2014), 1679–1702.

doi:10.1112/S0010437X14007271

FOUNDATION
COMPOSITIO
MATHEMATICA

LONDON
MATHEMATICAL
SOCIETY

Compositio Math. 150 (2014) 1679–1702
doi:10.1112/S0010437X14007271

Rational rigidity for $E_8(p)$

Robert Guralnick and Gunter Malle

Abstract

We prove the existence of certain rationally rigid triples in $E_8(p)$ for good primes p (i.e. $p > 5$) thereby showing that these groups occur as Galois groups over the field of rational numbers. We show that these triples arise from rigid triples in the algebraic group and prove that they generate an interesting subgroup in characteristic zero. As a byproduct of the proof, we derive a remarkable symmetry between the character table of a finite reductive group and that of its dual group. We also give a short list of possible overgroups of regular unipotent elements in simple exceptional groups.

1. Introduction

The question of whether all finite groups occur as Galois groups over the field of rational numbers is still wide open. Even if one restricts to the case of finite non-abelian simple groups, only rather few types have been realized as Galois groups over $\mathbb{Q}$. These include the alternating groups, the sporadic groups apart from M_{23} and some families of groups of Lie type, but even over fields of prime order mostly with additional congruence conditions on the characteristic (see [MM99]). Zywina [Z13] has recently shown that $\mathrm{L}_2(p)$ is a Galois group over $\mathbb{Q}$ for all primes p.

In the present paper we show that the infinite series of simple groups $E_8(p)$ occur as Galois groups over $\mathbb{Q}$ for all good primes p.

Our paper was inspired by the recent result of Zhiwei Yun [Yu14] who showed the Galois realizability of $E_8(p)$ for all sufficiently large primes p, but without giving a bound. In fact, Yun proved much more: he showed that E_8 is a motivic Galois group, answering a conjecture of Serre.

Our proof relies on the well-known rigidity criterion of Belyi, Fried, Matzat and Thompson, but in addition uses deep results mainly of Liebeck and Seitz on maximal subgroups of algebraic groups and from Lusztig on the parametrization of irreducible characters of finite reductive groups, the Springer correspondence and computations of Green functions. We also require results of Lawther on fusion of unipotent elements in reductive subgroups.

Table 1 contains a description of the class triples in the algebraic groups $G(k)$ over an algebraically closed field k of good characteristic (the classes actually make sense as long as the characteristic is not two). Note that the centralizers of elements in these classes (in good characteristic) are connected and that they are defined over the prime field. Thus, we can view these classes over $G(q)$ as well. Here, the involution classes are identified by the structure of their centralizer in G, while the unipotent classes are denoted as in [Ca93, § 13.1].

Our first main result is the following theorem.

Theorem 1.1. *Let k be an algebraic closure of $\mathbb{F}_p$ with p prime. Let G be either $G_2(k)$ or $E_8(k)$. Assume that p is good for G (i.e. $p > 3$ and if $G = E_8$, $p > 5$). Let C_i, $1 \leqslant i \leqslant 3$, be the conjugacy classes described in Table 1. Let X denote the variety of triples in $C_1 \times C_2 \times C_3$ with product one. Then X is a single regular G-orbit and if $(x_1, x_2, x_3) \in X$, then $\langle x_1, x_2\rangle \cong G(\mathbb{F}_p)$.*

Received 5 July 2012, accepted in final form 8 November 2013, published online 17 July 2014.
2010 Mathematics Subject Classification 12F12, 20C33 (primary), 20E28 (secondary).
Keywords: inverse Galois problem, rigidity, Lie primitive subgroups, regular unipotent elements.

Table 1. Candidate classes.

	$G_2(k)$	$E_8(k)$	
C_1	$A_1+\tilde{A}_1$	D_8	Involution
C_2	$\tilde{A}_1$	$4A_1$	Unipotent
C_3	G_2	E_8	Regular unipotent

In particular, this gives an affirmative answer to [Yu14, Conjecture 5.16].

We also consider fields of characteristic zero. See § 6 for the details. Since $G(k)$ has a single regular orbit on X for k algebraically closed of good positive characteristic, it follows easily that the same is true if k is an algebraically closed field of characteristic zero and that X is also a single regular orbit. We also show that some (and so any) such triple generates a Zariski-dense subgroup of $G(k)$ when k is algebraically closed of characteristic zero.

Let $\mathbb{Z}_p$ denote the ring of p-adic integers. We can also produce such triples over $G(\mathbb{Z}_p)$ and so show the following result.

Theorem 1.2. *Let k be an algebraically closed field of characteristic zero. Let G be $G_2(k)$ or $E_8(k)$. Let C_i, $1 \leqslant i \leqslant 3$, be the conjugacy classes described in Table 1. Let X be the set of elements in $C_1 \times C_2 \times C_3$ with product one. For $x \in X$, let $\Gamma(x)$ denote the group generated by x.*

(i) *For any $x \in X$, $\Gamma(x)$ is Zariski dense in $G(k)$.*

(ii) *If k_0 is a subfield of k, then $X(k_0)$ is a single $G(k_0)$-orbit (where $G(k_0)$ is the split group over k_0).*

(iii) *Let m be the product of the bad primes for G (i.e. $m = 6$ in the first case and $m = 30$ for E_8) and set $R = \mathbb{Z}[1/m]$. There exists $x \in X(R)$ such that $\Gamma(x) \leqslant G(R)$ and surjects onto $G(R/pR)$ for any good prime p. In particular, $\Gamma(x)$ is dense in $G(\mathbb{Z}_p)$ for any good prime p.*

Theorem 1.1 implies the following result (answering the question of Yun for E_8).

Theorem 1.3. *Let C_1, C_2, C_3 be the conjugacy classes described in Table 1. The following hold:*

(i) *(C_1, C_2, C_3) is rationally rigid for $G_2(p)$, $p \geqslant 5$, and for $E_8(p)$, $p \geqslant 7$;*

(ii) *the finite simple groups $G_2(p)$ ($p \geqslant 5$ prime) and $E_8(p)$ ($p \geqslant 7$ prime), occur as (regular) Galois groups over $\mathbb{Q}(t)$;*

(iii) *for each p, there are infinitely many linearly disjoint Galois extensions of $\mathbb{Q}$ with Galois group $E_8(p)$, $p \geqslant 7$, and $G_2(p)$, $p \geqslant 5$.*

Remarks 1.4. (i) The case of $G_2(p)$ ($p \geqslant 5$) had already been shown by Feit–Fong [FF85] (for $p > 5$) and Thompson [Th85] (for $p = 5$). See also [DR10].

(ii) The second author had shown in 1986 that $F_4(p)$ is a Galois group over $\mathbb{Q}(t)$ whenever $p \geqslant 5$ has multiplicative order 12 modulo 13, and that $E_8(p)$ is a Galois group over $\mathbb{Q}(t)$ whenever $p \geqslant 7$ has multiplicative order 15 or 30 modulo 31 (see [MM99, Theorems II.8.5 and II.8.10]).

(iii) There are several possible choices of triples for F_4 including one suggested by Yun. Guralnick, Lübeck and Yu [GLY14] have recently shown that for Yun's triple, $F_4(p)$ is a regular Galois group over $\mathbb{Q}(t)$ for all $p > 3$ using the methods of this paper. On the other hand, in the final section, we do exhibit a rigid triple of conjugacy classes in $F_4(k)$ but any such triple generates a subgroup H of $F_4(p)$ with $H/O_p(H) \cong G_2(p)$ and $|O_p(H)| = p^{14}$.

https://doi.org/10.1112/S0010437X14007271 Published online by Cambridge University Press

(iv) See [LLM11] for an interesting rigid triple in G_2.

(v) We do not know whether $E_8(p)$ is a Galois group over $\mathbb{Q}$ for $p = 2, 3$ or 5. There are several issues that arise for bad primes. The first is that the character theory is much more difficult. The second is that the centralizer of a regular unipotent element in the algebraic group is no longer connected. For $p = 2$, the conjugacy class of involutions needs to be changed.

It is directly clear from the known classification of unipotent conjugacy classes (see, for example, [Ca93, 13.1]) that the classes C_2, C_3 are rational, and for class C_1 this is obvious. As usual, the proof of rigidity breaks up into two quite different parts: showing that all triples $(x_1, x_2, x_3) \in C_1 \times C_2 \times C_3$ with product $x_1x_2x_3 = 1$ do generate G, and showing that there is exactly one such triple modulo G-conjugation. The first statement will be shown in § 5, the second in § 2.

On the way we prove two results which may be of independent interest: in Theorem 2.5 we note a remarkable symmetry property between the character table of a finite reductive group and that of its dual, and in Theorem 3.4 we give a short list of possible Lie primitive subgroups of simple exceptional groups containing a regular unipotent element (in particular, there are none in characteristic larger than 113). Combining this with the result of Saxl and Seitz [SS97], we essentially know all proper closed subgroups of exceptional groups which contain regular unipotent elements.

The application of our approach to the other large exceptional groups of Lie type over prime fields fails due to the fact that for E_6 and E_7 the finite simple groups are not always the group of fixed points of a corresponding algebraic group. In particular, the class of regular unipotent elements in E_7 splits into two classes in the finite simple group, which are never rational over the prime field, when $p > 2$. In type E_6, again the class of regular unipotent elements splits, and our approach for controlling the structure constant does not yield the necessary estimates. Note that by a result of the second author the groups $E_6(p)$ and ${}^2E_6(p)$ are known to occur as Galois groups for all primes $p \geqslant 5$ which are primitive roots modulo 19 (see [MM99, Corollary II.8.8 and Theorem II.8.9]).

Note that, on the other hand almost all families of finite simple groups are known to occur as Galois groups over suitable (finite) abelian extensions of $\mathbb{Q}$, a notable exception being given by the series of Suzuki and Ree groups in characteristic two. An overview on most results in this area can be found in the monograph [MM99, § II.10].

2. Structure constants

In this section we derive estimates for certain structure constants. For this we need to collect various results on characters of finite groups of Lie type. We introduce the following set-up, where, in this section only, algebraic groups are denoted by boldface letters, in order to better distinguish them from their finite analogues. Let $\mathbf{G}$ be a connected reductive linear algebraic group over the algebraic closure of a finite field of characteristic p, and $F : \mathbf{G} \to \mathbf{G}$ a Steinberg endomorphism with (finite) group of fixed points $G := \mathbf{G}^F$. We write q for the common absolute value of all eigenvalues of F on the character group of an F-stable maximal torus of $\mathbf{G}$.

Fix an F-stable maximal torus $\mathbf{T}_0$ of $\mathbf{G}$. Then the G-conjugacy classes of F-stable maximal tori of $\mathbf{G}$ are naturally parametrized by F-conjugacy classes in the Weyl group $W = N_{\mathbf{G}}(\mathbf{T}_0)/\mathbf{T}_0$ of $\mathbf{G}$, that is, by W-classes in the coset $W\varphi$, where φ denotes the automorphism of W induced by F. If $\mathbf{T}$ is parametrized by the class of $w\varphi$, then $\mathbf{T}$ is said to be *in relative position* $w\varphi$ (with respect to $\mathbf{T}_0$). Note that in this case $N_G(\mathbf{T})/\mathbf{T}^F \cong C_W(w\varphi)$ (see [MT11, Proposition 25.3]).

https://doi.org/10.1112/S0010437X14007271 Published online by Cambridge University Press

For $\mathbf{T} \leqslant \mathbf{G}$ an F-stable maximal torus and $\theta \in \mathrm{Irr}(\mathbf{T}^F)$, Deligne and Lusztig defined a generalized complex character $R_{\mathbf{T},\theta}^{\mathbf{G}}$ of G. This character $R_{\mathbf{T},\theta}^{\mathbf{G}}$ only depends on the G-conjugacy class of $(\mathbf{T},\theta)$.

Its values on unipotent elements have the following property (see [Ca93, Corollary 7.2.9]).

Proposition 2.1. *Let $u \in G$ be unipotent. Then $R_{\mathbf{T},\theta}^{\mathbf{G}}(u)$ is independent of θ.*

Assume that $\mathbf{T}$ is in relative position $w\varphi$. Then we write $Q_{w\varphi}(u) := R_{\mathbf{T},\theta}^{\mathbf{G}}(u)$ for this common value. In this way each unipotent element $u \in G$ defines an F-class function $W \to \mathbb{C}$, $w \mapsto Q_{w\varphi}(u)$, on W, the so-called *Green function*. By Lusztig's algorithm (see [Lu86, § 24]), the values $Q_{w\varphi}(u)$ are expressible by polynomials in q, at least for good primes p, with q in fixed congruence classes modulo an integer $N_{\mathbf{G}}$ only depending on the root system of $\mathbf{G}$ and on φ. For q in a fixed congruence class modulo $N_{\mathbf{G}}$, we can thus write

$$Q_{w\varphi}(u) = \sum_{i \geqslant 0} \psi_i^u(w\varphi)\, q^i$$

for suitable class functions ψ_i^u on $W\varphi$, depending on u. (In fact, these ψ_i^u are known to be characters of $W\varphi$ when $C_{\mathbf{G}}(u)$ is connected.) We also need to understand the values of Deligne–Lusztig characters on semisimple elements. First observe the following vanishing result.

Lemma 2.2. *Let $H \leqslant \mathrm{Irr}(\mathbf{T}^F)$ be a subgroup, and $s \in \mathbf{T}^F$ semisimple such that no $\mathbf{G}^F$-conjugate lies in the kernel of all $\theta \in H$. Then*

$$\sum_{\theta \in H} R_{\mathbf{T},\theta}^{\mathbf{G}}(s) = 0.$$

Proof. According to [DM91, Lemma 12.16] we have

$$R_{\mathbf{T},\theta}^{\mathbf{G}}(s) \cdot \mathrm{St}(s) = \pm \mathrm{Ind}_{\mathbf{T}^F}^{\mathbf{G}^F}(\theta)(s),$$

where St denotes the Steinberg character of $\mathbf{G}^F$, and the sign only depends on $\mathbf{T}$, $\mathbf{G}$ and φ, not on θ. Thus,

$$\mathrm{St}(s) \sum_{\theta \in H} R_{\mathbf{T},\theta}^{\mathbf{G}}(s) = \pm \sum_{\theta \in H} \mathrm{Ind}_{\mathbf{T}^F}^{\mathbf{G}^F}(\theta)(s) = \pm \mathrm{Ind}_{\mathbf{T}^F}^{\mathbf{G}^F}\left(\sum_{\theta \in H} \theta\right)(s) = \pm \mathrm{Ind}_{\mathbf{T}^F}^{\mathbf{G}^F}(\gamma_H)(s),$$

where γ_H takes value $|H|$ on $\{t \in \mathbf{T}^F \mid \theta(t) = 1 \text{ for all } \theta \in H\}$ and zero otherwise. The claim follows since St does not vanish on semisimple elements by [DM91, Corollary 9.3]. □

Now let $\mathbf{G}^*$ be a group in duality with $\mathbf{G}$, with corresponding Steinberg endomorphism also denoted by F, and $\mathbf{T}_0^* \leqslant \mathbf{G}^*$ an F-stable maximal torus in duality with $\mathbf{T}_0$. There is a bijection between G-classes of pairs $(\mathbf{T},\theta)$ as above, and $G^* := \mathbf{G}^{*F}$-classes of pairs $(\mathbf{T}^*, t)$, where $\mathbf{T}^* \leqslant \mathbf{G}^*$ denotes an F-stable maximal torus and $t \in \mathbf{T}^{*F}$. Two pairs $(\mathbf{T}_1,\theta_1)$, $(\mathbf{T}_2,\theta_2)$ are called *geometrically conjugate* if under this bijection they correspond to pairs $(\mathbf{T}_1^*, t_1)$, $(\mathbf{T}_2^*, t_2)$ with G^*-conjugate elements t_1 and t_2 (see [Ca93, ch. 4]).

Proposition 2.3. *Let $s \in G$ be semisimple. Let $(\mathbf{T},\theta)$ be in the geometric conjugacy class of $t \in G^*$, where $\mathbf{T} \leqslant \mathbf{G}$ is in relative position $w\varphi$ with respect to a reference torus $\mathbf{T}_0$ inside $\mathbf{C} := C_{\mathbf{G}}^{\circ}(s)$. Let $W(s)$ denote the Weyl group of $\mathbf{C}$, $W(t)$ the Weyl group of $C_{\mathbf{G}^*}^{\circ}(t)$*

https://doi.org/10.1112/S0010437X14007271 Published online by Cambridge University Press

and $W_1 := C_{W(t)}(w\varphi)$. *Then*

$$R^{\mathbf{G}}_{\mathbf{T},\theta}(s) = |\mathbf{C}^F : \mathbf{T}^F|_{p'} \cdot \sum_{i=1}^{r} |W_1 : W_1 \cap W(s)^{u_i}| \cdot \theta(s^{u_i}),$$

where $u_1, \ldots, u_r \in W(s)\backslash W/W_1$ *are representatives for those double cosets such that* ${}^{u_i}(w\varphi) \in W(s)\varphi$.

Proof. By [DM91, Corollary 12.4] we have

$$R_{\mathbf{T},\theta}(s) = \frac{1}{|\mathbf{C}^F|} \sum_{\substack{g\in G\\ s\in {}^g\mathbf{T}^F}} R^{\mathbf{C}}_{{}^g\mathbf{T},{}^g\theta}(s).$$

Now $s \in ({}^g\mathbf{T})^F$ if and only if ${}^g\mathbf{T} \subseteq \mathbf{C}$. Let $(\mathbf{T}_1, \theta_1), \ldots, (\mathbf{T}_r, \theta_r)$ be a system of representatives of the $C := \mathbf{C}^F$-classes of G-conjugates of $(\mathbf{T}, \theta)$ with first component contained in $\mathbf{C}$. Let $N_G(\mathbf{T}, \theta) := \{g \in N_G(\mathbf{T}) \mid {}^g\theta = \theta\}$ denote the stabilizer of $(\mathbf{T}, \theta)$ in G, and similarly define $N_C(\mathbf{T}_i, \theta_i)$, the stabilizer of $(\mathbf{T}_i, \theta_i)$ in C. Then using $|N_G(\mathbf{T}_i, \theta_i)| = |N_G(\mathbf{T}, \theta)|$ the above formula can be rewritten as

$$R_{\mathbf{T},\theta}(s) = \sum_{i=1}^{r} \frac{|N_G(\mathbf{T}, \theta)|}{|N_C(\mathbf{T}_i, \theta_i)|} R^{\mathbf{C}}_{\mathbf{T}_i,\theta_i}(s).$$

Let $(\mathbf{T}_1^*, t_1), \ldots, (\mathbf{T}_r^*, t_r)$ be a system of representatives of the $\mathbf{C}^{*F}$-classes of G^*-conjugates of $(\mathbf{T}^*, t)$ with first component in $\mathbf{C}^*$. Write $w_i\varphi \in W(s)\varphi$ for the relative position of $\mathbf{T}_i^*$, and let $u_i \in W(s)\backslash W/W_1$ such that ${}^{u_i}(w\varphi, W(t)) = (w_i\varphi, W(t_i))$. Now $N_G(\mathbf{T}, \theta)$ is an extension of $\mathbf{T}^F$ by the subgroup of $N_G(\mathbf{T})/\mathbf{T}^F$ fixing θ, which under the above duality bijection is isomorphic to $C_W(w\varphi) \cap W(t) = W_1$. Similarly $N_C(\mathbf{T}_i, \theta_i)$ is an extension of $\mathbf{T}_i^F$ by the subgroup of $N_C(\mathbf{T}_i)/\mathbf{T}_i^F$ fixing θ_i, which is isomorphic to

$$C_{W(t_i)}(w_i\varphi) \cap W(s) = {}^{u_i}(W_1) \cap W(s) \cong W_1 \cap W(s)^{u_i}.$$

Since s lies in the centre of $\mathbf{C}$ we have

$$R^{\mathbf{C}}_{\mathbf{T}_i,\theta_i}(s) = R^{\mathbf{C}}_{\mathbf{T}_i,1}(1)\, \theta_i(s) = |\mathbf{C}^F : \mathbf{T}_i^F|_{p'} \cdot \theta_i(s),$$

where the first equality holds by [Ca93, Proposition 7.5.3]. The claim follows as $|\mathbf{T}_i^F| = |\mathbf{T}^F|$. □

We next compute some values of semisimple characters. For any semisimple element $t \in G^* = \mathbf{G}^{*F}$ there is an associated *semisimple character* χ_t of G, depending only on the G^*-class of t, defined as follows: let $W(t)$ denote the Weyl group of the centralizer $C^\circ_{\mathbf{G}^*}(t)$. Let $v\varphi \in W\varphi$ denote the automorphism of $W(t)$ induced by F. As explained above, to any pair $(\mathbf{T}^*, t)$ with $\mathbf{T}^* \leqslant C^\circ_{\mathbf{G}^*}(t)$ an F-stable maximal torus there corresponds by duality a pair $(\mathbf{T}, \theta)$ consisting of an F-stable maximal torus $\mathbf{T} \leqslant \mathbf{G}$ (in duality with $\mathbf{T}^*$) and $\theta \in \mathrm{Irr}(\mathbf{T}^F)$, up to G-conjugation. We then write $R^{\mathbf{G}}_{\mathbf{T}^*,t} := R^{\mathbf{G}}_{\mathbf{T},\theta}$. Then by [DM91, Definition 14.40] the semisimple character corresponding to t is given by

$$\chi_t = \pm \frac{1}{|W(t)|} \sum_{w\in W(t)} R^{\mathbf{G}}_{\mathbf{T}^*_{wv\varphi},t},$$

where $\mathbf{T}^*_{wv\varphi}$ denotes an F-stable maximal torus in relative position $wv\varphi$ to $\mathbf{T}_0^*$, and where the sign only depends on $C_{\mathbf{G}^*}(t)$. This semisimple character is irreducible if $C_{\mathbf{G}^*}(t)$ is connected (see [DM91, Proposition 14.43]), so in particular if $\mathbf{G}$ has connected center.

https://doi.org/10.1112/S0010437X14007271 Published online by Cambridge University Press

Thus, $\chi_t(g)$ is nothing else but the multiplicity of the trivial F-class function on $W(t)$ in the F-class function on $W(t)$ which maps an element $w \in W(t)$ to $R^{\mathbf{G}}_{\mathbf{T}^*,t}(g)$, where $\mathbf{T}^* \leqslant C^\circ_{\mathbf{G}^*}(t)$ is an F-stable maximal torus in relative position $wv\varphi$. For unipotent elements this gives the following result.

Corollary 2.4. *Let $u \in G$ be unipotent, and $Q_{w\varphi}(u) = \sum_{i\geqslant 0} \psi_i^u(w\varphi)\, q^i$ for $w \in W$ and q in a fixed congruence class modulo $N_{\mathbf{G}}$. Then*

$$\chi_t(u) = \pm \sum_{i\geqslant 0} \langle \psi_i^u|_{W(t)v\varphi}, 1\rangle_{W(t)v\varphi}\; q^i,$$

where $\langle\, ,\, \rangle_{W(t)v\varphi}$ denotes the scalar product of class functions on the coset $W(t)v\varphi$.

Proof. The above formula for χ_t and Proposition 2.1 give

$$\chi_t(u) = \pm \frac{1}{|W(t)|} \sum_{w\in W(t)} Q_{wv\varphi}(u) = \pm \sum_{i\geqslant 0} \frac{1}{|W(t)|} \sum_{w\in W(t)} \psi_i^u(wv\varphi)\, q^i.$$

As pointed out above the inner term is just the scalar product of the trivial character with ψ_i^u restricted to the coset $W(t)v\varphi$. □

For example, if $u \in G$ is regular unipotent, then $Q_{w\varphi}(u) = 1$ for all $w\varphi$ by [Ca93, Proposition 8.4.1], and thus $\chi_t(u) = \pm\langle 1, 1\rangle_{W(t)v\varphi} = \pm 1$.

We now derive a remarkable symmetry between the 'semisimple parts' of character tables of dual groups. For this, we embed $\mathbf{G}$ into a connected reductive group $\hat{\mathbf{G}}$ with connected center and having the same derived subgroup as $\mathbf{G}$, and with an extension $F : \hat{\mathbf{G}} \to \hat{\mathbf{G}}$ of F to $\hat{\mathbf{G}}$, which is always possible. Then an irreducible character of G is called semisimple, if it is a constituent of the restriction to G of a semisimple character of $\hat{G} := \hat{\mathbf{G}}^F$. By a result of Lusztig, restriction of irreducible characters from $\hat{\mathbf{G}}$ to $\mathbf{G}$ is multiplicity free. Note that all G-constituents of a given semisimple character of $\hat{G}$ take the same value on all semisimple elements of G since they have the same scalar product with all Deligne–Lusztig characters, and the characteristic functions of semisimple conjugacy classes are uniform.

Theorem 2.5. *Let $s \in G$, $t \in G^*$ both be semisimple. Then*

$$|C_{\mathbf{G}^*}(t)^F|_{p'}\, \chi_t(s) = |C_{\mathbf{G}}(s)^F|_{p'}\, \chi_s(t).$$

Proof. Write $\mathbf{C} := C_{\mathbf{G}}(s)$ and $\mathbf{C}' := C_{\mathbf{G}^*}(t)$. By [Ca93, Proposition 7.5.5] the characteristic function of the G-conjugacy class of s is given by

$$\psi_s = \epsilon \frac{1}{|\mathbf{C}^F|_p\, |\mathbf{C}^F|} \sum_{\substack{(\mathbf{T},\theta)\\ s\in\mathbf{T}}} \epsilon_{\mathbf{T}}\, \theta(s)^{-1} R_{\mathbf{T},\theta},$$

where the sum ranges over pairs $(\mathbf{T},\theta)$ consisting of an F-stable maximal torus $\mathbf{T}$ of $\mathbf{G}$ containing s and some $\theta \in \mathrm{Irr}(\mathbf{T}^F)$, and where ϵ, $\epsilon_{\mathbf{T}}$ are signs depending on $\mathbf{C}$, $\mathbf{T}$ respectively. (Note that $|\mathbf{C}^{\circ F}|_p = |\mathbf{C}^F|_p$ always.) Now for any character ρ of G we have $\rho(s) = |\mathbf{C}^F|\, \langle \psi_s, \rho\rangle$, so that

$$\chi_t(s) = \epsilon \frac{1}{|\mathbf{C}^F|_p} \sum_{\substack{(\mathbf{T},\theta)\\ s\in\mathbf{T}}} \epsilon_{\mathbf{T}}\, \theta(s)^{-1} \langle R_{\mathbf{T},\theta}, \chi_t\rangle.$$

But $\langle R_{\mathbf{T},\theta}, \chi_t\rangle$ is non-zero if and only if $(\mathbf{T},\theta)$ lies in the geometric conjugacy class parametrized by t, and in this case it equals ϵ' (a sign depending on $\mathbf{C}'$ only). Indeed, this equality is true for

https://doi.org/10.1112/S0010437X14007271 Published online by Cambridge University Press

the group $\hat{\mathbf{G}}$ with connected center, and then remains true for χ_t since the restriction to G is multiplicity free (see [Lu88, Proposition 5.1]). So

$$\chi_t(s) = \epsilon\epsilon' \frac{1}{|\mathbf{C}^F|_p} \sum_{\substack{(\mathbf{T},\theta)\sim t\\ s\in\mathbf{T}}} \epsilon_{\mathbf{T}}\, \theta(s)^{-1}.$$

Summing over the whole G-conjugacy class of s we get

$$|G|\chi_t(s) = \epsilon\epsilon'\, |\mathbf{C}^F|_{p'} \sum_{s'\sim s} \sum_{\substack{(\mathbf{T},\theta)\sim t\\ s'\in\mathbf{T}}} \epsilon_{\mathbf{T}}\, \theta(s')^{-1},$$

whence

$$|\mathbf{C'}^F|_{p'}\, \chi_t(s) = \epsilon\epsilon'\, \frac{|\mathbf{C}^F|_{p'}\, |\mathbf{C'}^F|_{p'}}{|G|} \sum_{s'\sim s} \sum_{\substack{(\mathbf{T},\theta)\sim t\\ s'\in\mathbf{T}}} \epsilon_{\mathbf{T}}\, \theta(s')^{-1}.$$

But this last expression on the right-hand side is symmetric in s, t: Let $(\mathbf{T}, \theta)$ be in the geometric conjugacy class of t and $s' \in \mathbf{T}^F$. Let $(\mathbf{T}^*, t')$ be dual to $(\mathbf{T}, \theta)$ in the sense of [DM91, Proposition 13.13], so $t' \in \mathbf{T}^{*F}$ which is conjugate to t. Furthermore s' defines an element $\sigma \in \mathrm{Irr}(\mathbf{T}^{*F})$, and $s' \in \mathbf{T}^F$ is equivalent to the fact that $(\mathbf{T}^*, t')$ lies in the geometric conjugacy class of s', hence of s. By construction $N_G(\mathbf{T}, \theta)/\mathbf{T}^F$ is isomorphic to $N_{G^*}(\mathbf{T}^*, t')/\mathbf{T}^{*F}$, so since $\mathbf{T}^{*F}$ has the same order as $\mathbf{T}^F$, the number of G-conjugates of $(\mathbf{T}, \theta)$ and of G^*-conjugates of $(\mathbf{T}^*, t')$ agree. Thus, instead of summing over triples $(s', \mathbf{T}, \theta)$ we may sum over the dual triples $(t', \mathbf{T}^*, \sigma)$, with $t' \sim t$, and $\sigma \in \mathrm{Irr}(\mathbf{T}^{*F})$, so that $\theta(s') = \sigma(t')$. The claim follows. □

Remark 2.6. For every semisimple element $t \in G^*$ there is also a *regular character*

$$\chi_t^{\mathrm{reg}} = \pm \frac{1}{|W(t)|} \sum_{w\in W(t)} \epsilon_{\mathbf{T}^*_{wv\varphi}} R^{\mathbf{G}}_{\mathbf{T}^*_{wv\varphi},t}$$

of G (see [DM91, Definition 14.40]), where $\mathbf{T}^*_{wv\varphi}$ denotes an F-stable maximal torus in relative position $wv\varphi$ to $\mathbf{T}^*_0$, $\epsilon_{\mathbf{T}^*_{wv\varphi}}$ is a sign, and where the global sign only depends on $C_{\mathbf{G}^*}(t)$. This regular character is irreducible if $C_{\mathbf{G}^*}(t)$ is connected (see [DM91, Proposition 14.43]), so in particular if $\mathbf{G}$ has connected center (and then it is the Curtis–Alvis dual of the corresponding semisimple character). Entirely analogously to Theorem 2.5 one can show that

$$|C_{\mathbf{G}^*}(t)^F|_{p'}\, \chi_t^{\mathrm{reg}}(s) = |C_{\mathbf{G}}(s)^F|_{p'}\, \chi_s^{\mathrm{reg}}(t)$$

for all semisimple $s \in G$, $t \in G^*$.

We now come to the main result of this section.

THEOREM 2.7. *Let $G = G(q)$ be one of the finite simple groups of Lie type in Table 1, with $q = p^f$ a power of a good prime p for G. Let $x \in G$ be an involution, $y \in G$ a unipotent element as indicated in the table, and z a regular unipotent element. Set*

$$f(q) := \sum_{1\neq\chi\in\mathrm{Irr}(G)} \frac{\chi(x)\chi(y)\chi(z)}{\chi(1)}.$$

Then $f(q)$ is a rational function in q of degree less than zero, for all q in a fixed residue class modulo a sufficiently large integer only depending on the type of G.

https://doi.org/10.1112/S0010437X14007271 Published online by Cambridge University Press

Proof. Let $\mathbf{G}$ denote a simple algebraic group of exceptional type G_2 or E_8 defined over $\mathbb{F}_q$ and $F : \mathbf{G} \to \mathbf{G}$ a Steinberg endomorphism so that $G = \mathbf{G}^F$.

In order to investigate the sum, we make use of Lusztig's theory of characters. We argue for all q in a fixed congruence class modulo $N_{\mathbf{G}}$ (see above). First of all, since we assume that p is a good prime for G, it follows that only the semisimple characters of G do not vanish on the class $[z]$ of regular unipotent elements, and the semisimple characters take value ± 1 on that class (see [Ca93, Corollary 8.3.6], or the remark after Corollary 2.4). Since $\mathbf{G}$ has connected center, the dual group $\mathbf{G}^*$ is of simply connected type, hence all semisimple elements of $\mathbf{G}^*$ have connected centralizer. Thus, the semisimple characters of G are in one-to-one correspondence with the F-stable semisimple conjugacy classes of $\mathbf{G}^*$, and we write χ_t for the semisimple character indexed by (the class of) a semisimple element $t \in G^*_{\mathrm{ss}}$.

Let us say that two semisimple elements of $\mathbf{G}^{*F}$ are equivalent if their centralizers in $\mathbf{G}^{*F}$ are conjugate. Then it is known that the number of equivalence classes is bounded independently of q, and can be computed purely combinatorially from the root datum of $\mathbf{G}$ (see, for example, [MT11, Corollary 14.3]). Now note that if $t_1, t_2 \in G^*_{\mathrm{ss}}$ are equivalent, then χ_{t_1} and χ_{t_2} agree on all unipotent elements, since by the formula in Corollary 2.4 the value of χ_t only depends on $C_{\mathbf{G}^*}(t)$. Thus, in order to prove the claim it suffices to show that for each of the finitely many equivalence classes A of semisimple elements in G^*_{ss} up to conjugation we have

$$\left| \frac{\chi(y)\chi(z)}{\chi(1)} \sum_{t \in A} \chi_t(x) \right| = O(q^{-1}),$$

where $\chi(u) := \chi_t(u)$ denotes the common values of all χ_t, $t \in A$, on a unipotent element u. For this, we compute the degree $d_u(A)$ in q of the rational function $(\chi(y)\chi(z))/(\chi(1))$ explicitly from the known values of the Green functions (see Lusztig [Lu86] and Spaltenstein [Sp85]) using Corollary 2.4. This is a purely mechanical computation with reflection cosets inside the Weyl group of $\mathbf{G}$ and can be done in Chevie [Mi] for example.

It remains to control the sums $\sum_{t \in A} \chi_t(x)$, for A an equivalence class of semisimple elements (up to conjugation). Let us fix $t_0 \in A$ and set $\mathbf{C}_A := C^\circ_{\mathbf{G}^*}(t_0) = C_{\mathbf{G}^*}(t_0)$. By duality, we may interpret x as a linear character (of order two) on all maximal tori of $\mathbf{C}_A$. First of all, since $\mathbf{C}_A$ has only finitely many G-classes of F-stable maximal tori, and each torus only contains finitely many involutions (conjugate to x), there are only finitely many possibilities for the values $\{\chi_t(x) \mid t \in A\}$, as a polynomial in q. Using Chevie again, we can calculate the maximal degree $d_s(A)$ in q of any such polynomial, as follows: by Theorem 2.5, in order to determine these degrees we may instead compute $\chi_x(t)$, for $t \in A$. Now by the remarks following the definition of semisimple characters, this value can be interpreted as the multiplicity of the trivial character of the Weyl group $W(x)$ of $C_{\mathbf{G}}(x)$ in the F-class function given by $w \mapsto R^{\mathbf{G}^*}_{\mathbf{T}_w, x}(t)$, where $\mathbf{T}_w$ is a maximal torus of type $w\varphi$. In turn this F-class function is described in Proposition 2.3 in terms of data only involving the Weyl group $W(x)$, and which thus can be computed in Chevie.

Second, the number of elements in A is a polynomial in q of degree $d(A) := \dim Z(\mathbf{C}_A)$ since the set

$$\{t \in Z(\mathbf{C}_A) \mid C^\circ_{\mathbf{G}^*}(t) = \mathbf{C}_A\}$$

is dense in $Z(\mathbf{C}_A)$ (see [MT11, Example 20.11]). But whenever there is some $t \in A$ no conjugate of which lies in the kernel of x, then $\sum_{t \in Z(\mathbf{C}_A)^F} \chi_t(x) = 0$ by Lemma 2.2. So $\sum_{t \in A} \chi_t(x) = -\sum_{t \in Z(\mathbf{C}_A)^F \setminus A} \chi_t(x)$, and the number of elements in $Z(\mathbf{C}_A)^F \setminus A$ is given by a polynomial in q of degree strictly smaller than $d(A)$.

https://doi.org/10.1112/S0010437X14007271 Published online by Cambridge University Press

Table 2. Data for G_2.

A (centralizer type)	$d_u(A)$	$d_s(A)$	$d(A)$	Corr. term
$(q-1)^2$	-4	2	2	-1
$(q+1)^2$	-4	2	2	-1
$(q-1)A_1$	-3	2	1	-1
$(q+1)A_1$	-3	2	1	-1
$(q-1)\tilde{A}_1$	-3	2	1	-1
$(q+1)\tilde{A}_1$	-3	2	1	-1
A_2	-2	1	0	
${}^2A_2$	-2	1	0	
$\tilde{A}_1A_1$	-2	1	0	

Explicit computation now shows that for all equivalence classes A of semisimple elements in G^*, the sum of the degrees $d_u(A)+d_s(A)+d(A)$, respectively $d_u(A)+d_s(A)+d(A)-1$ in the case that there is some $t \in A$ not in the kernel of x, is smaller than zero, whence the claim. □

We give some precisions on the computations needed to derive the values of d_u, d_s, needed in the proof of the theorem. The possible centralizer types in the algebraic group are among the maximal rank subgroups generated by A_1-subgroups corresponding to arbitrary subsets of the set of simple roots union the negative of the highest root. The center of such a maximal rank subgroup is then computed with the `Chevie`-command `AlgebraicCentre`. The possible rational types of these maximal rank subgroups and of their centers are obtained through the command `Twistings`.

In Table 2 we list the data needed in the proof of Theorem 2.7 for the case of G_2. Note that the semisimple character corresponding to the identity element is the principal character, which does not occur in the sum for $f(q)$, so the centralizer type G_2 does not contribute. Algebraic groups of type E_8 have 65 different centralizer types, and the total number of twistings is 872 (for example, the type corresponding to a maximal torus splits into 120 rational types), so we do not print the analogous table for type E_8.

Remark 2.8. In fact, using information on subgroups containing regular unipotent elements, we will conclude from Theorem 2.7 that $f(q)=0$ for all $q=p^a$ with p good, see Theorem 5.3.

Remark 2.9. A computation with the generic character table gives that for $G={}^3D_4(p^f)$, $p \geqslant 3$, the normalized structure constant of (C_1,C_2,C_3) with C_1 the class of involutions, C_2 the class of unipotent elements of type $3A_1$ and C_3 the class of regular unipotent elements equals one. But since all three classes intersect $G_2(p)$ nontrivially, and the structure constant there equals one as well, these triples only generate $G_2(p)$.

3. Lie primitive subgroups containing regular unipotent elements

Let G be a simple algebraic group over an algebraically closed field of characteristic $p \geqslant 0$. We want to consider the closed subgroups of G containing a regular unipotent element of G. The maximal closed subgroups of positive dimension containing a regular unipotent element are classified in [SS97, Theorem A]. Of course, subfield subgroups and parabolic subgroups contain regular unipotent elements. Thus, we focus on the Lie primitive subgroups (those finite groups

https://doi.org/10.1112/S0010437X14007271 Published online by Cambridge University Press

Table 3. Orders of regular unipotent elements.

	G				
	$p=2$	$p=3$	$p=5$	$5<p<h$	$h\leqslant p$
G_2	8	9	25	p^2	p
F_4, E_6	16	27	25	p^2	p
E_7	32	27	25	p^2	p
E_8	32	81	125	p^2	p

which do not contain a subgroup of the form $O^{p'}(G^F)$ where F is some Steinberg endomorphism of G and are not contained in any proper closed positive-dimensional subgroup). Note that if $p=0$, unipotent elements have infinite order and so any closed subgroup containing a regular unipotent element has positive dimension. So we assume that $p>0$.

We use the results of Liebeck and Seitz [LS03] about maximal Lie primitive subgroups of exceptional groups. In particular, all conjugacy classes of such subgroups are known aside from the almost simple groups. In the latter case, at least we know the possibilities up to isomorphism (rather than conjugacy).

We record the following well-known lemma.

Lemma 3.1. *Let G be a simple algebraic group of rank r over an algebraically closed field. Let $W=\mathrm{Lie}(G)$ denote the adjoint module for G. If $w\in W$, then the stabilizer of w in G has dimension at least r.*

Proof. Let V be an irreducible variety that G acts on. Let $\phi\colon G\times V\to V\times V$ be the map sending (g,v) to $(g\cdot v,v)$. Let M denote the image of ϕ. So M is irreducible. If $(g\cdot v,v)\in M$, then $\phi^{-1}(g\cdot v,v)\cong G_v$ as varieties (here G_v is the stabilizer of v in G).

By semicontinuity of the dimension of a fiber, we know that the minimum dimension of a fiber is attained on an open subvariety of M. In particular, taking $V=W$, then the set of regular semisimple elements of W is an open subvariety. If $w\in W$ is regular semisimple, then G_w is a maximal torus of dimension r, whence the result. □

We only consider exceptional groups here. One could prove a similar result for the classical groups using [GPPS99] and [Di12]. The following well-known result on the orders of regular unipotent elements in the exceptional groups will be used throughout the subsequent proof. This can be read off from the tables in [La95]. Note that the exponent of the regular unipotent element is precisely the smallest power of p that is at least the Coxeter number h.

Lemma 3.2. *Let G be a simple algebraic group of exceptional type in characteristic $p>0$ with Coxeter number h. Then the order of regular unipotent elements of G is as given in Table 3.*

We will give all possibilities for maximal Lie primitive subgroups of simple exceptional groups containing a regular unipotent element (we are certainly not classifying all cases up to conjugacy nor are we claiming that all cases actually do occur; although one can show that several of the cases do occur).

We deal with G_2 first. In this case, all maximal subgroups of the associated finite groups are known [Co81, Kl88] and so it is a simple matter to deduce the following result.

Theorem 3.3. *Let $G=G_2(k)$ with k algebraically closed of characteristic $p>0$. Suppose that M is a maximal Lie primitive subgroup of G containing a regular unipotent element. Then one of the following holds:*

(i) *$p = 2$ and $M = J_2$;*
(ii) *$p = 7$ and $M = 2^3.\mathrm{L}_3(2)$, $G_2(2)$ or $\mathrm{L}_2(13)$; or*
(iii) *$p = 11$ and $M = J_1$.*

Note that in the previous theorem, each of the possibilities does contain a regular unipotent element. In part (i), this follows by observing that since $G_2(k) < \mathrm{Sp}_6(k)$, any element of order eight has a single Jordan block and so is regular unipotent in G. In all possibilities in part (ii), M acts irreducibly on the seven-dimensional module V for G and has a Sylow 7-subgroup of order seven. Thus, V is a projective M-module, whence an element of order seven has a single Jordan block of size seven. The only unipotent elements of G having a single Jordan block on V are the regular unipotent elements [La95]. In part (iii), we note that M contains $\mathrm{L}_2(11)$ which acts irreducibly and so elements of order 11 have a single Jordan block.

We now consider G of type F_4, E_6, E_7 or E_8; here we let $t(G)$ be defined as in [LS03]. The values of $t(G)$ are given by $t(G) = (2, p-1)u(G)$ where $u(G_2) = 12$, $u(F_4) = 68$, $u(E_6) = 124$, $u(E_7) = 388$ and $u(E_8) = 1312$. See Lawther [La] or [MT11, Proposition 29.13].

Theorem 3.4. *Let G be a simple algebraic group over an algebraically closed field k of characteristic $p > 0$. Assume moreover that G is exceptional of rank at least four. Suppose that M is a maximal Lie primitive subgroup of G containing a regular unipotent element.*

(i) *If $G = F_4(k)$, then one of the following holds:*
   (a) *$p = 2$ and $F^*(M) = \mathrm{L}_3(16)$, $\mathrm{U}_3(16)$ or $\mathrm{L}_2(17)$;*
   (b) *$p = 13$ and $M = 3^3 : \mathrm{SL}_3(3)$ or $F^*(M) = \mathrm{L}_2(25)$, $\mathrm{L}_2(27)$ or ${}^3D_4(2)$; or*
   (c) *$M = \mathrm{L}_2(p)$ with $13 \leqslant p \leqslant 43$.*

(ii) *If $G = E_6(k)$, then one of the following holds:*
   (a) *$p = 2$ and $F^*(M) = \mathrm{L}_3(16)$, $\mathrm{U}_3(16)$ or Fi_{22};*
   (b) *$p = 13$ and $M = 3^{3+3} : \mathrm{SL}_3(3)$ or $F^*(M) = {}^2F_4(2)'$; or*
   (c) *$M = \mathrm{L}_2(p)$ with $13 \leqslant p \leqslant 43$.*

(iii) *If $G = E_7(k)$, then one of the following holds:*
   (a) *$p = 19$ and $F^*(M) = \mathrm{U}_3(8)$ or $\mathrm{L}_2(37)$; or*
   (b) *$M = \mathrm{L}_2(p)$ with $19 \leqslant p \leqslant 67$.*

(iv) *If $G = E_8(k)$, then one of the following holds:*
   (a) *$p = 2$ and $F^*(M) = \mathrm{L}_2(31)$;*
   (b) *$p = 7$ and $F^*(M) = \mathrm{S}_8(7)$ or $\Omega_9(7)$;*
   (c) *$p = 31$ and $M = 2^{5+10}.\mathrm{SL}_5(2)$ or $5^3.\mathrm{SL}_3(5)$, or $F^*(M) = \mathrm{L}_2(32)$, $\mathrm{L}_2(61)$ or $\mathrm{L}_3(5)$; or*
   (d) *$M = \mathrm{L}_2(p)$ with $31 \leqslant p \leqslant 113$.*

Proof. Let G be a simple exceptional algebraic group over k of rank at least four. Let M be a maximal Lie primitive subgroup of G (i.e. M is Lie primitive, not a subfield group and is not contained in any finite subgroup of G other than subfield groups). We split the analysis into various cases. The possibilities for M are essentially listed in [LS03, Theorem 8]. See also [MT11].

https://doi.org/10.1112/S0010437X14007271 Published online by Cambridge University Press

Case 1: M has a normal elementary abelian r-subgroup. If $r = p$, then M is contained in a proper parabolic subgroup (see, for example, [MT11, Remark 17.16(a)]). When $r \neq p$, then by [MT11, Theorem 29.3] this implies that one of the following holds:

(i) $p \neq 3$, $G = F_4(k)$ with $M \cong 3^3 : \mathrm{SL}_3(3)$;
(ii) $p \neq 3$, $G = E_6(k)$ with $M \cong 3^{3+3} : \mathrm{SL}_3(3)$;
(iii) $p \neq 2$, $G = E_8(k)$ with $M \cong 2^{5+10}.\mathrm{SL}_5(2)$; or
(iv) $p \neq 5$, $G = E_8(k)$ with $M \cong 5^3.\mathrm{SL}_3(5)$.

By considering the order of a regular unipotent element, we see that the only possibilities are $p = 13$ in parts (i) or (ii) and $p = 31$ in parts (iii) or (iv).

Case 2: $F(M) = 1$ but M is not almost simple. By [LS03], the only possibility is that $G = E_8(k)$ and $M \cong (A_5 \times A_6).2^2$. Note that the order of a regular unipotent element in $E_8(k)$ is larger than the order of any p-element of M.

Case 3: $F^*(M)$ is a simple group of Lie type in characteristic p. We first deal with the case that $F^*(M) = \mathrm{L}_2(p^a)$. Suppose that a regular unipotent element of G has order p^b with $b > 1$. Since a Sylow p-subgroup of $F^*(M)$ has exponent p, it follows that $[M : F^*(M)] \geqslant p^{b-1}$. Thus, M must contain field automorphisms of order p^{b-1}, whence $a \geqslant p^{b-1}$.

If $p = 2$, this implies that $a \geqslant 8$ and $a \geqslant 16$ for $G = E_8$. Thus, $2^a > t(G)$ unless $G = E_7$, whence M is contained in a positive-dimensional proper subgroup [LS03, Theorem 5]. Consider the remaining case of E_7. Note that any involution in $F^*(M)$ has all Jordan blocks of size two on any nontrivial irreducible representation in characteristic two. Thus, an element of order 16 in M will have all Jordan blocks of size 16. So if $x \in M$ is a regular unipotent element in E_7, it will have all Jordan blocks on the adjoint module of size 1 or 16. A regular unipotent element does not act as such [La95], whence this case cannot occur.

If $p = 3$, then $a \geqslant 9$ and if $5 \leqslant p < h$, then $p^a \geqslant 5^5$. In all of these cases, $p^a > t(G)$. It follows by [LS03, Theorem 5] that M is contained in a positive-dimensional proper subgroup.

Thus, we may assume that the regular unipotent element has order p which gives us the lower bound for p in the result. It follows by [ST93, Theorems 1.1 and 1.2] that $a = 1$ and $M = \mathrm{L}_2(p)$. The upper bound for p follows by [ST90, Theroem 2] (see also [MT11, Theorem 29.11]).

If $p = 2$ and $F^*(M) = {}^2B_2(2^{2a+1})$, $a \geqslant 1$, then the exponent of a Sylow 2-subgroup of M is 4 and so M will not contain a regular unipotent element.

If $p = 3$ and $F^*(M) = {}^2G_2(3^{2a+1})'$, then the exponent of a Sylow 3-subgroup of $F^*(M)$ is 9. Thus, there must be a field automorphism of order 3 in M (or of order 9 when $G = E_8(k)$). It follows that $3^{2a+1} > t(G)$ unless $2a+1 = 3$ and $G = F_4, E_6$ or E_7. So aside from this case, [LS03, Thm. 5] implies that M is contained in a positive-dimensional subgroup.

Suppose that $M = {}^2G_2(27).3$. Let V be the adjoint module for G. The only irreducible representations of M in characteristic three of dimension at most $\dim V$ are the trivial module, a module of dimension 21 or if $G = E_7$ a module of dimension 81. By noting that $\dim H^1(M, W) \leqslant 1$ for any of the possible modules W occurring as composition factors of V (see [Si93]), it follows easily that M has fixed points on V, whence by Lemma 3.1 that M is contained in a positive-dimensional subgroup of G.

It follows by [LS03, Theorem 8] that $2r \leqslant s$ where s is the rank of G and r is the untwisted rank of $F^*(M)$. Similarly it follows that either $q \leqslant 9$ or $F^*(M) = \mathrm{U}_3(16)$ or $\mathrm{L}_3(16)$.

https://doi.org/10.1112/S0010437X14007271 Published online by Cambridge University Press

The cases to deal with are therefore $F^*(M) = \mathrm{U}_3(2^a)$, $1 < a \leqslant 4$ or $\mathrm{L}_3(2^a)$, $1 \leqslant a \leqslant 4$ with $p = 2$. In this case, the exponent of a Sylow p-subgroup of M is at most 8 unless $2^a = 16$ and so M contains no regular unipotent elements. If $2^a = 16$, the same argument rules out $E_7(k)$ and $E_8(k)$.

Next suppose that $F^*(M) = \mathrm{L}_3(q)$ or $\mathrm{U}_3(q)$ with $q = 3, 5, 7$ or 9. The exponent rules out the possibility that M contains a regular unipotent element.

Similarly, if $F^*(M) = {}^3D_4(q)$ or ${}^2F_4(q)'$, then $G = E_8$ and the exponent of M is too small. If $F^*(M) = G_2(q)$, the exponent is too small unless M involves a field automorphism and so $M = G_2(4).2$ is the only possibility. The exponent of a Sylow 2-subgroup of M is 16 and so $G = F_4(q)$ or $E_6(q)$. The only absolutely irreducible nontrivial modules of M in characteristic 2 have dimension $12, 28, 36$ or dimension greater than 78. By [Si92], $H^1(M, V) = 0$ for any of these modules whence M has fixed points on the adjoint module for F_4 or E_6. Thus by Lemma 3.1, M is contained in a positive-dimensional subgroup.

Next consider the case that $F^*(M) = \mathrm{S}_4(q), \mathrm{L}_4(q)$ or $\mathrm{U}_4(q)$ with $q = p^a \leqslant 9$. If p is odd, then the exponent of a Sylow p-subgroup of M is either p or nine, a contradiction. If q is even, the exponent of M is at most eight, also a contradiction.

Next suppose that $F^*(M) = \mathrm{S}_6(q)$ or $\Omega_7(q)$ with $q = p^a \leqslant 9$. Again, it follows that the exponent of a Sylow p-subgroup of M is smaller than the order of a regular unipotent element of G.

The remaining cases are when M has rank four and is defined over a field of size $q = p^a \leqslant 9$ and so we may assume that $G = E_8(k)$ since $s \geqslant 2r$. If $p = 2$, then aside from the case $M \neq F^*(M) = F_4(4)$, the exponent of a Sylow 2-subgroup of M is at most 16, which is too small by Table 3.

In the case $F^*(M) = F_4(4)$, an element x of order 32 would have x^2 a regular unipotent element of $F_4(4)$. It follows by [Lu01] that the only irreducible M-modules in characteristic two are either trivial, have dimension 52 or have dimension greater than 248. It follows that M has at least 40 trivial composition factors on the adjoint module of $E_8(k)$. Since $H^1(M, V) = 0$ for $\dim V = 52$ [JP76], this implies that M has fixed points on the adjoint module. Thus, by Lemma 3.1, M is contained in a positive-dimensional subgroup (and, by [LS03], this is not possible).

Similarly, if $p = 3$ or 5, then the exponent of a Sylow p-subgroup of M is at most 27 or 25 and so M cannot contain a regular unipotent element of E_8. The remaining possibility is that $p = q = 7$, whence $F^*(M) = \mathrm{S}_8(7)$ or $F^*(M) = \Omega_9(7)$.

Case 4: $F^*(M)$ is a simple group not of Lie type in characteristic p. We can eliminate almost all of these by comparing the order of a regular unipotent element to the exponent of the possibilities for M given in [LS03, Theorem 8]. Moreover, the element of the right order must have centralizer a p-subgroup (since this is true for regular unipotent elements). The possibilities remaining are given in the theorem. □

Remark 3.5. One can show that some of the subgroups listed in Theorem 3.4 are Lie primitive and do contain regular unipotent elements. On the other hand, most of the possibilities with $M \cong \mathrm{L}_2(p)$ given above likely do not occur (indeed this follows by Magaard's thesis [Ma90] for F_4 and by unpublished work of Aschbacher [As91] for E_6).

Note, in particular, that if $p > 113$, then there are no Lie primitive subgroups containing a regular unipotent element (and likely this is true for $p > 31$).

We note the following easy result.

https://doi.org/10.1112/S0010437X14007271 Published online by Cambridge University Press

Lemma 3.6. *Let V be a finite dimensional vector space over an algebraically closed field k. Let $x, y \in \mathrm{GL}(V)$ be elements with quadratic minimal polynomials. Then $H := \langle x, y\rangle$ leaves invariant a subspace of dimension at most two.*

Proof. If $p \neq 2$ and x, y are both semisimple, then we can replace x by $ax + b$ and y by $cy + d$ and thus assume that x, y are involutions, whence H is dihedral (similarly, if $p = 2$ and x, y are unipotent).

In the general case let V_x and V_y be eigenspaces of x, y of maximal dimension. If $V_x \cap V_y \neq 0$, then H has a one-dimensional invariant space. Since x, y are quadratic, $\dim V_x, \dim V_y \geqslant (\dim V)/2$. So we may assume that $\dim V_x = \dim V_y = (\dim V)/2$ and $V = V_x \oplus V_y$.

Thus, with respect to this decomposition, we may assume that

$$x := \begin{pmatrix} aI & B \\ 0 & cI \end{pmatrix}, \quad y := \begin{pmatrix} dI & 0 \\ E & fI \end{pmatrix},$$

with scalars a, c, d and f. If B is not invertible, then x and y have a common fixed 1-space. So assume that B is invertible. Conjugating x, y by diagonal matrices allows us to assume that $B = I$ and to replace E by any matrix similar to E. In particular, we may assume that E is upper triangular, whence x, y have a common two-dimensional invariant space. □

Corollary 3.7. *Let $G = E_8(k)$ over an algebraically closed field k of characteristic $p > 5$. Suppose that x is an involution in G, y is in the conjugacy class $4A_1$ and z is a regular unipotent element with $xyz = 1$:*

(i) *if $p > 7$, then $\langle x, y\rangle$ is not contained in a Lie primitive subgroup;*

(ii) *if $p = 7$ and $\langle x, y\rangle$ is contained in a Lie primitive subgroup, then $\langle x, y\rangle$ is contained in a proper closed subgroup of G of positive dimension.*

Proof. We use Theorem 3.4. Suppose that $H := \langle x, y\rangle \leqslant M$ with M a maximal Lie primitive subgroup of G. Consider the possibilities for M in Theorem 3.4(iv) with $p > 5$.

Note that the Sylow p-subgroup of M cannot be cyclic of order p (because y and z do not generate conjugate subgroups). This rules out the cases $M = \mathrm{L}_2(p)$ and $p = 31$.

The only cases remaining are with $p = 7$ and $F^*(M) = \mathrm{S}_8(7)$ or $F^*(M) = \Omega_9(7)$. Thus, part (i) holds. So consider the remaining case with $p = 7$ and assume that H is not contained in a proper closed positive-dimensional subgroup of G.

It follows that H is not contained in a parabolic subgroup of M either (for then H would normalize a unipotent subgroup and so be contained in a parabolic subgroup of G as well).

Since H is generated by unipotent elements, it follows that $H \leqslant F^*(M)$. Moreover, H acts irreducibly on the natural module for M (for stabilizers of nondegenerate spaces do not contain regular unipotent elements and stabilizers of totally singular spaces are contained in parabolic subgroups). Thus, y does not act quadratically on the natural module for M by Lemma 3.6.

If $H = \Omega_9(7)$, then similarly, we see that y is not a short root element. It follows by the main results of [Su09] that on any irreducible module other than the natural or the trivial module for M in characteristic seven, y has a Jordan block of size at least five. However, y has all Jordan blocks of size at most four on the adjoint module W for E_8 (by [La95]). It follows that all composition factors are trivial in the case $H \leqslant \mathrm{S}_8(7)$ (since the natural module is not a module for the simple group). In the case $H \leqslant \Omega_9(7)$, since $H^1(H, V) = \mathrm{Ext}^1_H(V, V) = 0$ for the natural module V (see [Mc98]), it follows that W is a semisimple M-module and M must have

https://doi.org/10.1112/S0010437X14007271 Published online by Cambridge University Press

a fixed point on W (since 248 is not a multiple of 9). However, the stabilizer of a point of W has dimension at least eight by Lemma 3.1 and so H is contained in a positive-dimensional proper closed subgroup, a contradiction.

This completes the proof. □

4. Some nonexistence results

Lemma 4.1. *Let k be a field of characteristic $p \neq 2$. Let $G = \mathrm{SL}_n(k) = \mathrm{SL}(V)$. Assume that $x \in G$ is an involution, $y \in G$ is a unipotent element with quadratic minimal polynomial and $z \in G$ is a regular unipotent element. Then $xyz \neq 1$.*

Proof. If $n = 2$, the only involution is central and the result is clear. If $n = 3$, we see that x and y have a common eigenvector v with $xv = -v$. Thus, xy is not unipotent.

So assume that $n \geqslant 4$. If x and y have a common eigenvector, the result follows by induction. Thus, $n = 2m$ and the fixed spaces of x and y on V each have dimension m. Thus, choosing an appropriate basis for V, we may assume that

$$x = \begin{pmatrix} I_m & J \\ 0 & -I_m \end{pmatrix} \quad \text{and} \quad y = \begin{pmatrix} I_m & 0 \\ I_m & I_m \end{pmatrix},$$

where J is in Jordan canonical form. If J has more than one block, then $V = V_1 \oplus V_2$ with V_i invariant under $\langle x, y \rangle$, whence xy is certainly not regular unipotent. Note that

$$xy - I_n = \begin{pmatrix} J & J \\ -I_m & -2I_m \end{pmatrix}.$$

If J is not nilpotent, then we see that $xy - I_n$ is invertible, whence xy is not unipotent (indeed has no eigenvalue one). If J is nilpotent, we see that -2 is an eigenvalue and so again xy is not unipotent. □

By viewing $\mathrm{SO}_{2m}(k)$ inside $\mathrm{SL}_{2m}(k)$ and starting with $m = 2$, essentially the same proof yields the following result.

Lemma 4.2. *Let $G = \mathrm{SO}_{2m}(k)$, $m \geqslant 2$, with k of characteristic $p \neq 2$. Assume that $x \in G$ is an involution, $y \in G$ is a unipotent element with quadratic minimal polynomial and $z \in G$ is a regular unipotent element. Then $xyz \neq 1$.*

We will also need to deal with one special case where the unipotent element does not necessarily act quadratically.

Lemma 4.3. *Let k be a field of characteristic $p \neq 2$. Let $G = \mathrm{Spin}_{14}(k)$. Let V be the natural 14-dimensional module for G. If $x \in G$ is an involution, $y \in G$ is unipotent with $\dim C_V(y) \geqslant 8$ and $z \in G$ is a regular unipotent element, then $xyz \neq 1$.*

Proof. Since x is an involution in G, the -1 eigenspace of x on V either has dimension at least eight or has dimension at most four. If this dimension is at least eight, then x and y have a common eigenvector v with $xv = -v$, whence xy is not unipotent. If this dimension is at most four and $xyz = 1$, then $2 = \dim C_V(z) \geqslant \dim C_V(x) \cap C_V(y) \geqslant 4$, a contradiction. □

https://doi.org/10.1112/S0010437X14007271 Published online by Cambridge University Press

5. Rigidity for E_8

Let p be a prime with $p \geqslant 7$. Let $G = E_8(k)$ with k an algebraic closure of the prime field $\mathbb{F}_p$. Let C_1 be the conjugacy class of involutions with centralizer $D_8(k)$, C_2 the unipotent conjugacy class $4A_1$ and C_3 the class of regular unipotent elements in G. Observe that since $p > 5$, the centralizers of elements in these classes are connected and so $C_i \cap E_8(q)$ is a single conjugacy class for any finite subfield $\mathbb{F}_q \leqslant k$.

Lemma 5.1. *Let G be a simple algebraic group with a maximal parabolic subgroup P. Write $P = QL$ where Q is the unipotent radical of P and L is a Levi subgroup. If $u \in P$ is a regular unipotent element in P and $u = u_1u_2$ where $u_1 \in Q$ and $u_2 \in L$, then u_2 is a regular unipotent of L.*

Proof. Let B be a Borel subgroup of P containing u. Let T be a maximal torus of B and $X_\alpha = \{x_\alpha(t) \mid t \in k\}$ be the root subgroup in B corresponding to a positive root α. So we may write $u = \prod x_\alpha(t_\alpha)$. By conjugating, we may assume that $L = \langle T, X_\beta \rangle$ for all roots β not involving the simple root defining P. Then u is regular if and only if $t_\alpha \neq 0$ for all simple roots α, whence u_1 is a regular unipotent element of L. □

Theorem 5.2. *Let $G = E_8(k)$ with k an algebraic closure of $\mathbb{F}_p$ with $p > 5$. If $(x, y, z) \in C_1 \times C_2 \times C_3$ with $xyz = 1$, then $\langle x, y \rangle \cong E_8(q)$ with $q = p^a$ for some a.*

Proof. Assume that $H := \langle x, y \rangle$ does not contain a conjugate of $E_8(p)$. By Corollary 3.7, it follows that H is contained in a maximal closed subgroup of G of positive dimension. By [SS97, Theorem A], the only reductive such subgroup would be isomorphic to $A_1(k)$. Since $A_1(k)$ has a unique conjugacy class of unipotent elements, it cannot intersect both y^G and z^G.

The remaining possibility is that $H \leqslant P$ where P is a maximal parabolic subgroup. Write $P = QL$ where L is a Levi subgroup of P and Q is the unipotent radical. Set $S = [L, L]$. Since y and z are unipotent, $H \leqslant [P, P] = QS$.

Write $x = x_1x_2$, $y = y_1y_2$ and $z = z_1z_2$ where $x_1, y_1, z_1 \in Q$ and $x_2, y_2, z_2 \in L$. By Lemma 5.1, z_2 is a regular unipotent element in L.

It follows by [La95] that if S_1 is a direct factor of S of type A, then the projection of y_2 in S_1 is a nontrivial quadratic unipotent element (because of the Jordan block structure on the adjoint module). Applying Lemma 4.1 gives a contradiction if $S_1 \cong A_j(k)$ with $j \geqslant 2$.

Thus, $S \cong E_7(k), \mathrm{Spin}_{14}(k)$ or $A_1(k)E_6(k)$. If $S = \mathrm{Spin}_{14}(k)$, it follows by [La95] that y_2 is either a quadratic unipotent element or has one Jordan block of size three and all other Jordan blocks of size at most two. Now Lemma 4.3 gives a contradiction.

So we see that either $S \cong E_7(k)$ or $A_1(k)E_6(k)$. Suppose that $S = A_1(k)E_6(k)$. It then follows that x_2 must be trivial in $A_1(k)$ by Lemma 4.1. So in this case H is contained in a (nonmaximal) parabolic subgroup P_1 with unipotent radical Q_1 and semisimple part $E_6(k)$. Let H_0 be the projection of H in $E_6(k)$. By [La95], it follows that y_2 will be in one of the classes $3A_1, 2A_1, A_1$ or 1. Let $J = E_6(k) \leqslant S$. Let V be the Lie algebra of J. Then $\dim[x_2, V] \leqslant 40$ and $\dim[y_2, V] \leqslant 40$. It follows that $\dim[x_2, V] + \dim[y_2, V] + \dim[z_2, V] \leqslant 152$. By Scott's lemma [Sc77], H_0 has a fixed point on V (since V is a self-dual module). Thus, H_0 is contained in a positive-dimensional maximal closed subgroup M of J by Lemma 3.1. By [SS97], this implies that M is either parabolic or $M \cong F_4(k)$. If H_0 is contained in a proper parabolic subgroup of $E_6(k)$, then H is contained in at least three non-conjugate maximal parabolic subgroups. However, this contradicts the fact that there are at most two maximal parabolic subgroups containing our triple (i.e. the $E_7(k)$ parabolic or the $A_1(k)E_6(k)$ parabolic). So H_0 is not contained in a proper parabolic subgroup of $E_6(k)$.

https://doi.org/10.1112/S0010437X14007271 Published online by Cambridge University Press

Thus, H_0 is contained in $F_4(k)$. By Theorem 3.4, H_0 is not contained in a Lie primitive subgroup of $F_4(k)$. By [SS97], H_0 is not contained in a proper positive-dimensional subgroup of $F_4(k)$. This implies that H_0 contains a conjugate of $F_4(p)$. However, $F_4(p)$ has no fixed points on V (V is a direct sum of the adjoint module for $F_4(p)$ and an irreducible 26-dimensional module). Thus, this case cannot occur.

It follows that H is contained only in an $E_7(k)$ parabolic. Since $E_7(k)$ in $E_8(k)$ is simply connected, it follows that x_2 has centralizer $D_6(k)A_1(k)$. Arguing as above, we see that y_2 is in the closure of $4A_1$ (in $E_7(k)$). Let W denote the Lie algebra of $E_7(k)$. It follows that $\dim[x_2, W] + \dim[y_2, W] + \dim[z_2, W] < 2 \dim W$, whence H has a fixed point acting on W and so QH is contained in a positive-dimensional subgroup of P. By [SS97], H is either contained in a proper parabolic subgroup of P or in $X := A_1(k) \wr \mathrm{L}_2(7)$ with $p = 7$. In the first case, H would be contained in another maximal parabolic subgroup (not of type E_7), a contradiction. In the latter case, we note that a regular unipotent element of G has order 49 and in particular is not contained in $F^*(X)$. Note that y has order seven and all Jordan blocks of y on the Lie algebra of E_8 have size at most four [La95]. However, any unipotent element of X outside $F^*(X)$ has a Jordan block of size seven on any module where $F^*(X)$ acts nontrivially. This contradiction completes the proof. □

THEOREM 5.3. *The subvariety $X = \{(x, y, z) \in C_1 \times C_2 \times C_3 \mid xyz = 1\}$ of G^3 is a regular G-orbit and if $(x, y, z) \in X$, then $\langle x, y\rangle$ is a conjugate of $E_8(p)$. In particular, $(C_i \cap E_8(p) \mid 1 \leqslant i \leqslant 3)$ is a rationally rigid triple.*

Proof. Let $q = p^a$ for some a. We first want an estimate of the size of $X(q)$, the set of $\mathbb{F}_q$-points of X. As we have already observed, $C_i(q) := C_i \cap E_8(q)$ is a single conjugacy class in $E_8(q)$.

Let $x_i \in C_i \cap E_8(p)$. Then

$$|X(q)| = \frac{|C_1(q)|C_2(q)||C_3(q)|}{|G|} \sum_{\chi} \frac{\chi(x_1)\chi(x_2)\chi(x_3)}{\chi(1)},$$

where the sum is over all irreducible characters of $E_8(q)$. By Theorem 2.7, $|X(q)| \leqslant (1 + \epsilon)q^{248}$ for q sufficiently large (for a given $\epsilon > 0$).

By Theorem 5.2, the centralizer of any triple in X is trivial, whence any G-orbit in X has dimension 248 and any $G(q)$-orbit has size $|G(q)| = q^{248} + O(q^{247})$. It follows that $X(q)$ is a single $G(q)$-orbit for q sufficiently large. Thus, X is a single G-orbit and as we have observed any orbit is regular.

Note that X is defined over $\mathbb{F}_p$. So by Lang's theorem (since the stabilizer of a point of the orbit X is trivial and in particular connected), the $\mathbb{F}_p$-points of X form a single $E_8(p)$-orbit. Applying Theorem 5.2 once again, we see that any triple generates a subgroup isomorphic to $E_8(p)$. □

An application of the rigidity criterion (see, for example, [MM99, Theorem I.4.8]) now completes the proof of Theorem 1.3.

6. Characteristic zero

6.1 Fields

Let G be a simple algebraic group of type G_2 or E_8 over an algebraically closed field k of characteristic zero with the conjugacy classes C_i defined as in Table 1. Let X be the variety of

https://doi.org/10.1112/S0010437X14007271 Published online by Cambridge University Press

triples $(x, y, z) \in C_1 \times C_2 \times C_3$ with product one. Note that this variety is actually defined over $\mathbb{Z}[1/2]$ (since the conjugacy classes are defined over $\mathbb{Z}[1/2]$).

We can extend our results to characteristic zero in a fairly straightforward manner. First we note the following result.

Lemma 6.1. *Let k be an algebraically closed field of characteristic zero. Then $X(k)$ is an irreducible variety of dimension* 248.

Proof. As we have noted, X is defined over $\mathbb{Z}[1/2]$. Thus, $\dim X(\bar{\mathbb{Q}}) = \dim X(\overline{\mathbb{F}_p})$ for p sufficiently large. This implies the statement about dimension. Similarly, since $X(\overline{\mathbb{F}_p})$ is irreducible for all $p > 5$, the same is true for $X(\bar{\mathbb{Q}})$ (all this is saying is that if R is an affine commutative ring over $S := \mathbb{Z}[1/n]$ and $R \otimes_S \overline{\mathbb{F}_p}$ is a domain for all large p, then $R \otimes_S \bar{\mathbb{Q}}$ is as well). □

We can prove a variant of Theorem 5.2 in characteristic zero.

Theorem 6.2. *Let $G = E_8(k)$ with k an algebraically closed field of characteristic* 0. *If $(x, y, z) \in X(k)$, then $H := \langle x, y \rangle$ is Zariski dense in G.*

Proof. Just as in the proof of Theorem 5.2, we see that H is not contained in a proper parabolic subgroup of G. Since unipotent elements have infinite order, the only other possibility would be that H is contained in a closed reductive subgroup L of G containing a regular unipotent element. By [SS97, Theorem 1], $L \cong A_1(k)$. Thus, all unipotent elements of L are conjugate, a contradiction. □

Theorem 6.3. *Let k_0 be a field of characteristic zero. Let k be an algebraic closure of k_0. Let $G(k_0)$ be the split group over k_0 (of type G_2 or E_8):*

(i) *$X(k_0)$ is a regular G-orbit; and*

(ii) *if $(x, y, z) \in X(k)$, then $\langle x, y \rangle$ is a Zariski-dense subgroup of $G(k)$ which is conjugate to a subgroup of $G(\mathbb{Q})$.*

Proof. We only give the proof for E_8, the one for G_2 being identical (but easier). It follows by Theorem 6.2 that if $(x, y, z) \in X$, then the centralizer of $\langle x, y \rangle$ is trivial. In particular, every $G(k)$-orbit on $X(k)$ has dimension 248 by Lemma 6.1, whence $X(k)$ is a regular $G(k)$-orbit. If (x, y, z) and (x', y', z') are in $X(k_0)$, then $g \cdot (x, y, z) = (x', y', z')$ for some $g \in G(k)$. If σ is in the absolute Galois group of k/k_0, then $\sigma(g)$ also takes (x, y, z) to (x', y', z') whence $\sigma(g) = g$ and so $g \in G(k_0)$. This shows that $X(k_0)$ is either empty or is a single regular $G(k_0)$-orbit.

We now show that $X(k_0)$ is nonempty. Fix $z \in C_3$ in $G(\mathbb{Q})$ (for example, take z the product over a set of nontrivial elements from root subgroups for the simple roots). Let $D = C_G(z)$. Note that D is a connected abelian unipotent group of dimension r, the rank of G.

Let Y be the subvariety of X with the third coordinate equal to z. Note that Y is a regular D-orbit (because X is a regular G-orbit). Thus, Y defines a D-torsor [Se02, I.5.3]. Since connected unipotent groups have no nontrivial torsors (by the additive version of Hilbert's Theorem 90 [Se02, III.2.1]), it follows that $Y(\mathbb{Q})$ is nonempty and so $X(k_0)$ is nonempty. Thus, if $(x, y, z) \in X$ we see that $\langle x, y \rangle$ is conjugate to a subgroup of $G(\mathbb{Q})$ and is Zariski dense (by Theorem 6.2). □

6.2 The p-adic case

Here we give elementary proofs for some more general results for the p-adic case.

Fix a prime p and set $\mathbb{Z}_p$ to be the ring of p-adic integers with field of fractions $\mathbb{Q}_p$. Let K be a finite unramified extension of $\mathbb{Q}_p$ with R the integral closure of $\mathbb{Z}_p$ in K. Let G be a split

https://doi.org/10.1112/S0010437X14007271 Published online by Cambridge University Press

simply connected simple Chevalley group over R. Let P be the maximal ideal of R over p. Say $R/P \cong \mathbb{F}_q$. For convenience, we assume that $q > 4$.

Let N_j be the congruence kernel of the natural map from $G(R)$ to $G(R/P^j)$ and set $N = N_1$.

LEMMA 6.4. *Let $x_1, \dots, x_r \in G(R)$ with $\prod x_i \in N$ and set $y_i = x_i N$. Assume that $\langle y_1, \dots, y_r \rangle = G(R)/N$. Then there are conjugates w_i of x_i such that $\prod w_i = 1$ and $x_i N = w_i N$. Moreover, $\langle x_1, \dots, x_r \rangle$ and $\langle w_1, \dots, w_r \rangle$ are dense in $G(R)$ in the p-adic topology.*

Proof. By induction and a straightforward compactness argument, it suffices to assume that $\prod x_i \in N_j$ and then show that we can choose $n_{ij} \in N_j$ so that $\prod x_i^{n_{ij}} \in N_{j+1}$. This follows from the fact that $\langle y_1, \dots, y_r \rangle = G(R)/N$ and $G(R)/N$ has no covariants on $N_j/N_{j+1} \cong \mathrm{Lie}(G(R)/N)$ (see [We96, 3.5]).

The fact that $\langle w_1, \dots, w_r \rangle$ and $\langle x_1, \dots, x_r \rangle$ are each dense in $G(R)$ follows from the fact that N is contained in the Frattini subgroup of $G(R)$ (see [We96]). □

Remark 6.5. If $y_1, \dots, y_r \in G(R)/N$ with $\prod y_i = 1$, where the order of each y_i is prime to p and $\langle y_1, \dots, y_r \rangle = G(R)/N$, then we can lift each y_i to an element $x_i \in G(R)$ with $y_i = x_i N$ and y_i of the same order as x_i and so the previous result applies in this case. See [GT13] for a more general result.

THEOREM 6.6. *Let $p > 5$ be prime. Let C_1, C_2, C_3 be the conjugacy classes in $G = E_8$ given in Table 1. Then*

$$Y := \{(x_1, x_2, x_3) \mid x_i \in C_i \cap G(R), x_1 x_2 x_3 = 1, \langle x_1, x_2 \rangle \textit{ is dense in } G(R)\}$$

is a single regular orbit of $G(R)$.

Proof. By Theorem 5.3 and Lemma 6.4, Y is nonempty. Any two points of Y are in the same $G(K)$-orbit via some $g \in G(K)$. However, since both triples generate dense subgroups of $G(R)$, g normalizes $G(R)$ and $G(R)$ is self-normalizing, so $g \in G(R)$. □

Finally, we show that there are triples in X which are close to integral.

THEOREM 6.7. *Let G be a simple algebraic group of type G_2 or E_8. Let m be the product of the bad primes for G. Set $S = \mathbb{Z}[1/m]$. There exists $(x, y, z) \in X \cap G(S)^3$ such that $\langle x, y \rangle$ is dense in $G(\mathbb{Z}_p)$ for all good primes p.*

Proof. Let $K = \mathbb{Q}_p$ with p a good prime for G. Let D_i, $i = 1, 2, 3$, be the corresponding conjugacy classes in $G(\mathbb{F}_p) = G(R)/N$ and let C_i be the classes in $G(\mathbb{Q})$. By Lemma 6.4, we can choose $w_i \in C_i \cap G(R)$ with $w_1 w_2 w_3 = 1$. Note that if $w := (w_1, w_2, w_3) \in Y(R)$, then since $\Gamma(w) := \langle w_1, w_2 \rangle$ is dense in $G(R)$, it follows that $G(R)$ acts regularly on those elements in $X(R)$ which generate a dense subgroup of $G(R)$.

By Theorem 6.3, we may choose $x \in X(\mathbb{Q})$. Thus, $x \in X(\mathbb{Z}[1/d])$ for some positive (squarefree) integer d which is a multiple of the bad primes. Moreover, by replacing d by a multiple, we may assume that $\Gamma(x)$ surjects onto $G(\mathbb{F}_p)$ and in particular generates a dense subgroup of $G(\mathbb{Z}_p)$ for any p which does not divide d. Suppose that some good prime p divides d. By Lemma 6.4, we may choose $y \in X(\mathbb{Z}_p)$ with $\Gamma(y)$ generating a dense subgroup of $G(\mathbb{Z}_p)$. So $y = g.x$ for some $g \in G(\mathbb{Q}_p)$.

We note that $G(\mathbb{Q}_p) = G(\mathbb{Z}[1/p])G(\mathbb{Z}_p)$. Indeed, $G(\mathbb{Z}_p)$ is open in $G(\mathbb{Q}_p)$ in the p-adic topology, and $G(\mathbb{Z}[1/p])$ is dense in $G(\mathbb{Q}_p)$, since $\mathbb{Z}[1/p]$ is dense in $\mathbb{Q}_p$ and $G(\mathbb{Q}_p)$ is generated by root subgroups each isomorphic to $\mathbb{Q}_p$. So write $g = g_1 g_2$ where $g_1 \in G(\mathbb{Z}[1/p])$ and $g_2 \in G(\mathbb{Z}_p)$.

https://doi.org/10.1112/S0010437X14007271 Published online by Cambridge University Press

Thus, $g_1^{-1}.y = g_2.x$, and so $w := g_1^{-1}.y = g_2.x \in G(\mathbb{Z}[1/d]) \cap G(\mathbb{Z}_p) = G(\mathbb{Z}[1/d'])$ where $d = pd'$. Moreover, we see that $\Gamma(w)$ surjects onto $G(\mathbb{F}_r)$ for any r not dividing d' (because y and so $g_1^{-1}.y$ have this property and also for $r = p$ since $g_2.x$ has this property).

Continuing in this manner, we see that we can produce such an embedding into $G(S)$ as required. □

Note that the results of this section give Theorem 1.2.

For $G = G_2$, Dettweiler and Reiter [DR10] exhibited a triple in $X(\mathbb{Z})$ (and so every triple generates a subgroup conjugate to one in $G(\mathbb{Z})$). If $G = E_8$, we do not know if the group generated by our triple is in fact conjugate to a subgroup of $G(\mathbb{Z})$.

Suppose that $x = (x_1, x_2, x_3) \in X(\mathbb{Z})$. Let $\Gamma = \Gamma(x)$. Let $W = \mathrm{Lie}(G(\mathbb{F}_2))$ and $V = \mathrm{Lie}(G(\mathbb{C}))$. It is clear that $\dim[x_i, W] \leqslant \dim[x_i, V]$ and since x_1 is an involution, $\dim[x_1, W] \leqslant (1/2)\dim W < \dim[x_1, V]$. Thus,

$$\sum \dim[x_i, W] < \sum \dim[x_i, V] = 2\dim W.$$

By Scott's Lemma [Sc77] it follows that the image of Γ in $G(\mathbb{F}_2)$ either has fixed points or covariants on W. Since $G(\mathbb{F}_2)$ has no fixed points on W, it follows that the image of Γ is a proper subgroup of $G(\mathbb{F}_2)$. Indeed, the same shows that the image of Γ is contained in a proper positive-dimensional subgroup of $G(\overline{\mathbb{F}_2})$.

7. Remarks on F_4

Let k be an algebraically closed field of characteristic $p > 3$ and $G = F_4(k)$. Let C_1 be the conjugacy class of G consisting of involutions with centralizer $A_1(k)C_3(k)$, C_2 the conjugacy class of unipotent elements $A_1 + \tilde{A}_1$ and C_3 the conjugacy class of regular unipotent elements. We set

$$X := \{(x, y, z) \in C_1 \times C_2 \times C_3 \mid xyz = 1\}.$$

The character theory proof as in Theorem 2.7 goes through for this set of triples showing that $\dim X = 52$ and there is at most one component of dimension 52. By standard intersection theory, any component of X has dimension at least 52, whence we obtain the following result.

Proposition 7.1. *The variety X is irreducible of dimension* 52.

If $x = (x_1, x_2, x_3) \in X$, let $\Gamma(x) = \langle x_1, x_2\rangle$.

Unfortunately, no triple in X generates an $F_4(p)$ because elements of both C_1 and C_2 have a 14-dimensional fixed space on the 26-dimensional module V for G (see [La95]). Thus, if $x_i \in C_i$, $\langle x_1, x_2\rangle$ has at least a two-dimensional fixed space on V. Since x_3 has a two-dimensional fixed space on V, this is precisely the fixed space of $\Gamma(x)$. Choose a B_3-parabolic subgroup P containing x_3. Then P has a unique one-dimensional invariant space on V, whence it follows that $\Gamma(x) < P$.

We can show the following result.

Theorem 7.2. *If $(x_1, x_2, x_3) \in X$, then $\langle x_1, x_2, x_3\rangle = RG_2(p)$ where R is nilpotent of class two and has order p^{14}. Moreover, X is a single regular G-orbit.*

Proof. Consider $G_2(k) < B_3(k) < QB_3(k) < P < G$ where P is a maximal parabolic subgroup and Q is the unipotent radical of P.

By [CKS76, Proposition 4.5], $[Q, Q]$ is the natural seven-dimensional module for $B_3(k)$ and $A := Q/[Q, Q]$ is the eight-dimensional spin module for $B_3(k)$. Since $G_2(k)$ has only nontrivial irreducible modules of dimension 7 or dimension at least 14, it follows that as $G_2(k)$-modules,

https://doi.org/10.1112/S0010437X14007271 Published online by Cambridge University Press

$[Q, Q]$ is irreducible and $A \cong k \oplus B$ with B a seven-dimensional irreducible module for $G_2(k)$ (it must split because A is self-dual). Note that an element of Q fixed by $G_2(k)$ (even modulo $[Q, Q]$) is not of the form $u_4(t)$ for some $t \neq 0$ (because the stabilizer of such an element is a maximal parabolic subgroup of $B_3(k)$ and so does not contain $G_2(k)$).

Let $x \in G_2(k)$ be an involution, $y \in G_2(k)$ a unipotent element in the class $\tilde{A}_1$ and z in the class of regular unipotent elements of $G_2(k)$ with $xyz = 1$. Then, by the rigidity result for $G_2(k)$, $\langle x, y\rangle \cong G_2(p)$ and so we may assume that $\langle x, y\rangle = G_2(p)$. Moreover, by conjugating in $G_2(p)$, we may assume that $z = u_1(1)u_2(1)u_3(1)$ where $\{u_i(t) \mid t \in k\}$, $1 \leqslant i \leqslant 3$, are the root subgroups corresponding to the simple roots of G inside $B_3(k)$.

It is straightforward to see that $\dim C_G(x) = 24$ and that y has the same Jordan block structure on the adjoint module for G as do elements in C_2. This implies that $x \in C_1$ and $y \in C_2$.

By the remarks above, $[G_2(p), Q]$ is a codimension-one subgroup of Q. Indeed, setting $R = Q(p)$, we see that $R_0 := [G_2(p), R]$ has order p^{14} and has index p in $Q(p)$. It follows easily that every element of R_0 can be written as $[x, q_1][y, q_2]$ for some $q_1, q_2 \in Q(p)$. In particular, $u_4(-1) = [x, q_1][y, q_2]v$ where $q_1, q_2 \in Q(p)$ and v is a product of root elements in R corresponding to nonsimple roots. Let $q_3 \in R$ with $x^{q_1}y^{q_2}(q_3z) = 1$. Then $q_3z = \prod_{i=1}^{4} u_i(1)v'$ where v' is a product of root elements in R corresponding to nonsimple roots. In particular, q_3z is a regular unipotent element of G.

Thus, we have produced a triple $w := (w_1, w_2, w_3) = (x^{q_1}, y^{q_2}, q_3z) \in X$. Note that $H := \Gamma(w) \leqslant [R, G_2(p)]G_2(p)$. Since H contains a regular unipotent element, $H[R, R]/[R, R]$ intersects $R/[R, R]$ nontrivially. The argument above shows that x does not act trivially on this intersection, whence $H[R, R]/[R, R]$ contains the hyperplane $R_0[R, R]/[R, R]$ of $R/[R, R]$. Note that $H \cap [R, R] \neq 1$ for otherwise $H \cap [R, R]$ is abelian of order at least p^7 and centralizes $[R, R] < Z(Q)$. Then $(H \cap R)[R, R]$ is abelian of order p^{14} (and this is not possible, either by inspection or by [GLS98, Table 3.3.1]). Since H acts irreducibly on $[R, R]$, this implies that $[R, R] \leqslant H$. Thus, $H \cap R = [G_2(p), R]$ has index p in R.

We next claim that $C := C_G(H) = 1$. Suppose not. Since $G_2(p)$ is self centralizing in $B_3(k)$ and $C \leqslant C_G(w_3) < P$, it follows that $C \leqslant Q$. Since $G_2(p)$ acts without fixed points on $[G_2(p), Q]$, it follows that $C \cap [G_2(p), Q] = 1$. Let T be the torus centralizing $B_3(k)$. Then T normalizes H (because it centralizes $G_2(k)$ and normalizes Q). Thus, T also normalizes C. Since $C_Q(T) = 1$, it follows that C has positive dimension and that $Q = [G_2(p), Q]C$, whence C centralizes Q. Thus, $C \leqslant Z(Q) = [Q, Q]$, a contradiction.

We next show that any $x = (x_1, x_2, x_3) \in X$ is as above. As noted, we may assume that $x_3 \in P$ and so $H \leqslant P_3$.

Arguing as in the E_8 case, we see that HQ/Q cannot be contained in a parabolic subgroup of $B_3(k)$. It follows easily from the fact that HQ/Q contains a regular unipotent element of $B_3(k)$ that either HQ/O contains a conjugate of $B_3(p)$ or is contained in $G_2(k)$. Arguing as above, we see that in HQ/Q, the x_iQ are precisely in the rigid classes for G_2 (inside B_3). Note that on the eight-dimensional module W for B_3, $\sum \dim[x_i, W] < 16$, whence by Scott's Lemma, H does not act irreducibly on W and so $HQ/Q \leqslant G_2(k)$. By the rigidity result for $G_2(k)$, this implies that $HQ/Q \cong G_2(p)$. Now we argue as above to conclude that $H = [R, G_2(p)]G_2(p)$ and has trivial centralizer in G.

By Proposition 7.1 we conclude that since X is an irreducible variety of dimension 52 and every orbit of G on X has dimension 52, X is a single G -orbit. □

https://doi.org/10.1112/S0010437X14007271 Published online by Cambridge University Press

There are several other candidates for rigid triples (satisfying the necessary condition that $\sum \dim C_i = 2 \dim G$). In all cases, C_3 will be the regular unipotent class. The possibilities are:

(i) C_1 consists of involutions of type B_4 and C_2 consists of unipotent elements of type $F_4(a_3)$;

(ii) C_1 consists of involutions of type A_1C_3 and C_2 is the class of elements which are a commuting product of a B_4-involution and a long root element;

(iii) C_1 consists of unipotent elements of type $A_1 + \tilde{A}_1$ and C_2 is the class of elements which are a commuting product of a B_4-involution and a long root element.

The second triple was suggested by Yun and it was recently shown [GLY14] that this triple does give a rationally rigid triple in $F_4(p)$, $p > 3$.

Acknowledgements

The first author was partially supported by the NSF grant DMS-1001962 and the Simons Foundation Fellowship 224965. He also thanks the Institute for Advanced Study for its support. The second author gratefully acknowledges financial support by ERC Advanced Grant 291512.

We thank Zhiwei Yun for asking the question and for helpful remarks. We thank Burt Totaro for some suggestions which helped simplify the proof of Theorem 1.2. We thank Stefan Reiter for observing that the original triple we considered for F_4 could not work by considering the action on the 26-dimensional module. Finally, we thank Frank Lübeck and the referees for their careful reading and helpful comments.

References

As91 M. Aschbacher, The maximal subgroups of E_6, Preprint (1991).

Ca93 R. W. Carter, *Finite groups of Lie type. Conjugacy classes and complex characters*, Wiley Classics Library (John Wiley and Sons, Chichester, 1993).

Co81 B. N. Cooperstein, *Maximal subgroups of* $G_2(2^n)$, J. Algebra **70** (1981), 23–36.

CKS76 C. Curtis, W. M. Kantor and G. M. Seitz, *The 2-transitive permutation representations of the finite Chevalley groups*, Trans. Amer. Math. Soc. **218** (1976), 1–59.

DR10 M. Dettweiler and S. Reiter, *Rigid local systems and motives of type* G_2*. With an appendix by Michael Dettweiler and Nicholas M. Katz*, Compositio Math. **146** (2010), 929–963.

DM91 F. Digne and J. Michel, *Representations of finite groups of Lie type*, London Mathematical Society Student Texts, vol. 21 (Cambridge University Press, Cambridge, 1991).

Di12 J. DiMuro, *On prime power order elements of general linear groups*, J. Algebra **367** (2012), 222–236.

FF85 W. Feit and P. Fong, *Rational rigidity of* $G_2(p)$ *for any prime* $p > 5$, in *Proceedings of the Rutgers group theory year 1983–1984 (New Brunswick, NJ)* (Cambridge University Press, Cambridge, 1985), 323–326.

GLS98 D. Gorenstein, R. Lyons and R. Solomon, *The classification of the finite simple groups. Number 3*, Mathematical Surveys and Monographs (American Mathematical Society, Providence, RI, 1998).

GLY14 R. M. Guralnick, F. Lübeck and J. Yu, Rational rigidity for $F_4(p)$, Preprint (2014).

GPPS99 R. M. Guralnick, T. Penttila, C. Praeger and J. Saxl, *Linear groups with orders having certain large prime divisors*, Proc. Lond. Math. Soc. (3) **78** (1999), 167–214.

GT13 R. M. Guralnick and P. Tiep, *Lifting in Frattini covers and a characterization of finite solvable groups*, J. Reine Angew. Math., published online (2013), doi:10.1515/crelle-2013-0085.

https://doi.org/10.1112/S0010437X14007271 Published online by Cambridge University Press

JP76 W. Jones and B. Parshall, *On the 1-cohomology of finite groups of Lie type*, in *Proceedings of the conference on finite groups (University of Utah, Park City, 1975)* (Academic Press, New York, 1976), 313–328.

Kl88 P. B. Kleidman, *The maximal subgroups of the Chevalley groups $G_2(q)$ with q odd, the Ree groups ${}^2G_2(q)$, and their automorphism groups*, J. Algebra **117** (1988), 30–71.

La95 R. Lawther, *Jordan block sizes of unipotent elements in exceptional algebraic groups*, Comm. Algebra **23** (1995), 4125–4156.

La09 R. Lawther, *Unipotent classes in maximal subgroups of exceptional algebraic groups*, J. Algebra **322** (2009), 270–293.

La R. Lawther, *Sublattices generated by root differences*, J. Algebra, to appear.

LLM11 M. W. Liebeck, A. J. Litterick and C. Marion, *A rigid triple of conjugacy classes in G_2*, J. Group Theory **41** (2011), 31–35.

LS99 M. W. Liebeck and G. M. Seitz, *On finite subgroups of exceptional algebraic groups*, J. Reine Angew. Math. **515** (1999), 25–72.

LS03 M. W. Liebeck and G. M. Seitz, *A survey of maximal subgroups of exceptional groups of Lie type*, in *Groups, combinatorics and geometry (Durham, 2001)* (World Scientific, River Edge, NJ, 2003), 139–146.

Lu01 F. Lübeck, *Small degree representations of finite Chevalley groups in defining characteristic*, LMS J. Comput. Math. **4** (2011), 135–169.

Lu86 G. Lusztig, *Character sheaves V*, Adv. Math. **61** (1986), 103–155.

Lu88 G. Lusztig, *On the representations of reductive groups with disconnected centre*, Astérisque **168** (1988), 157–166.

Ma90 K. Magaard, *The maximal subgroups of $F_4(F)$ where F is a finite or algebraically closed field of characteristic* $\neq 2, 3$, PhD thesis, Caltech (1990).

MM99 G. Malle and B. H. Matzat, *Inverse Galois theory*, Springer Monographs in Mathematics (Springer, Berlin, 1999).

MT11 G. Malle and D. Testerman, *Linear algebraic groups and finite groups of Lie type*, Cambridge Studies in Advanced Mathematics, vol. 133 (Cambridge University Press, Cambridge, 2011).

Mc98 G. McNinch, *Dimensional criteria for semisimplicity of representations*, J. Lond. Math. Soc. (2) **76** (1998), 95–149.

Mi J. Michel, The GAP-part of the Chevie system. GAP 3-package available for download from http://people.math.jussieu.fr/∼jmichel/chevie/chevie.html.

SS97 J. Saxl and G. M. Seitz, *Subgroups of algebraic groups containing regular unipotent elements*, J. Lond. Math. Soc. (2) **55** (1997), 370–386.

Sc77 L. L. Scott, *Matrices and cohomology*, Ann. of Math. (2) **105** (1977), 473–492.

ST90 G. M. Seitz and D. Testerman, *Extending morphisms from finite to algebraic groups*, J. Algebra **131** (1990), 559–574.

ST93 G. M. Seitz and D. Testerman, *Subgroups of type A_1 containing semiregular unipotent elements*, J. Algebra **196** (1997), 595–619.

Se02 J. -P. Serre, *Galois cohomology*, Springer Monographs in Mathematics (Springer, Berlin, 2002), corrected reprint of the 1997 English edition.

Si92 P. Sin, *On the 1-cohomology of the groups $G_2(2^n)$*, Comm. Algebra **20** (1992), 2653–2662.

Si93 P. Sin, *Extensions of simple modules for $G_2(3^n)$ and ${}^2G_2(3^m)$*, Proc. Lond. Math. Soc. (2) **66** (1993), 327–357.

Sp85 N. Spaltenstein, *On the generalized Springer correspondence for exceptional groups*, in *Algebraic groups and related topics (Kyoto/Nagoya, 1983)*, Advanced Studies in Pure Mathematics, vol. 6 (North-Holland, Amsterdam, 1985), 317–338.

https://doi.org/10.1112/S0010437X14007271 Published online by Cambridge University Press

Su09 I. Suprunenko, *The minimal polynomials of unipotent elements in irreducible representations of the classical groups in odd characteristic*, Memoirs of the American Mathematical Society, vol. 200, no. 939 (American Mathematical Society, Providence, RI, 2009).

Th85 J. G. Thompson, *Rational rigidity of* $G_2(5)$, in *Proceedings of the Rutgers group theory year, 1983–1984 (New Brunswick, NJ, 1983–1984)* (Cambridge University Press, Cambridge, 1985), 321–322.

We96 T. Weigel, *On the profinite completion of arithmetic groups of split type*, in *Lois d'algèbres et variétés algébriques (Colmar, 1991)*, Travaux en Cours, vol. 50 (Hermann, Paris, 1996), 79–101.

Yu14 Z. Yun, *Motives with exceptional Galois groups and the inverse Galois problem*, Invent. Math. **196** (2014), 267–337.

Z13 D. Zywina, The inverse Galois problem for $\mathrm{L}_2(\mathbb{F}_p)$, Preprint (2013), arXiv:1303.3646.

Robert Guralnick guralnic@usc.edu
Department of Mathematics, University of Southern California,
Los Angeles, CA 90089-2532, USA

Gunter Malle malle@mathematik.uni-kl.de
FB Mathematik, TU Kaiserslautern, Postfach 3049,
67653 Kaiserslautern, Germany

https://doi.org/10.1112/S0010437X14007271 Published online by Cambridge University Press