DEGREE 5 INVARIANT OF E_8

SKIP GARIBALDI AND NIKITA SEMENOV

Abstract. We give a formula for the recently-discovered degree 5 cohomological invariant of groups of type E_8. We use this formula to calculate the essential dimension and cohomological invariants of $H^1(*, \mathrm{Spin}_{16})_0$, and to give a precise interpretation of Serre's "funny-looking statement" in terms of embeddings finite subgroups in the split E_8.

1. Introduction

Let G be a split simple linear algebraic group over a field k of characteristic 0. One of the main goals of the theory of linear algebraic groups over arbitrary fields is to compute the Galois cohomology set $H^1(k, G)$.

One of the main tools was suggested by J-P. Serre in the 90s, namely the *Rost invariant*

$$r_G \colon H^1(*, G) \to H^3(*, \mathbb{Q}/\mathbb{Z}(2))$$

discovered by M. Rost and explained in Merkurjev's portion of the book [GMS]. It is a morphism of functors from the category of fields over k to the category of pointed sets.

Mimicking the situation in topology one can consider the kernel of the Rost invariant and try to define a cohomological invariant on it. In the theory of quadratic forms this procedure leads to the invariants defined on the powers of the fundamental ideal I^n.

In the present paper we consider the most complicated and yet unsettled case when G has Cartan-Killing type E_8. The paper is organized as follows. In Section 2 we recall the recently-discovered invariant u defined on the kernel of the Rost invariant for groups of type E_8. Section 3 is devoted to a computation of the value $u(G)$ for groups G obtained by a Tits construction. Sections 4 and 5 provide applications of u to cohomological invariants and essential dimension of Spin_{16}.

In the last section we investigate the finite subgroups of algebraic groups. It turns out that under some additional conditions cohomological invariants provide an obstruction for certain finite groups to be subgroups of algebraic groups. This is connected with Serre's "funny-looking statement" from [GR, p. 209]:

> "Let K be a field of characteristic 0, and G a group of type E_8 over K. Suppose that $\mathrm{SL}_2(32)$ can be embedded in $G(K)$. Then $\mathrm{PGL}_2(31)$ can be embedded in $G(K)$. Nice!"

More precisely, Serre proved that $\mathrm{PGL}_2(31)$ can be embedded in $G(K)$ iff G "is compact", i.e., isomorphic to the scalar extension of the anisotropic E_8 over $\mathbb{Q}$, and that $\mathrm{SL}_2(32)$ embeds in $G(K)$ iff G is compact and $\cos(2\pi/11)$ is in K. This led

2000 *Mathematics Subject Classification.* Primary 11E72; secondary 17B25, 20C33, 20G15.

him to the question: How to tell, e.g., if the split E_8 is compact in this sense? We show:

1.1. **Theorem.** $\mathrm{PGL}_2(31)$ *embeds in* $E_8(K)$ *if and only if* -1 *is a sum of* 16 *squares in* K. *The group* $\mathrm{SL}_2(32)$ *embeds in* $E_8(K)$ *if and only if* -1 *is a sum of* 16 *squares in* K *and* $\cos(2\pi/11)$ *is in* K.

2. Preliminaries

Let k denote a field of characteristic 0. We write E_8 for the split simple algebraic group with Killing-Cartan type E_8. The Galois cohomology set $H^1(k, E_8)$ classifies simple algebraic groups of type E_8 over k.

We put

$$H^1(k, E_8)_0 := \{\eta \in H^1(k, E_8) \mid r_{E_8}(\eta) \text{ has odd order}\}.$$

In [Sem 08, Corollary 8.7], the second author defined a morphism of functors:

$$u\colon H^1(*, E_8)_0 \to H^5(*, \mathbb{Z}/2\mathbb{Z}).$$

This is the degree 5 invariant from the title.

Let now G be a group of type E_8. It corresponds with a canonical element of $H^1(k, E_8)$, so it makes sense to speak of "the Rost invariant of G"; we denote it by $r(G)$. Suppose now that $r(G)$ has odd order, so G belongs to $H^1(k, E_8)_0$. The second author also proved in [Sem 08]:

(2.1) $u(G) = 0$ *if and only if there is an odd-degree extension of* k *that splits* G.

For example, the compact group G of type E_8 over $\mathbb{R}$ has Rost invariant zero and $u(G) = (-1)^5$.

As an obvious corollary, we have:

(2.2) *If* k *has cohomological dimension* ≤ 2, *then every* k*-group of type* E_8 *is split by an odd-degree extension of* k.

Serre's "Conjecture II" for groups of type E_8 is that in fact every group of type E_8 over such a field is split.

3. Tits's construction of groups of type E_8

3.1. There are inclusions of algebraic groups $G_2 \times F_4 \subset E_8$, where G_2 and F_4 denote split groups of those types. Furthermore, this embedding is essentially unique. Applying Galois cohomology gives a function $H^1(k, G_2) \times H^1(k, F_4) \to H^1(k, E_8)$. The first two sets classify octonion k-algebras and Albert k-algebras respectively, so this map gives a construction by Galois descent of groups of type E_8:

$$\boxed{\text{octonion } k\text{-algebras}} \times \boxed{\text{Albert } k\text{-algebras}} \to \boxed{\text{groups of type } E_8}$$

Jacques Tits gave concrete formulas on the level of Lie algebras for this construction in [T], see also [J]. This method of constructing groups of type E_8 is known as the *Tits construction*. (Really, Tits's construction is more general and gives other kinds of groups as well. The variety of possibilities is summarized in Freudenthal's magic square as in [Inv, p. 540]. However, the flavor in all cases is the same, and this case is the most interesting.)

Our purpose is to compute the value of u on those groups of type E_8 with Rost invariant of odd order (so that it makes sense to speak of u) and arising from Tits's construction. We do this in Theorem 3.7.

3.2. Following [Inv], we write $f_3(-)$ for the even component of the Rost invariant of an Albert algebra or an octonion algebra (equivalently, a group of type F_4 or G_2). We write $g_3(-)$ for the odd component of the Rost invariant of an Albert algebra; such algebras also have an invariant f_5 taking values in $H^5(k, \mathbb{Z}/2\mathbb{Z})$. *An Albert algebra A has $g_3(A) = 0$ and $f_5(A) = 0$ iff A has a nonzero nilpotent, iff the group* $\mathrm{Aut}(A)$ *is isotropic.*

Suppose now that $G \in H^1(k, E_8)$ is the image of an octonion algebra O and an Albert algebra A. It follows from a twisting argument as in the proof of Lemma 5.8 in [GQ] — and was pointed out by Rost as early as 1999 — that

$$r(G) = r_{G_2}(O) + r_{F_4}(A). \tag{3.3}$$

In particular, G belongs to $H^1(k, E_8)_0$ if and only if $f_3(O)+f_3(A) = 0$ in $H^3(k, \mathbb{Z}/2\mathbb{Z})$, i.e., if and only if $f_3(O) = f_3(A)$.

3.4. **Definition.** Define

$$t\colon H^1(*, F_4) \to H^1(*, E_8)_0$$

by sending an Albert k-algebra A to the group of type E_8 constructed from A and the octonion algebra with norm form $f_3(A)$, via Tits's construction from 3.1. By the preceding paragraph, $r(G) = g_3(A) \in H^3(k, \mathbb{Z}/3\mathbb{Z})$, so G does indeed belong to $H^1(k, E_8)_0$.

3.5. **Example.** *If A has a (nonzero) nilpotent element, then the group $t(A)$ is split.* Indeed, $g_3(A)$ is zero so $t(A)$ is in the kernel of the Rost invariant. Also, $t(A)$ is isotropic because it contains the isotropic subgroup $\mathrm{Aut}(A)$, hence $t(A)$ is split by, e.g., [Ga, Prop. 12.1(1)].

3.6. **Example.** In case $k = \mathbb{Q}$ or $\mathbb{R}$, there are exactly three Albert algebras up to isomorphism. All have $g_3 = 0$; they are distinguished by the values of f_3 and f_5.

$f_3(A)$	$f_5(A)$	$t(A)$
0	0	split by Example 3.5
$(-1)^3$	0	split by Example 3.5
$(-1)^3$	$(-1)^5$	anisotropic by [J, p. 118]

It follows from Chernousov's Hasse Principle for groups of type E_8 [PR] that for every number field K with a unique real place, the set $H^1(K, E_8)_0$ has two elements: the split group and the anisotropic group constructed as in the last line of the table.

3.7. **Theorem.** *For every Albert k-algebra A, we have:*

$$u(t(A)) = f_5(A) \quad \in H^5(k, \mathbb{Z}/2\mathbb{Z}).$$

Proof. The composition ut is an invariant $H^1(*, F_4) \to H^5(*, \mathbb{Z}/2\mathbb{Z})$, hence is given by

$$ut(A) = \lambda_5 + \lambda_2 \cdot f_3(A) + \lambda_0 \cdot f_5(A)$$

for uniquely determined elements $\lambda_i \in H^i(\mathbb{Q}, \mathbb{Z}/2\mathbb{Z})$, see [GMS, p. 50].

We apply this formula to each of the three lines in the table from Example 3.6. Obviously u of the split E_8 is zero, so the first line gives:

$$0 = u(\text{split } E_8) = \lambda_5 \quad \in H^5(\mathbb{Q}, \mathbb{Z}/2\mathbb{Z}).$$

Applying this to the second line gives:

$$0 = u(\text{split } E_8) = \lambda_2 \cdot (-1)^3 \in H^5(\mathbb{Q}, \mathbb{Z}/2\mathbb{Z}).$$

For the last line, u of the compact E_8 is $(-1)^5$ by (2.1), see the end of [Sem 08] for details. We find:

$$(-1)^5 = u(\text{compact } E_8) = \lambda_0 \cdot (-1)^5,$$

so λ_0 equals 1 in $H^0(\mathbb{Q}, \mathbb{Z}/2\mathbb{Z}) = \mathbb{Z}/2\mathbb{Z}$.

To show that $\lambda_2 = 0$ we proceed as follows. Consider the purely transcendental extension $F = \mathbb{Q}(x, y, z, a, b)$ and let H be the group of type F_4 with $f_3(H) = (x, y, z)$, $f_5(H) = f_3(H) \cdot (a, b)$ and $g_3(H) = 0$. Then $ut(H) = f_5(H) + f_3(H) \cdot \lambda_2$.

Let K be a generic splitting field for the symbol $f_5(H)$. Since H_K is isotropic, the resulting group $t(H)$ of type E_8 is isotropic over K, and, since it has trivial Rost invariant, it splits over K [Ga, Prop. 12.1]. Obviously, $ut(H)$ is killed by K. Therefore $f_3(H) \cdot \lambda_2$ is zero over K. If $f_3(H) \cdot \lambda_2$ is zero over F, then by taking residues we see that λ_2 is zero in $H^2(\mathbb{Q}(a, b), \mathbb{Z}/2\mathbb{Z})$, hence also in $H^2(\mathbb{Q}, \mathbb{Z}/2\mathbb{Z})$. Otherwise, $f_3(H) \cdot \lambda_2$ is equal to $f_5(H)$ by [OViVo, Theorem 2.1], and again completing and taking residues with respect to the x-, y-, and z-adic valuations, we find that $\lambda_2 = (a, b) \in H^2(\mathbb{Q}(a, b), \mathbb{Z}/2\mathbb{Z})$. But this is impossible because λ_2 is defined over $\mathbb{Q}$. This proves that $\lambda_2 = 0$. □

3.8. **Corollary.** *For every field k of characteristic zero and every group $G \in H^1(k, E_8)_0$ in the image of t, we have:*

$$\langle 60 \rangle (\mathrm{Kill}_G - \mathrm{Kill}_{E_8}) = 2^3 \cdot u(G) \quad \in I^8(k),$$

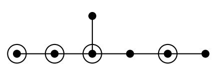
where Kill_- *denotes the Killing form of* $-$ *and* E_8 *the split group.*

Proof. Follows from [Ga, 13.5 and Example 15.9] and Theorem 3.7. □

3.9. **Example.** Whatever field k of characteristic zero one starts with, there is an extension K/k that supports an anisotropic 5-Pfister quadratic form q_5—one can adjoin 5 indeterminates to k, for example. Let q_3 be a 3-Pfister form dividing q_5 and let A be the Albert K-algebra with $f_d(A) = e_d(q_d)$ for $d = 3, 5$. The group $G := t(A)$ of type E_8 over K has Rost invariant zero yet $u(G) = f_5(A)$ nonzero by Theorem 3.7. In particular, G is not split, hence is anisotropic by [Ga, Prop. 12.1(1)].

Example 15.9 in [Ga] produced anisotropic groups of type E_8 in a similar manner, but used the Killing form to see that the resulting groups were anisotropic; that method does not work if -1 is a square in k. Roughly, Example 3.9 above exhibits more anisotropic groups because u is a finer invariant than the Killing form.

3.10. *Remark* (Application to E_7). Write E_7^{sc} for the split simply connected group of type E_7. The set $H^1(k, E_7^{\mathrm{sc}})_0$ is zero by [Ga 01]. Suppose now that G is simply connected with Tits index



i.e., non-split with a minimal parabolic subgroup that is "wesentlich" in the language of [H, p. 132]. Twisting the inclusion of $(\mathrm{SL}_2 \times E_7)/\mu_2$ in E_8 gives an embedding of G in (the split) E_8 and the composition $H^1(*, G)_0 \to H^1(*, E_8)_0 \xrightarrow{u} H^5(*, \mathbb{Z}/2\mathbb{Z})$ is an invariant. It is not difficult to show that this invariant is not zero if G has Tits algebra $(-1, -1)$ and $(-1)^5 \in H^5(k, \mathbb{Z}/2\mathbb{Z})$ is not zero. (And trivially that $H^1(k,G)_0$ may be nonzero.) One expects that the invariant is nonzero in general and that this follows from Theorem 3.7.

4. Invariants of $H^1(*, \mathrm{Spin}_{16})_0$

Recall from [Inv, pp. 436, 437] that the Rost invariant of a class $\eta \in H^1(k, \mathrm{Spin}_{16})$ is given by the formula

$$r_{\mathrm{Spin}_{16}}(\eta) = e_3(q_\eta) \quad \in H^3(k, \mathbb{Z}/2\mathbb{Z})$$

where q_η is the 16-dimensional quadratic form in I^3k corresponding to the image of η in $H^1(k, \mathrm{SO}_{16})$ and e_3 is the Arason invariant. It follows that η belongs to the kernel of the Rost invariant if and only if q_η belongs to I^4k.

We can quickly find some invariants of the kernel $H^1(k, \mathrm{Spin}_{16})_0$ of the Rost invariant. For η in that set, q_η is $\langle \alpha_\eta \rangle \gamma$ for some $\alpha_\eta \in k^\times$ and some 4-Pfister quadratic form γ [Lam, X.5.6]. (One can take α_η to be any element of $k^\times$ represented by q_η [Lam, X.1.8].) We define invariants $f_d \colon H^1(*, \mathrm{Spin}_{16})_0 \to H^d(*, \mathbb{Z}/2\mathbb{Z})$ for $d = 4, 5$ via:

$$f_4(\eta) := e_4(q_\eta) \quad \text{and} \quad f_5(\eta) := (\alpha_\eta) \cdot e_4(q_\eta),$$

where e_4 is the usual additive map $I^4(*) \to H^4(*, \mathbb{Z}/2\mathbb{Z})$. If q_η is isotropic, then q_η is hyperbolic and $e_4(q_\eta)$ is zero, so the value of $f_5(\eta)$ depends only on η and not on the choice of α_η, see [Ga 09, 10.2].

We can identify two more (candidates for) invariants of $H^1(*, \mathrm{Spin}_{16})_0$. The split E_8 has a subgroup isomorphic to HSpin_{16}, the nontrivial quotient of Spin_{16} that is neither adjoint (i.e., not PSO_{16}) nor SO_{16}. Further, the composition

$$H^1(*, \mathrm{Spin}_{16}) \to H^1(*, \mathrm{HSpin}_{16}) \to H^1(*, E_8) \xrightarrow{r_{E_8}} H^3(*, \mathbb{Z}/60\mathbb{Z}(2))$$

is the Rost invariant of Spin_{16} [Ga, (5.2)]. We find a morphism of functors

$$H^1(*, \mathrm{Spin}_{16})_0 \to H^1(*, E_8)_0.$$

Composing this with the invariant u gives an invariant

$$u_5 \colon H^1(*, \mathrm{Spin}_{16})_0 \to H^5(*, \mathbb{Z}/2\mathbb{Z}).$$

(Roughly speaking, we have used the invariant u of $H^1(*, E_8)_0$ to get an invariant of $H^1(*, \mathrm{Spin}_{16})_0$ in the same way that Rost used the f_5 invariant of $H^1(*, F_4)$ to get an invariant of $H^1(*, \mathrm{Spin}_9)$, see [Rost] or [Ga 09, 18.9].)

The purpose of this section is to prove:

4.1. **Theorem.** *The invariants $H^1(*, \mathrm{Spin}_{16})_0 \to H^\bullet(*, \mathbb{Z}/2\mathbb{Z})$ form a free $H^\bullet(k, \mathbb{Z}/2\mathbb{Z})$-module with basis*

$$1, f_4, f_5, u_5, u_6,$$

where the invariant u_6 is given by the formula $u_6(\eta) := (\alpha_\eta) \cdot u_5(\eta)$.

We first replace Spin_{16} with a more tractable group. The first author described in [Ga, §11] a subgroup of HSpin_{16} isomorphic to $\mathrm{PGL}_2^{\times 4}$. Examining the root system data for this subgroup given in Tables 7B and 11 of that paper, we see that the inverse image of this subgroup in Spin_{16} is a subgroup H obtained by modding $\mathrm{SL}_2^{\times 4}$ out by the subgroup generated by $(-1,-1,1,1)$, $(-1,1,-1,1)$, and $(-1,1,1,-1)$. The image of the center of each copy of SL_2 has the same nonidentity element; this defines a homomorphism $\mu_2 \to H$ that gives a short exact sequence:

$$1 \to \mu_2 \to H \to \mathrm{PGL}_2^{\times 4} \to 1.$$

The image of $H^1(k,H)$ in $H^1(k,\mathrm{PGL}_2)^{\times 4}$ consists of quadruples (Q_1,Q_2,Q_3,Q_4) of quaternion algebras so that $Q_1\otimes Q_2\otimes Q_3\otimes Q_4$ is split.

Let φ map the Klein four-group $V:=\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ into $(\mathrm{SL}_2\times\mathrm{SL}_2)/\mu_2$ via

$$\varphi(1,0):=\left(\left(\begin{smallmatrix}-1&0\\0&1\end{smallmatrix}\right),\left(\begin{smallmatrix}-1&0\\0&1\end{smallmatrix}\right)\right)\quad\text{and}\quad\varphi(0,1):=\left(\left(\begin{smallmatrix}0&1\\-1&0\end{smallmatrix}\right),\left(\begin{smallmatrix}0&1\\-1&0\end{smallmatrix}\right)\right).$$

This defines a homomorphism. Twisting $(\mathrm{SL}_2\times\mathrm{SL}_2)/\mu_2$ by a pair $(a,b)\in k^\times/k^{\times 2}\times k^\times/k^{\times 2}=H^1(k,V)$ gives $(\mathrm{SL}(Q)\times\mathrm{SL}(Q))/\mu_2$, where Q denotes the quaternion algebra (a,b). (Of course, composing φ with either of the projections $(\mathrm{SL}_2\times\mathrm{SL}_2)/\mu_2\to\mathrm{PGL}_2$ sends (a,b) to the same quaternion algebra Q.) The composition

$$V\times V\xrightarrow{\varphi\times\varphi}(\mathrm{SL}_2\times\mathrm{SL}_2)/\mu_2\times(\mathrm{SL}_2\times\mathrm{SL}_2)/\mu_2\to H$$

gives a map whose image does not meet the center of Spin_{16}, which we denote by Z. This gives a homomorphism $Z\times V\times V\to\mathrm{Spin}_{16}$.

4.2. We now fix a $\nu\in H^1(K,Z\times V\times V)$, write ζ for its image in $H^1(K,Z)$, write Q_1,Q_2 respectively for its images under the two projections

$$H^1(K,Z\times V\times V)\to H^1(K,V)\to H^1(K,\mathrm{PGL}_2),$$

and write q_i for the 2-Pfister norm form of Q_i. It follows from the description of the map $H^1(K,\mathrm{HSpin}_{16})\to H^1(K,\mathrm{PSO}_{16})$ in [Ga, §4] that the image of ν in $H^1(K,\mathrm{SO}_{16})$ is $\langle\alpha_\nu\rangle q_1q_2$ for some $\alpha_\nu\in K^\times$. Hence $r_{\mathrm{Spin}_{16}}(\nu)=0$.

Conversely, given $\eta\in H^1(K,\mathrm{Spin}_{16})_0)$, there is some $\alpha\in K^\times$ so that $\langle\alpha\rangle q_\eta$ is a 4-Pfister form. Fix $\nu\in H^1(K,Z\times V\times V)$ so that $q_1q_2=\langle\alpha\rangle q_\eta$. Then the image of ν in $H^1(K,\mathrm{Spin}_{16})$ is $\lambda\cdot\eta$ for some $\lambda\in H^1(K,Z)$ and $\lambda\cdot\nu$ maps to η. We have shown:

(4.3) *The map $Z\times V\times V\to\mathrm{Spin}_{16}$ gives a surjection $H^1(K,Z\times V\times V)\to H^1(K,\mathrm{Spin}_{16})_0$.*

It follows (using [Ga 09, 5.3]) that the module of invariants $H^1(*,\mathrm{Spin}_{16})_0\to H^\bullet(*,\mathbb{Z}/2\mathbb{Z})$ injects into the module of invariants $H^1(*,Z\times V\times V)\to H^\bullet(*,\mathbb{Z}/2\mathbb{Z})$. But we know this larger module by [GMS, p. 40] or [Ga 09, 6.7]: it is spanned by products $\pi_1\pi_2\pi_3$ for $\pi_1\colon H^1(*,Z)\to H^\bullet(*,\mathbb{Z}/2\mathbb{Z})$ and π_2,π_3 invariants $H^1(*,V)\to H^\bullet(*,\mathbb{Z}/2\mathbb{Z})$ composed with projection on the 2nd or 3rd term in the product.

4.4. **Lemma.** *In the notation of 4.2, if $[Q_1]\cdot[Q_2]=0$ in $H^4(K,\mathbb{Z}/2\mathbb{Z})$, then the image of ν in $H^1(K,\mathrm{Spin}_{16})$ is zero.*

Proof. If $[Q_1]\cdot[Q_2]$ is zero, then q_1q_2 is in $I^5(k)$ and so is hyperbolic. It follows that the image of ν in $H^1(K,\mathrm{PSO}_{16})$ is zero, hence the image of ν in $H^1(K,\mathrm{Spin}_{16})$ is in the image of $H^1(K,Z)$. But Spin_{16} is split semisimple, so the image of H^1 of the center in H^1 of the group is zero. □

Proof of Theorem 4.1. We abuse the notation of 4.2 and write (ζ,Q_1,Q_2) for ν. The invariant f_4 sends (ζ,Q_1,Q_2) to $[Q_1]\cdot[Q_2]$. Lemma 4.4 combined with arguments like those in [GMS, pp. 43, 44] shows that every invariant of $H^1(*,\mathrm{Spin}_{16})_0$ restricts to one of the form $\lambda+\phi\cdot f_4$ for uniquely determined $\lambda\in H^\bullet(k,\mathbb{Z}/2\mathbb{Z})$ and $\phi\colon H^1(*,Z)\to H^\bullet(*,\mathbb{Z}/2\mathbb{Z})$, i.e., is given by the formula

$$(\zeta,Q_1,Q_2)\mapsto\lambda+\phi(\zeta)\cdot[Q_1]\cdot[Q_2].$$

The collection of such invariants of $H^1(*,Z\times V\times V)$ forms a free $H^\bullet(k,\mathbb{Z}/2\mathbb{Z})$-module with basis

$$1,\quad f_4,\quad \chi_v\cdot f_4,\quad \chi_h\cdot f_4,\quad \chi_v\cdot\chi_h\cdot f_4,$$

where χ_v and χ_h denote the maps $H^1(*, Z) \to H^1(*, \mathbb{Z}/2\mathbb{Z})$ defined by restricting to Z the vector representation $\mathrm{Spin}_{16} \to \mathrm{SO}_{16}$ and the half-spin representation $\mathrm{Spin}_{16} \to \mathrm{HSpin}_{16}$ implicit in our root-system description above. Obviously, f_5 restricts to be $\chi_v \cdot f_4$.

At this point, it suffices to prove:

$$(4.5) \qquad u_5 \textit{ restricts to be } \chi_h \cdot f_4.$$

Indeed, this statement implies that u_5 is zero when q_η is isotropic, hence by [Ga 09, 10.2] the formula for u_6 gives a well-defined invariant; it obviously restricts to $\chi_v \cdot u_5 = \chi_v \cdot \chi_h \cdot f_4$ on $H^1(*, Z \times V \times V)$. Spanning and linear independence follow from the previous paragraph.

We now prove (4.5). The restriction of u_5 sends zero to zero, so it is $\phi \cdot f_4$ for some $\phi : H^1(*, Z) \to H^1(*, \mathbb{Z}/2\mathbb{Z})$ that itself sends zero to zero. Therefore (by [GMS, p. 40]) ϕ is induced by some homomorphism $\chi \colon Z \to \mathbb{Z}/2\mathbb{Z}$. As u_5 is defined by pulling back along the map $\mathrm{Spin}_{16} \to E_8$, one quickly sees that χ must be zero or χ_h. As χ, the zero invariant, and χ_h are all defined over $\mathbb{Q}$, it suffices to prove that χ is not the zero invariant in the case where $k = \mathbb{Q}$. Example 15.1 of [Ga] gives a class $\nu \in H^1(\mathbb{R}, Z \times V \times V)$ whose image in $H^1(\mathbb{R}, E_8)$ is the compact E_8, on which u is nonzero. Hence the restriction of u_5 to $Z \times V \times V$ is not zero over $\mathbb{Q}$ and must be $\chi_h \cdot f_4$. □

5. Essential dimension of $H^1(*, \mathrm{Spin}_{16})_0$

The following is a corollary of the previous section:

5.1. **Corollary.** *The essential dimension of the functor $H^1(*, \mathrm{Spin}_{16})_0$ over every field of characteristic zero is* 6.

Proof. The existence of the nonzero invariant $u_6 : H^1(*, \mathrm{Spin}_{16})_0 \to H^6(*, \mathbb{Z}/2\mathbb{Z})$ implies that the essential dimension is at least 6 by [RY, Lemma 6.9]; this is the interesting inequality. One can deduce that the essential dimension is at most 6 by, for example, the surjectivity in (4.3). □

By way of contrast, Merkurjev proved that the essential dimension of the functor $H^1(*, \mathrm{Spin}_{16})$ (without restricting to the kernel of the Rost invariant) is 24 by [BRV, Remark 3.9].

6. Galois descent for representations of finite groups

In this section, we restate some observations of Serre from [Serre 00] and [GR] regarding projective embeddings of simple groups in exceptional algebraic groups. Combining these results with the u-invariant for E_8 gives some new embeddings results, see Example 6.5 below.

Let A be an abstract finite group and G a semisimple linear algebraic group defined over $\mathbb{Q}$. Fix a faithful representation $\pi \colon G \to \mathrm{GL}_N$ defined over $\mathbb{Q}$.

6.1. **Definition.** Let $\mathbb{Q} \subset F$ be a field. The *character* of a homomorphism $\alpha \colon A \to G(\overline{F})$ is the character of the composition $\pi \circ \alpha \colon A \to \mathrm{GL}_N(\overline{F})$. We say that the character of α is *defined over* F if all its values belong to F.

Let $\varphi \colon A \to G(\overline{F})$ be a monomorphism and χ its character. Assume that χ is defined over F, $Z_{G(\overline{F})}(A) = 1$, that there is exactly one $G(\overline{F})$-conjugacy class of homomorphisms $A \to G(\overline{F})$ with character χ, and G is either split or $\mathrm{Aut}\, G = G$.

The following theorem can be extracted from Serre's paper [Serre 00, 2.5.3]:

6.2. **Theorem.** *In the above notation there exists a twisted form G_0 of G defined over F together with a monomorphism $A \to G_0(F)$. Moreover, for a field extension K/F there is a representation $A \to G(K)$ with character χ iff $G \simeq G_0$ over K.*

Proof. Let

$$P = \{\alpha\colon A \to G \mid \alpha \text{ is a representation with character } \chi\};$$

it is a variety over F and G acts on it by conjugation. By assumptions on A and G this action is transitive. Moreover, the condition on the centralizer guarantees that this action is simply transitive, i.e., for any $\alpha, \beta \in P(\overline{F})$ there exists a unique $g \in G(\overline{F})$ with $\beta = \alpha^g$. Thus, P is a G-torsor.

Let $\eta \in H^1(F, G)$ be the 1-cocycle corresponding to the torsor P. Then $\sigma \cdot \varphi = \eta_\sigma^{-1} \varphi \eta_\sigma$ for all σ in the absolute Galois group $\mathrm{Gal}(\overline{F}/F)$. Define now G_0 as the twisted form of G over F by the torsor P. The group G_0 is defined out of $G(\overline{F})$ by a twisted Galois action $*$:

$$\sigma * g = \eta_\sigma (\sigma \cdot g) \eta_\sigma^{-1} \qquad (g \in G(\overline{F})).$$

Now it is easy to see that the homomorphism $\varphi\colon A \to G(\overline{F})$ is an F-defined homomorphism $A \to G_0(F)$.

Let K/F be a field extension. If there is a representation $A \to G(K)$ with character χ, then obviously G and G_0 are isomorphic over K. Conversely, if G and G_0 are isomorphic over K, then the image of the cocycle η in $H^1(K, \mathrm{Aut}(G))$ is zero. Since the centralizer of A in G is trivial, the group G is adjoint. If G is split or $\mathrm{Aut}\, G = G$, it follows that η is already zero in $H^1(K, G)$. □

To characterize the isomorphism criterion of Theorem 6.2 we need the following proposition.

6.3. **Proposition.** *For each Killing-Cartan type Φ in the table*

Type Φ	F_4	G_2	E_8
n	3	3	5

there is a unique algebraic group G_0 of type Φ that is compact at every real place of every number field; it is defined over $\mathbb{Q}$. For every field K of characteristic zero and n as in the table, the following are equivalent:

(1) *$G_0 \otimes K$ is split.*
(2) $(-1)^n = 0 \in H^n(K, \mathbb{Z}/2)$.
(3) -1 *is a sum of 2^{n-1} squares of the field K.*

Proof. The first sentence is a standard part of the Kneser-Harder-Chernousov Hasse principle. The group G_0 is split at every finite place.

For the second claim, all cases but E_8 are well-known. For E_8, if $G_0 \otimes K$ is split, then $(-1)^5$ is zero by the existence of u; see 2.1. For the converse, G_0 equals $t(A)$ where A is the unique Albert $\mathbb{Q}$-algebra with no nilpotents (see Example 3.6). If $(-1)^5$ — i.e., $f_5(A)$ — is zero in $H^5(K, \mathbb{Z}/2\mathbb{Z})$, then $A \otimes K$ has nilpotents and $G_0 \otimes K$ is split by Example 3.5. □

In the following examples we write Alt_l for the alternating group of degree l and as $\zeta_l = e^{2\pi i/l}$ a primitive l-th root of unity.

6.4. **Example** (type G_2). Let G denote the split group of type G_2, $A = G(\mathbb{F}_2)$ (resp. $\mathrm{PSL}(2,8)$, $\mathrm{PSL}(2,13)$), and K a field of characteristic zero. Then there is an embedding $A \to G(K)$ iff -1 is a sum of 4 squares of K and $\zeta_9 + \bar\zeta_9 \in K$ (for $\mathrm{PSL}(2,8)$), resp. $\sqrt{13} \in K$ (for $\mathrm{PSL}(2,13)$).

Indeed, fix the minimal fundamental representation $G \to \mathrm{GL}_7$. By [A87, Theorem 9(3,4,5)] there is a representation $\varphi\colon A \to G(\overline{\mathbb{Q}})$ whose character χ is defined over $F = \mathbb{Q}$ (resp. $F = \mathbb{Q}(\zeta_9 + \bar\zeta_9)$, $F = \mathbb{Q}(\sqrt{13})$). Moreover, G acts transitively on the homomorphisms $A \to G(\overline{\mathbb{Q}})$ with character χ (see [A87] and [Griess, Cor. 1 and 2]).

By [A87, 9.3(1)] the representation φ is irreducible, so $Z_{G(\overline{\mathbb{Q}})}(A) = 1$. Thus, all conditions of Theorem 6.2 are satisfied. Therefore there is a twisted form G_0 of G defined over F and an embedding $A \to G_0(F)$.

In particular, there is an embedding $A \to G_0(\mathbb{R})$. Since any finite subgroup of a Lie group is contained in its maximal compact subgroup, it is easy to see that $G_0 \otimes_F \mathbb{R}$ is compact for all embeddings of F into $\mathbb{R}$. Moreover, by Theorem 6.2 we have an embedding $A \to G(K)$ iff G_0 and G are isomorphic over K. By Proposition 6.3 the latter occurs iff -1 is a sum of 4 squares of K.

(Thus, we have recapitulated the argument from [Serre 00, 2.5.3]).

6.5. **Example** (type E_8). Let G denote the split group of type E_8, $A = \mathrm{PGL}(2,31)$ (resp. $A = \mathrm{SL}(2,32)$), and K a field of characteristic zero. We view G as a subgroup of GL_{248} via the adjoint representation. There is an embedding $A \to G(K)$ iff -1 is a sum of 16 squares and $\zeta_{11} + \bar\zeta_{11} \in K$ (for $\mathrm{SL}(2,32)$).

Indeed, by [GR, Theorem 2.27 and Theorem 3.25] there exists an embedding $A \to G(\overline{\mathbb{Q}})$ whose character is defined over $F = \mathbb{Q}$ (resp. $F = \mathbb{Q}(\zeta_{11} + \bar\zeta_{11})$). Using [GR] one can check all conditions of Theorem 6.2 (cf. Example 6.4).

It follows by Theorem 6.2 that there is an embedding $A \to G_0(F)$ for some twisted form G_0 of G. Again as in Example 6.4 one can see that G_0 is the unique group such that $G_0 \otimes_F \mathbb{R}$ is compact for all embeddings of F into $\mathbb{R}$. Finally by Proposition 6.3 G and G_0 are isomorphic over a field extension K/F iff -1 is a sum of 16 squares in K. This proves Theorem 1.1.

Roughly speaking, we have added the facts about the compact E_8 contained in the proof of Proposition 6.3 (which uses the existence of the u-invariant) to Serre's appendix [GR, App. B].

One can also take G to be the form of E_8 over $\mathbb{Q}$ that is neither split nor anisotropic. Then in the same way one can show that A embeds in $G(K)$ iff -1 is a sum of 4 squares and $\zeta_{11} + \bar\zeta_{11} \in K$ (for $A = \mathrm{SL}(2,32)$).

In the same way one can get the following example:

6.6. **Example** (type A_1). Let $G = \mathrm{PGL}_2$, $A = \mathrm{Alt}_4$ (resp. Alt_5), and K a field of characteristic zero. Then there is an embedding $A \to G(K)$ iff -1 is a sum of 2 squares and for Alt_5 additionally $\sqrt{5} \in K$ (see [Serre 72, §2.5] and [Serre 80, §1]).

Acknowledgments. Both authors thank J-P. Serre for his helpful comments on an earlier version of this paper. The first author's research was partially supported by the National Science Foundation grant no. DMS-0653502. The second author was supported by DFG, project GI706/1-1.

References

[A87] M. Aschbacher. *Chevalley groups of type G_2 as the group of a trilinear form.* J. Alg. **109** (1987), 193–259.

[BRV] P. Brosnan, Z. Reichstein, and A. Vistoli, *Essential dimension, spinor groups, and quadratic forms*, to appear in Annals of Math.

[Ga 01] S. Garibaldi, *The Rost invariant has trivial kernel for quasi-split groups of low rank*, Comment. Math. Helv. **76** (2001), 684–711.

[Ga] ———, *Orthogonal involutions on algebras of degree* 16 *and the Killing form of E_8,* with an appendix by K. Zainoulline. To appear in Contemp. Math. Available from `arxiv.org`

[Ga 09] ———, *Cohomological invariants: exceptional groups and Spin groups*, Memoirs of the Amer. Math. Soc. **200** (2009), no. 937.

[GMS] S. Garibaldi, A. Merkurjev, J-P. Serre. *Cohomological invariants in Galois cohomology.* University Lecture Series **28**, Amer. Math. Soc., Providence, RI, 2003.

[GQ] S. Garibaldi and A. Quéguiner-Mathieu, *Restricting the Rost invariant to the center.* St. Petersburg Math. J. **19** (2008), no. 2, 197–213.

[GR] R. Griess and A. Ryba, *Embeddings of* $\mathrm{PGL}(2,31)$ *and* $\mathrm{SL}(2,32)$ *in* $E_8(\mathbb{C})$*,* with appendices by M. Larsen and J-P. Serre. Duke Math. J. **94** (1998), 181–211.

[Griess] R. Griess, *Basic conjugacy theorems for G_2*, Invent. math. **121** (1995), 257–277.

[H] G. Harder, *Über die Galoiskohomologie halbeinfacher algebraischer Gruppen. III*, J. Reine Angew. Math. **274/275** (1975), 125–138.

[Inv] M.-A. Knus, A. Merkurjev, M. Rost, J.-P. Tignol. *The book of involutions.* AMS Colloquium Publ., vol. 44, 1998.

[J] N. Jacobson, *Exceptional Lie algebras.* Lecture Notes in Pure and Applied Math., 1 Marcel Dekker, Inc., New York 1971.

[Lam] T.-Y. Lam, *Introduction to quadratic forms over fields*, Amer. Math. Soc., Providence, RI, 2005.

[OViVo] D. Orlov, A. Vishik, V. Voevodsky, *An exact sequence for $K^M_*/2$ with applications to quadratic forms*, Ann. of Math. **165** (2007), no. 1, 1–13.

[PR] V.P. Platonov and A.S. Rapinchuk, *Algebraic groups and number theory*, Academic Press, Boston, 1994.

[RY] Z. Reichstein and B. Youssin, *Essential dimension of algebraic groups and a resolution theorem for G-varieties*, Canad. J. Math. **52** (2000), 1018–1056.

[Rost] M. Rost, *On the Galois cohomology of* Spin(14), Preprint 1999. Available from `http://www.math.uni-bielefeld.de/~rost`

[Sem 08] N. Semenov, *Motivic construction of cohomological invariants.* Preprint 2008. Available from `http://arxiv.org/abs/0905.4384`

[Serre 72] J-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), 259–331 (= Oe., vol. III, #94).

[Serre 80] ———, *Extensions icosaédriques.* In *Seminar on Number Theory*, 1979–1980, exp. 19, Uni. Bordeaux I, Talence 1980 (= Oe., vol. III, #123).

[Serre 00] ———, *Sous-groupes finis des groupes de Lie.* Astérisque **266** (2000), 415–430 (= Oe., vol. IV, #174).

[T] J. Tits, *Algèbres alternatives, algèbres de Jordan et algèbres de Lie exceptionnelles.* Indag. Math. **28** (1966), 223–237.

(Garibaldi) Department of Mathematics & Computer Science, Emory University, Atlanta, GA 30322, USA

E-mail address: `skip@member.ams.org`

URL: `http://www.mathcs.emory.edu/~skip/`

(Semenov) Mathematisches Institut der LMU München, Theresienstr. 39, 80333 München, Germany

E-mail address: `semenov@mathematik.uni-muenchen.de`