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 some groups of type E_8 and use this formula 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 1990s, 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. In the first part of the paper we recall the recently-discovered invariant u defined on the kernel of the Rost invariant for groups of type E_8 and find an explicit formula of $u(G)$ for groups G obtained by a Tits construction. This formula leads to several suprising results—an answer to a question of Serre about Killing forms (Remark 3.14), cohomological invariants of Spin_{16} (Section 4), the kernel of the Rost invariant for some nonsplit groups of type E_7 (Section 5), and finite subgroups of algebraic groups (Section 6).

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"

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

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 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*.*

(This is the $p = 2$ case of [Gi 01, p. 302, Th. 4(2)].) 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. In [T]—or see [J]—Jacques Tits gave an explicit construction that takes an octonion k-algebra and an Albert k-algebra as inputs, where k is any field of characteristic $\neq 2, 3$, and gives as output a Lie algebra of type E_8. (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; see also Section 5.) As his construction is obviously functorial in k and compatible with automorphisms of the inputs, one finds an injective homomorphism $G_2 \times F_4 \to E_8$ where we have written the Killing-Cartan type for the corresponding split group. Applying Galois cohomology, we have a morphism of functors

$$H^1(*, G_2) \times H^1(*, F_4) \to H^1(*, E_8). \tag{3.2}$$

For a given field k, the three sets classify octonion k-algebras, Albert k-algebras, and simple Lie algebras of type E_8 respectively; by Galois descent it is obvious that this map coincides with the construction described by Tits.

3.3. Here is an alternative derivation of (3.2) that avoids Tits's paper [T] but assumes that k has characteristic zero (as we will anyway assume in the rest of the paper). The root system of E_8 contains a maximal subsystem of type $E_6 \times A_2$ corresponding to a copy of $(E_6^{\mathrm{sc}} \times \mathrm{SL}_3)/\mu_3$ in the group E_8, where E_6^{sc} denotes the split simply connected group of type E_6. The subgroup of E_6^{sc} fixed by the obvious automorphism of the Dynkin diagram (viewed as an automorphism of a pinning of E_6^{sc}) is split of type F_4, see e.g. [Ga 09a, 9.12]. The centralizer of this F_4 is a simple group of type G_2 (because this is so over $\mathbb{C}$; the F_4 and G_2 subgroups form a dual pair) and is split because it contains a copy of SL_3. This gives a subgroup $G_2 \times F_4$ of E_8 over k and applying Galois cohomology gives a morphism as in (3.2).

But note that the two derivations of (3.2) give the same morphism. Indeed, write ϕ, ϕ' for the embeddings of $G_2 \times F_4$ in the split E_8 over k. For $\overline{k}$ an algebraic closure of k, there exists some $g \in E_8(\overline{k})$ such that $g(\operatorname{im}\phi)g^{-1} = \operatorname{im}\phi'$ because this is so over $\mathbb{C}$ [D]. Further, the composition $(\phi')^{-1}\operatorname{Int}(g)\phi$ is a $\overline{k}$-automorphism of $G_2 \times F_4$ (where $\operatorname{Int}(g)\, y := gyg^{-1}$), hence is $\operatorname{Int}(x)$ for a unique $x \in (G_2 \times F_4)(\overline{k})$. That is, $\operatorname{Int}(g)\phi = \phi' \operatorname{Int}(x)$. Replacing g with $\phi'(x)^{-1}g$, we may assume that $\operatorname{Int}(g)\phi = \phi'$. For σ in the absolute Galois group $\operatorname{Gal}(\overline{k}/k)$ of k, we have:

$$\operatorname{Int}(g)\phi = \phi' = {}^{\sigma}\phi' = \operatorname{Int}({}^{\sigma}g)\phi \tag{3.4}$$

because ϕ and ϕ' are k-defined, hence $g^{-1}\,{}^{\sigma}g$ centralizes $\operatorname{im}\phi$, i.e., $g^{-1}\,{}^{\sigma}g = 1$ and $g \in E_8(k)$. It is now obvious that the morphisms (3.2) induced by ϕ and ϕ' are equal.

3.5. *Remark.* It follows quickly from the discussion in 3.3 that *a group G_0 of type E_8 is obtained by Tits's construction*—meaning, is in the image of

(3.2)—*if and only if it contains a subgroup of type $G_2 \times F_4$.* The "only if" direction is obvious by descent.

To see "if", recall that G_0 is an inner form of E_8, i.e., it can be obtained by twisting E_8 by a 1-cocycle $\eta\colon \mathrm{Gal}(\overline{k}/k) \to E_8(\overline{k})$. The group G_0 has the same $\overline{k}$-points as E_8, but a different Galois action $*$, namely $\sigma * g = \eta_\sigma(\sigma \cdot g)\eta_\sigma^{-1}$ for $g \in G_0(\overline{F})$. As G_0 contains a subgroup of type $G_2 \times F_4$ and all such subgroups of E_8 are conjugate over $\overline{k}$, we may replace η by a cohomologous cocycle and so assume that η_σ normalizes $G_2 \times F_4$ for every $\sigma \in \mathrm{Gal}(\overline{k}/k)$. But $G_2 \times F_4$ has only inner automorphisms and is its own centralizer in E_8, so η_σ belongs to $G_2 \times F_4$ for every σ, whence G_0 is in the image of (3.2).

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 3.10.

3.6. 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

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

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 $f_3(O) = f_3(A)$.

3.7. **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 $H^1(k, E_8)_0$.

3.8. **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 09b, Prop. 12.1(1)].

3.9. **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 3.8
$(-1)^3$	0	split by Example 3.8
$(-1)^3$	$(-1)^5$	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.

3.10. **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 3.9. 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 09b, 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 $\lambda_2 = 0$. $\square$

3.11. **Corollary.** *The invariant u is surjective on pure symbols. More precisely, for any field k of characteristic 0 and any pure symbol $v \in H^5(k, \mathbb{Z}/2\mathbb{Z})$ there exists a group of type E_8 with zero Rost invariant and with $u(G) = v$.*

3.12. *Remark.* In [Sem 08, pf. of Cor. 8.7] the second author constructed a ν_4-variety $\widetilde{Y}$ that splits u. Voevodsky has conjectured that if $u \in H^n(k, \mathbb{Z}/2\mathbb{Z})$ and X is a ν_{n-1}-variety that splits u, then u is a pure symbol. Theorem 3.10 confirms this conjecture for the E_8's constructed as in Definition 3.7, equivalently, that have odd-order Rost invariant and contain a subgroup of type $G_2 \times F_4$.

For G in the image of t, $u(G)$ is a symbol in $H^5(k, \mathbb{Z}/2\mathbb{Z})$, so it determines a 5-Pfister quadratic forms q_G such that $e_5(q_G) = u(G)$. We have:

3.13. **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:*

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

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

Proof. Combine the formula for Kill_G given in [J, p. 117, (114)] or [Ga 09b, 13.2] with Theorem 3.10. □

3.14. *Remark.* The invariant u was constructed using motives. One might hope to construct it using methods as in [GMS], in particular to deduce $u(G)$ from the Killing form of G (suggested by analogy with the way that $f_5(A)$ is deduced from the trace form on an Albert algebra A on pages 49–51 of ibid.). But this is impossible. Indeed, fix a formally real field k_0 and write k for the function field of the 8-Pfister quadratic form $\langle\langle -1\rangle\rangle^7 \cdot \langle\langle t_1 t_2\rangle\rangle$ over $k_0(t_1, t_2)$ where t_1 and t_2 are indeterminates. Put A_i for the reduced Albert algebra over k with

$$f_3(A_i) = (-1)^3 \quad \text{and} \quad f_5(A_i) = (-1)^4 \cdot (t_i), \quad i = 1, 2.$$

Put $G_i := t(A_i)$; it is a group of type E_8 over $k_0(t_1, t_2)$ and $q_{G_i} = \langle\langle -1\rangle\rangle^4 \cdot \langle\langle t_i\rangle\rangle$ by Theorem 3.10. As k_0 is formally real, q_{G_1} and q_{G_2} are distinct and anisotropic over $k_0(t_1, t_2)$. For dimension reasons [Lam, X.4.10], $\langle\langle -1\rangle\rangle^4 \cdot \langle\langle t_1 t_2\rangle\rangle$ is anisotropic over k, hence q_{G_1} and q_{G_2} are not isomorphic over k and in particular $u(G_1) \neq u(G_2)$ in $H^5(k, \mathbb{Z}/2\mathbb{Z})$. On the other hand, the isomorphism class of $\langle\langle -1\rangle\rangle^3 q_{G_i} \simeq \langle\langle -1\rangle\rangle^7 \langle\langle t_i\rangle\rangle$ over k does not depend on i, so G_1 and G_2 have isomorphic Killing forms over k by Corollary 3.13.

4. Application to Spin_{16}

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.

Write $H^1(*, \mathrm{Spin}_{16})_0$ for the kernel of the Rost invariant; we will determine the cohomological invariants $H^1(*, \mathrm{Spin}_{16})_0 \to H^\bullet(*, \mathbb{Z}/2\mathbb{Z})$. To avoid a long technical digression, we only outline the details of the argument. In [Ga 09b, §11], the first author described a subgroup of HSpin_{16} isomorphic to $\mathrm{PGL}_2^{\times 4}$. The inverse image of this subgroup in Spin_{16} contains a direct product $V \times V$ of two copies of the Klein four-group so that the image of a quadruple

$$(a_1, a_2, a_3, a_4) \in H^1(K, \mu_2)^{\times 4} = H^1(K, V \times V)$$

in $H^1(K, \mathrm{PGL}_2)^{\times 4}$ is the quadruple of quaternion algebras (a_1, a_2), (a_1, a_2), (a_3, a_4), (a_3, a_4). Together with the center of Spin_{16}—which is also isomorphic to V—we find a copy of $V^{\times 3}$ in Spin_{16} such that the induced map $H^1(K, V^{\times 3}) \to H^1(K, \mathrm{Spin}_{16})$ has image $H^1(K, \mathrm{Spin}_{16})_0$ for every K/k.

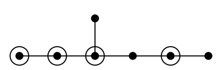
With this in hand, arguments similar to those in [Ga 09a, 18.1, 18.9] give that the invariant u of $H^1(*, E_8)_0$ can be used to construct invariants of $H^1(*, \mathrm{Spin}_{16})_0$ of degree 5 and 6, and that *the collection of invariants* $H^1(*, \mathrm{Spin}_{16})_0 \to H^\bullet(*, \mathbb{Z}/2\mathbb{Z})$ *is a rank* 5 *free* $H^\bullet(k, \mathbb{Z}/2\mathbb{Z})$*-module with basis consisting of invariants of degree* 0, 4, 5, 5, 6*.*

From the preceding paragraph, we deduce that the essential 2-dimension of $H^1(*, \mathrm{Spin}_{16})_0$ is at least 6. Standard arguments show that the essential dimension is at most 6, so we deduce that *the essential dimension and the essential* 2*-dimension of* $H^1(*, \mathrm{Spin}_{16})_0$ *both equal* 6. This should be contrasted with the essential dimension of the functor $H^1(*, \mathrm{Spin}_{16})$, which is 24, see [M 09, Th. 4.9] and [BRV, Th. 3.3(b)].

5. Application to E_7

5.1. **Example.** Put G and $\bar{G}$ for the simply connected and adjoint real forms of E_7 with Tits index

(5.2)



i.e., non-split with a minimal parabolic subgroup that is "wesentlich" in the language of [H, p. 132]. Élie Cartan proved that the set $H^1(\mathbb{R}, \bar{G})$ has four elements, corresponding to the four real forms of G. The image of the natural map $q\colon H^1(\mathbb{R}, G) \to H^1(\mathbb{R}, \bar{G})$ is the set $\{G, G^{\mathrm{cpt}}\}$ where G^{cpt} denotes the compact form of G; these are the groups whose Tits class is $[\mathbb{H}] \in H^2(\mathbb{R}, \mu_2)$. As is standard, H^1 of the center of G—i.e., $H^1(\mathbb{R}, \mu_2) = \mathbb{Z}/2\mathbb{Z}$—acts transitively on the fibers of q. Further, the Rost invariant

$$r_G\colon H^1(\mathbb{R}, G) \to H^3(\mathbb{R}, \mathbb{Z}/12\mathbb{Z}) = \{0, (-1)^3\} = \mathbb{Z}/2\mathbb{Z}$$

satisfies

$$r_G(z \cdot \eta) = r_G(\eta) + z \cdot (-1)^2 \quad \text{for } z \in H^1(\mathbb{R}, \mu_2) \text{ and } \eta \in H^1(\mathbb{R}, G)$$

by [GQ, 2.3] and [Ga 01, 7.1]. That is, q is 2-to-1 and each fiber has one element in the kernel of r_G and one element whose Rost invariant is $(-1)^3 \in H^3(\mathbb{R}, \mathbb{Z}/2\mathbb{Z})$; in total $H^1(\mathbb{R}, G)$ has four elements. (The description of $H^1(\mathbb{R}, G)$ and the fibers of q can also be obtained from [Serre GC,

§III.4.5, Exercise (a)], but that reference does not directly say anything about the Rost invariant.)

In particular, the kernel of the Rost invariant r_G is not zero. This is in contrast with the case of the split simply connected group E_7^{sc} of type E_7, where the kernel of the Rost invariant on $H^1(k, E_7^{\mathrm{sc}})$ is zero for every field k by [Ga 01].

We will now show how to use the invariant u to distinguish the classes in the kernel of r_G. Fix a field k of characteristic zero and a quaternion k-algebra Q. Define G to be the simply connected group of type E_7 whose Tits index is (5.2) (if Q is division) or is split (if Q is split). We have:

5.3. **Proposition.** *There are inclusions* $\mathrm{SL}(Q) \times F_4 \subset G \subset E_8$ *such that for* $(\lambda, A) \in H^1(k, \mathrm{SL}(Q)) \times H^1(k, F_4)$*, we have:*

1. *The image of* (λ, A) *in* $H^1(k, \mathrm{Aut}(G))$ *is a group of type* E_7 *whose Lie algebra arises from the Tits construction with* Q *and* A *as inputs.*
2. $r_G(\lambda, A) = r_{E_8}(\lambda, A) = (\lambda) \cdot [Q] + r_{F_4}(A)$.
3. *If* (λ, A) *is in the kernel of* r_{E_8}*, then* $u(\lambda, A) = f_5(A)$.

Regarding the statement in (1): Tits's construction of Lie algebra from [T], when fed a quaternion algebra Q and an Albert algebra A as inputs, produces a Lie algebra (equivalently, a group) of type E_7 as output. As in 3.1 and 3.3, Tits's construction amounts to applying H^1 to an inclusion of groups $\mathrm{PGL}_2 \times F_4 \subset E_7^{\mathrm{adj}}$, where E_7^{adj} denotes the split adjoint group of type E_7.

5.4. **Example.** Before we prove the proposition, we apply it to the case $k = \mathbb{R}$ and $Q = \mathbb{H}$ from Example 5.1. It follows from the description of real forms of E_7 in terms of the Tits construction from [J, pp. 120, 121] that the fiber of q over G contains the classes $(\pm 1, \text{split Albert})$ and the fiber over G^{cpt} is $(\pm 1, \text{compact Albert})$. By 5.3(2), these four classes are distinct and so represent all the elements of $H^1(\mathbb{R}, G)$. The kernel of r_G consists of $(1, \text{split})$ and $(-1, \text{compact})$, and 5.3(3) says that u sends these two classes to 0 and $(-1)^5$ respectively. That is, u distinguishes the two classes in $\ker r_G$, as promised.

For use in the proof of Proposition 5.3, we note that examining the extended Dynkin diagram of G_2 shows that it contains a maximal subgroup D isomorphic to $(\mathrm{SL}_2 \times \mathrm{SL}_2)/\mu_2$, where the first copy of SL_2 has Dynkin index 1 in G_2 and the second has Dynkin index 3.

5.5. **Lemma.** *For each quaternion k-algebra Q, there is a unique class $q \in H^1(k, D)$ whose image in $H^1(k, G_2)$ is zero and such that D twisted by q is isomorphic to* $(\mathrm{SL}(Q) \times \mathrm{SL}(Q))/\mu_2$.

Proof. Write $\phi \colon \mathrm{SL}_2 \to D$ for the diagonal embedding $\phi(g) = (g, g)$. Fix a square root i of -1 in some algebraic closure of k and put

$$x := \phi \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \quad \text{and} \quad y := \phi \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \quad \in D(k(i)).$$

One checks that x and y are fixed by $\mathrm{Gal}(k(i)/k)$ and so are k-points. Further, $x^2 = y^2 = 1$ and $xy = yx$. Therefore, they generate a subgroup of D isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Write $Q = (a, b)$ for $a, b \in k^\times/k^{\times 2} = H^1(k, \mathbb{Z}/2\mathbb{Z})$, and put q for the image of $(a, b) \in H^1(k, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$ in $H^1(k, D)$. One checks that each of the two projections $D \to \mathrm{PGL}_2$ send q to the class of Q in $H^1(k, \mathrm{PGL}_2)$. It follows that D twisted by q is $(\mathrm{SL}(Q) \times \mathrm{SL}(Q))/\mu_2$.

It is an exercise to see that if Q is split, then q is trivial in $H^1(k, D)$. In particular, the image of q under the Rost invariant $H^1(k, G_2) \to H^3(k, \mathbb{Z}/2\mathbb{Z})$ is a symbol killed by the function field of the Severi-Brauer variety of Q, hence is of the form $[Q] \cdot (c)$ for some $c \in k^\times$. Map $\mathrm{SL}(Q)$ into $(\mathrm{SL}(Q) \times \mathrm{SL}(Q))/\mu_2$ by, say, $g \mapsto (g, 1)$ and consider the diagram

$$\begin{array}{ccccccc}
 & & H^1(k,D) & \longrightarrow & H^1(k,G_2) & \longrightarrow & H^3(k,\mathbb{Z}/2\mathbb{Z}) \\
 & & {\scriptstyle\tau_q}\big\downarrow{\scriptstyle\simeq} & & {\scriptstyle\tau_q}\big\downarrow{\scriptstyle\simeq} & & \big\downarrow{\scriptstyle ?-r_{G_2}(q)} \\
H^1(k,\mathrm{SL}(Q)) & \longrightarrow & H^1(k,D_q) & \longrightarrow & H^1(k,(G_2)_q) & \longrightarrow & H^3(k,\mathbb{Z}/2\mathbb{Z})
\end{array}$$

where τ_q denotes the twisting isomorphism. The diagram commutes by [Gi 00, p. 76, Lem. 7]. The image of $c \in k^\times/\mathrm{Nrd}(Q^\times) = H^1(k, \mathrm{SL}(Q))$ along the bottom row is $[Q] \cdot (c)$ because $\mathrm{SL}(Q)$ has Dynkin index 1 in D_q. Replacing q with $\tau_q^{-1}(c)$ gives the desired class. Tracing through the proof also demonstrates the uniqueness of q. $\square$

Proof of Prop. 5.3. Mapping $\mathrm{SL}_2 \to D$ via $g \mapsto (1, g)$ gives a diagram of inclusions

$$\begin{array}{ccccc}
\mathrm{SL}_2 \times F_4 & \longrightarrow & D \times F_4 & \longrightarrow & G_2 \times F_4 \\
\big\downarrow & & \big\downarrow & & \big\downarrow \\
E_7^{\mathrm{sc}} & \longrightarrow & (\mathrm{SL}_2 \times E_7^{\mathrm{sc}})/\mu_2 & \longrightarrow & E_8
\end{array}$$

where the SL_2 in the upper left has Dynkin index 3 in E_7^{sc} and contains the center of E_7^{sc}. Twisting this diagram by the class q from Lemma 5.5 gives a diagram of inclusions

$$\begin{array}{ccccc}
\mathrm{SL}(Q) \times F_4 & \longrightarrow & D_q \times F_4 & \longrightarrow & G_2 \times F_4 \\
\big\downarrow & & \big\downarrow & & \big\downarrow \\
G & \longrightarrow & (\mathrm{SL}(Q) \times G)/\mu_2 & \longrightarrow & E_8
\end{array}$$

(Twisting E_8 by q gives back the split E_8 because $(E_8)_q$ contains $G_2 \times F_4$, so has k-rank at least 6.) Claim (2) follows immediately and Theorem 3.10 gives (3). The image of $\mathrm{SL}_2 \times F_4$ under $E_7^{\mathrm{sc}} \to E_7^{\mathrm{adj}}$ is the subgroup $\mathrm{PGL}_2 \times F_4$ arising in Tits's construction, giving (1). $\square$

Example 5.1 showed that the Rost invariant could have nonzero kernel on $H^1(k, G)$ for G a group with Tits index (5.2). Proposition 5.3 gives more, namely a lower bound on the complexity of this kernel.

5.6. **Corollary.** *For every simply connected G with Tits index* (5.2)*, the functor $H^1(*, G)_0$ has essential* (2-)*dimension ≥ 3.*

Proof. Put Q for the quaternion division algebra underlying the Tits class of G. Suppose first that $\mathrm{cd}_2\, k \leq 2$. Put $E := k(t_1, t_2, t_3)$ where the t_i's are indeterminates, and write A for the reduced Albert E-algebra with $f_3(A) = [Q] \cdot (t_1)$ and $f_5(A) = f_3(A) \cdot (t_2) \cdot (t_3)$. By Prop. 5.3(2), the image η of (t_1, A) in $H^1(E, G)$ is in $H^1(E, G)_0$. Further, if $\eta = \mathrm{res}_{E'/k}(\eta')$ for some extension E' contained in E and $\eta' \in H^1(E', G)_0$, then $\mathrm{res}_{E/E'} u(\eta') = u(\eta)$, which is the nonzero class $f_5(A)$ in $H^5(E, \mathbb{Z}/2\mathbb{Z})$ by Prop. 5.3(3). Hence $\mathrm{cd}_2\, E' \geq 5$ and E'/k has transcendence degree at least 3. The claim is proved in this case.

For general k, the proof of [M 92, Th. 4] shows that there is an extension F/k such that $G \times F$ has Tits index (5.2) (because $Q \otimes F$ is division) and $\mathrm{cd}_2\, F \leq 2$. As the essential 2-dimension can only decrease when we enlarge the base field, the corollary is proved. $\square$

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 6.6 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, $Z_{G(\overline{F})}(\varphi(A)) = 1$ (in particular, G is adjoint), that there is exactly one $G(\overline{F})$-conjugacy class of homomorphisms $A \to G(\overline{F})$ with character χ, and G is 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, we have:*

(1) *There exists a unique inner form G_0 of G defined over F together with a monomorphism $A \to G_0(F)$ with character χ.*
(2) *If $\psi, \psi' : A \to G_0(F)$ have character χ, then there is a unique $g \in G_0(F)$ such that $\psi' = \mathrm{Int}(g)\, \psi$.*
(3) *For every field extension K/F there is a representation $A \to G(K)$ with character χ iff $G \simeq G_0$ over K.*

We recalled the definition of inner form in Remark 3.5. The composition $G(\overline{F}) \xrightarrow{\pi} \mathrm{GL}_N(\overline{F}) \xrightarrow{\mathrm{tr}} \overline{F}$ is invariant under the twisted Galois action $*$ and so defines a morphism of varieties $G_0 \to \mathbb{A}^1$ over F. Using this, it makes sense to speak of the character of a homomorphism $A \to G_0(F)$ as in the theorem.

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 $\sigma \in \mathrm{Gal}(\overline{F}/F)$. Define now G_0 as the twisted form of G over F by the torsor P, equivalently, the 1-cocycle η. As $\varphi\colon A \to G(\overline{F})$ is invariant under the twisted Galois action, it restricts to a homomorpihsm $A \to G_0(F)$, proving (1).

For (2), we assumed there is a $g \in G_0(\overline{F})$ such that $\psi' = \mathrm{Int}(g)\psi$, and this g is in $G_0(F)$ by the argument from (3.4).

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. As G is split adjoint or $\mathrm{Aut}\, G = G$, it follows that η is already zero in $H^1(K, G)$, proving (3). □

6.3. **Example.** Trivially, one may replace the conclusion of Theorem 6.2.2 with "there exists $f \in \mathrm{Aut}(G_0)(F)$ such that $\psi' = f\psi$"; one simply takes $f = \mathrm{Int}(g)$. However, this f need not be unique, as we now illustrate. Take A, G, φ, π as in Th. 6.2 with G split and suppose that the representation $\pi\varphi$ of A is irreducible (e.g., take $A = \mathrm{PSL}(2, 8)$, $G = G_2$ and π the 7-dimensional fundamental representation as in Example 6.5 below). We may apply the theorem also where G, φ, π are replaced by $G \times G$, $\varphi \times \varphi$, $\pi \times \pi$: the claim $Z_{G\times G}(\varphi(A), \varphi(A)) = 1$ is obvious and the irreducibility hypothesis shows that every homomorphism $A \to G \times G$ with the character $2 \,\mathrm{tr}\, \pi\varphi$ is conjugate to $\varphi \times \varphi$. Taking $F = \overline{F}$ and $\psi := \psi' := \varphi \times \varphi$, we find $g = 1$ in Th. 6.2.2 as stated, but also $\tau\psi = \psi$ where $\tau \in \mathrm{Aut}(G \times G)(F)$ interchanges the two summands.

To characterize the isomorphism criterion of Theorem 6.2.3 we need the following proposition.

6.4. **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 3.9). 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 3.8. $\square$

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.

6.5. **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 $\pi\colon G \to \mathrm{GL}_7$. By [A, 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 [A] and [Griess, Cor. 1 and 2]).

By [A, 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 6.4 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]).

6.6. **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 (resp. and $\zeta_{11} + \bar{\zeta}_{11} \in K$ for $A = \mathrm{SL}(2,32)$).

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 6.5).

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 6.5 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 6.4 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 6.4 (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 (resp., and $\zeta_{11} + \bar{\zeta}_{11} \in K$ for $A = \mathrm{SL}(2, 32)$).

In the same way one can get the following example:

6.7. **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, and by the MPIM Bonn.

References

[A] 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.

[D] E. Dynkin. Semisimple subalgebras of semisimple Lie algebras. *Amer. Math. Soc. Transl. (2)*, **6** (1957), 111–244. [Russian original: Mat. Sbornik N.S. **30(72)** (1952), 349–462].

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

[Ga 09b] ———, *Orthogonal involutions on algebras of degree* 16 *and the Killing form of E_8,* with an appendix by K. Zainoulline, in "Quadratic forms–algebra, arithmetic, and geometry" (R. Baeza, W.K. Chan, D.W. Hoffmann, and R. Schulze-Pillot, eds.), Contemp. Math. **493** (2009), 131–162.

[Gi 00] P. Gille. *Invariants cohomologiques de Rost en caractéristique positive. K-*theory. **21** (2000), 57–100.

[Gi 01] ———, *Cohomologie galoisienne des groupes algebriques quasi-déployés sur des corps de dimension cohomologique* ≤ 2. Compositio Math. **125** (2001), 283–325.

[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.

[M 92] A. Merkurjev. Simple algebras and quadratic forms. *Math. USSR Izv.* **38** (1992), 215–221.

[M 09] ———, *Essential dimension.* in "Quadratic forms–algebra, arithmetic, and geometry" (R. Baeza, W. Chan, D. Hoffmann, and R. Schulze-Pillot, eds.), Contemp. Math. **493** (2009), 299–325.

[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.

[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).

[Serre GC] ———, *Galois cohomology*, Springer, 2002. (Originally published as *Cohomologie galoisienne*, 1962.)

[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`