The kernel of the Rost invariant, Serre's Conjecture II and the Hasse principle for quasi-split groups ${}^{3,6}D_4, E_6, E_7$

V. Chernousov *
Forschungsinstitut für Mathematik
ETH–Zentrum
CH-8092 Zürich
Switzerland

Abstract

We prove that for a simple simply connected quasi-split group of type ${}^{3,6}D_4, E_6, E_7$ defined over a perfect field F of characteristic $\neq 2, 3$ the Rost invariant has trivial kernel. In certain cases we give a formula for the Rost invariant. It follows immediately from the result above that if $\operatorname{cd} F \leq 2$ (resp. $\operatorname{vcd} F \leq 2$) then Serre's Conjecture II (resp. the Hasse principle) holds for such a group. For a (C_2)-field, in particular $\mathbb{C}(x, y)$, we prove the stronger result that Serre's Conjecture II holds for all (not necessary quasi-split) exceptional groups of type ${}^{3,6}D_4, E_6, E_7$.

1 *Introduction*

This paper grew out of the letters [Ch98, Ch00] where we sketched how Harder's proof [H65, H66] of the Hasse principle for exceptional groups ${}^{3,6}D_4, E_6, E_7$ over number fields can be carried over to the case of quasi-split groups defined over a perfect field of cohomological dimension ≤ 2 and how the same ideas can be applied to describe in particular the kernel of the Rost invariant for ${}^2E_6$.

In this paper we give full proofs of all these results. The main ones are the following. Let G_0 be a quasi-split simple simply connected exceptional group of type ${}^{3,6}D_4, E_6, E_7$ defined over a perfect field F of characteristic $\neq 2, 3$. Then

- the kernel of the Rost invariant of G_0 is trivial;
- if $\operatorname{cd} F \leq 2$, then Serre's Conjecture II holds for G_0;
- if $\operatorname{vcd} F \leq 2$, then the Hasse principle Conjecture II holds for G_0;
- if F is a (C_2)-field, then Serre's Conjecture II holds for an arbitrary simple simply connected group (not necessary quasi-split) of the same type as G_0.

*The author gratefully acknowledge the support of TMR ERB FMRX CT-97-0107 and Forschungsinstitut für Mathematik, ETH in Zürich.

In [G97] Gille proved that a group G of inner type E_6 or E_7 defined over F is F-split iff there exist finite field extensions $E_1, \ldots, E_s$ of F splitting G and such that the

$$g.c.d.\{\, [E_1 : F], \ldots, [E_s : F] \,\} = 1.$$

As an easy corollary of our results we obtain that the same quasi-splitting criterion is true for outer forms of type ${}^{3,6}D_4$ or ${}^2E_6$.

Another corollary says that for any F-group G (not necessary quasi-split) of type ${}^{3,6}D_4$, ${}^{1,2}E_6$ or E_7 there exists a chain of cyclic extensions

$$L_0 = F \subset L_1 \subset \cdots \subset L_n$$

of degrees 2 or 3 such that G splits over L_n.

Recall that for all classical groups and groups of type G_2, F_4 Serre's Conjecture II and the Hasse principle Conjecture II were proved by E. Bayer-Fluckiger and R. Parimala [BP95, BP98]. J. Ferrar [Fer69] essentially proved the Hasse principle Conjecture II for inner groups E_6 with the Tits algebras of index ≤ 3. Note also that our results related to Serre's Conjecture II (items $2, 4$) were obtained independently by P. Gille [G01] using different methods.

S. Garibaldi [Gar01] also proved independently the triviality of the kernel of the Rost invariant for quasi-split groups E_6, E_7. His argument is based on consideration of explicit geometric realizations of quasi-split E_6, E_7 and studying properties of algebra structures which occur in his constructions. Since items $2, 3$ immediately follow from the first one, Garibaldi's result gives another proof of Serre's Conjecture II and the Hasse principle Conjecture II for quasi-split groups E_6, E_7.

Our approach is based on different ideas which, as we have already mentioned, come back to G. Harder. In contrast to Garibaldi's paper we focus on studying intrinsic properties of groups splitting over small extensions of the ground field F. The main body of the paper are Sections $4, 5$ where we study properties of groups splitting over an extension K/F of degree $p = 2, 3$. In this part F is an arbitrary field of characteristic $\neq 2, 3$. We show that the F-structure of such groups can be described completely by certain numerical invariants. In the case of quadratic extensions we follow the author proof [Cher89] of the Platonov-Margulis conjecture on the projective simplicity of groups of rational points splitting over a quadratic extension. The results obtained in these two sections allow us to give a formula for the Rost invariant of strongly inner or outer forms of type E_6, E_7 splitting over an extension of degree $p = 2, 3$ in the case where the Galois group $\mathrm{Gal}(F^s/F)$ is a pro-p-group (see 5.12 and 6.2.3).

Gille's splitting criterion [G97] for groups of inner type E_6, E_7 combined with the results described in Sections 4,5 gives proofs of the main theorems more or less quickly. This is done in Sections 6,7,8.

Finally we note that the same methods together with the results of [Ch94, Ch89] prove Serre's Conjecture II for E_8 in each of the following cases:

- the nilpotent closure of the basic field F has cohomological dimension 1;
- Gille's splitting criterion [G97] holds for E_8.

Acknowledgements. I am grateful to J.-P. Serre and S. Garibaldi for useful comments and discussions of the first version of the paper.

Notation

The letter F denotes a perfect field and F^s denotes a separable closure of F. If L/F is a separable extension, then $R_{L/F}$ denotes the Weil functor of restriction of scalars.

We say that a reductive F-subgroup $G' \subset G$ is standard if there is a maximal F-torus T of G normalizing G'.

If G is a reductive algebraic group and $T \subset G$ is a maximal torus, we let $\Sigma(G, T)$ denote the root system of G with respect to T.

If $S \subset G$ is a maximal F-split torus then the semisimple part of the centralizer $C_G(S)$ is called the semisimple F-anisotropic kernel of G.

We number the simple roots of exceptional groups as in [Bourb68].

2 *The Rost invariant and its properties*

In the 90s, for a simple simply connected linear algebraic group G defined over a field F, M. Rost [R] constructed a cohomological $H^3(\mathbb{Q}/\mathbb{Z}(2))$–invariant of G which nowadays is called the Rost invariant of the group G. Thus, for any field extension K/F the Rost invariant associates a canonical map of pointed sets

$$R_G^K : H^1(K, G) \to H^3(K, \mathbb{Q}/\mathbb{Z}(2)).$$

By abuse of language, instead of R_G^K we will use the abbreviated notation R_G for the Rost invariant whenever there is no danger of confusion.

In this section we will state (without proofs) properties of the Rost invariant used in Section 6. For the proofs we refer to [R], [KMRT98] (§31), [EKLV98], [G00], [M01] (Appendix A and B). We note that an explicit formula for R_G is known only in a few cases. But fortunately that will do for us to prove triviality of the kernel of the Rost invariant for quasi-split groups E_6, E_7.

2.1 Inner type A_n

Let A be a central simple algebra over F of exponent e and degree $n+1$. Let $G = SL_1(A)$. Assume that the characteristic of F doesn't divide $n+1$. Then $H^1(F, G) = F^\times / \operatorname{Nrd}(A^\times)$ and the formula for the Rost invariant R_G is given (up to a sign) by

$$R_G : F^\times/\operatorname{Nrd}(A^\times) \longrightarrow H^3(F, \mu_e^{\otimes 2}), \quad R_G(x \operatorname{Nrd}(A^\times)) = (x) \cup [A].$$

Theorem 2.1 ([MS82], Theorem 12.2) *If $n+1$ is square-free, then R_G is injective.*

2.2 Spinor groups

Let f be a quadratic form over a field F of characteristic $\neq 2$ of dimension at least 5 and let $G = Spin(f)$. The set $H^1(F, G)$ fits into the exact sequence

$$H^1(F, Spin(f)) \xrightarrow{\pi} H^1(F, SO(f)) \longrightarrow {}_2BrF.$$

It follows that $\operatorname{Im}\pi$ consists of classes of quadratic forms having the same dimension, discriminant and Hasse-Witt invariant as f. Therefore, for any cocycle $\xi \in Z^1(F, Spin(f))$ we obtain that $\pi([\xi]) - [f] \in I^3F$ and the formula for the Rost invariant is given by

$$R_{Spin(f)} : H^1(F, Spin(f)) \longrightarrow H^3(F, \mu_2^{\otimes 2}), \quad R_{Spin(f)}([\xi]) = e_3(\pi([\xi]) - [f]). \qquad (1)$$

Here e_3 is the Arason invariant [Ar75].

Proposition 2.2 *Let f be a quadratic form of dimension ≤ 12 over a field F such that $G = Spin(f)$ is quasi-split over F, i.e. f is of maximal Witt index. Then R_G has trivial kernel.*

Proof. The statement follows from (1) and the Arason-Pfister Hauptsatz [L73], X.3.1. $\square$

2.3 Outer forms A_n

Let K/F be a quadratic extension, V a vector space of dimension $n+1$ over K and h a hermitian form on V. The group $SU(V,h)$ of isometries with determinant 1 is an almost simple simply connected group of type A_n defined over F and splitting over K. The hermitian form h corresponds to the quadratic form q on the vector space V viewed as an F-vector space: q is given by the formula $q(v) = h(v,v)$. It easily follows that we have a natural embedding $SU(V,h) \hookrightarrow SO(V,q)$ which can be lifted to an embedding $SU(V,h) \hookrightarrow Spin(V,q)$, since $SU(V,h)$ is simply connected. It turns out that the Rost invariant for $SU(V,h)$ is just the restriction of R_{Spin}.

Proposition 2.3 *Let h be a quasi-split hermitian form of dimension ≤ 6. Then the Rost invariant $R_{SU(V,h)}$ has trivial kernel.*

Proof. Apply the same argument as in Proposition 2.2. $\square$

2.4 The Rost numbers

Let G, H be almost simple simply connected linear algebraic groups over F and let $\rho : H \hookrightarrow G$ be an F-embedding. The restriction R_G at $\rho(H)$ gives a cohomological invariant of H, hence is equal to $n_\rho R_H$ for a positive integer n_ρ (see [KMRT98], §31). The smallest such integer is called the Rost number of embedding ρ.

Proposition 2.4 *Let $\rho : H \hookrightarrow G$ be an F-embedding such that $\rho(H)$ is a standard subgroup. Assume that all roots of the root system $\Sigma = \Sigma(G,T)$ of G with respect to a maximal torus T have the same length. Then $n_\rho = 1$; in particular, for any $[\xi] \in H^1(F,H)$ one has $R_G(\rho([\xi])) = R_H([\xi])$.*

Proof. Let T be a maximal F-torus of G normalizing $\rho(H)$. Then $\rho(H)\cdot T$ is a reductive subgroup of G. Since T is a maximal torus of $\rho(H)\cdot T$ and all maximal tori are conjugate, we easily obtain that the connected component S of the intersection $T \cap \rho(H)$ is a maximal torus of $\rho(H)$. Since T normalizes $\rho(H)$, there is a natural embedding

$$\Sigma(\rho(H), S) \hookrightarrow \Sigma(G,T).$$

Hence the coroots of $\rho(H)$ are also the coroots of G (we used the fact that all roots of the root system $\Sigma = \Sigma(G,T)$ have the same length). The rest of the proof follows from [M01], Appendix B. $\square$

3 *Steinberg's theorem*

We state now two theorems which are due to Steinberg [St65]. Although they are not formulated explicitly in [St65], their proofs can be easily obtained from arguments contained in [St65], §10 (see also [PR94], Propositions 6.18, 6.19, p. 338–339).

Let G_0 be a simple (not necessary simply connected) linear algebraic group split or quasi-split over F. Let $\xi \in Z^1(F, G_0)$ be a cocycle and let $G = {}^{\xi}G_0$ be the corresponding twisted group.

Theorem 3.1 *For any maximal torus $S \subset G$ over F there is an F-embedding $S \hookrightarrow G_0$ such that the class $[\xi]$ lies in the image of $H^1(F, S) \to H^1(F, G_0)$.*

Theorem 3.2 *In the notation above assume that G_0 is a simple simply connected group split over F and that G is isotropic over F. Then ξ is equivalent to a cocycle with coefficients in a proper semisimple simply connected F-split subgroup of G_0 which is standard and isomorphic over F^s to a semisimple anisotropic kernel of G.*

Proof. Let $S_1 \subset G$ be a maximal F-split torus. Then the semisimple part of its centralizer $C_G(S_1)$ is a semisimple simply connected F-anisotropic subgroup of G (see [T66]). Let $S \subset G$ be a maximal torus over F containing S_1. By Theorem 3.1, there is an F-embedding $\phi : S \hookrightarrow G_0$ such that

$$[\xi] \in \mathrm{Im}\,[H^1(F, S) \to H^1(F, G_0)].$$

The centralizer $C_{G_0}(\phi(S_1)) \subset G_0$ is a reductive subgroup of G_0 and it follows from the construction of ϕ (see the proof of Proposition 6.18 in [PR94], p. 339) that the groups $C_{G_0}(\phi(S_1))$ and $C_G(S_1)$ are isomorphic over F^s. In particular,

$$H = [C_{G_0}(\phi(S_1)), C_{G_0}(\phi(S_1))]$$

is a simply connected semisimple algebraic group over F.

The group H is clearly standard. It is split over F, since any F-split subtorus in G_0, and in particular $\phi(S_1)$, lies in a maximal F-split torus. Furthermore, from the exact sequence

$$H^1(F, H) \longrightarrow H^1(F, C_{G_0}(\phi(S_1))) \longrightarrow H^1(F, C_{G_0}(\phi(S_1))/H) = 1$$

we see that ξ is equivalent to a cocycle with coefficients in H. □

4 *Groups splitting over a quadratic extension*

Throughout this section F denotes a field of characteristic $\neq 2$, $K = F(\sqrt{d})$ its quadratic extension and τ the non-trivial automorphism of K/F.

Let G be a simple simply connected algebraic group of rank n defined over F and splitting over K. By Lemma 6.17 in [PR94], p. 329, there is a Borel subgroup over K such that $B \cap \tau(B) = T$ is a maximal torus. We remark that this lemma in [PR94] is proved under the condition that $\mathrm{char}(F) = 0$. However the same proof with trivial modifications works in the case of positive characteristic.

The torus T is F-defined and splitting over K, since any K-torus in B splits over K. For our purposes it suffices to treat only the case where T is an F-anisotropic torus.

4.1 The structure of $G(K)$

Let $\mathfrak{g}$ be the Lie algebra of G and let $\Sigma = \Sigma(T, G)$ be the root system of G relative to T. The Borel subgroup B determines an ordering of Σ, hence the system of simple roots $\Pi = \{\alpha_1, \ldots, \alpha_n\}$. Let Σ^+ (resp. Σ^-) be the set of positive (resp. negative) roots and let

B^- be the Borel subgroup opposite to B with respect to T. We pick a Chevalley basis [St67]

$$\{H_{\alpha_1}, \dots H_{\alpha_n},\ X_\alpha,\ \alpha \in \Sigma\}$$

in $\mathfrak{g}$ corresponding to the pair (T, B). This basis is unique up to signs and automorphisms of $\mathfrak{g}$ which preserve B and T (see [St67], §1, Remark 1).

Since G is a Chevalley (in other words, quasi-split) group over K, its K-structure is well known. For details and proofs of all standard facts about $G(K)$ used in this section we refer to [St67]. In particular, we refer to [St67] for the definition of the operators $X_\alpha^n\,/n!$ in the case $\mathrm{char}(F) = p > 0$ (see also [SGA3]). Recall only that $G(K)$ is generated by the so-called root subgroups $U_\alpha = \langle x_\alpha(u) \mid u \in K\rangle$, where $\alpha \in \Sigma$ and

$$x_\alpha(u) = \sum_{n=0}^{\infty} u^n X_\alpha^n\,/n!\ ,$$

and T is generated by the one-parameter subgroups

$$T_\alpha = T \cap G_\alpha = \langle\, h_\alpha(t) \mid t \in K^*\,\rangle.$$

Here G_α is the subgroup generated by $U_{\pm\alpha}$ and

$$h_\alpha(t) = w_\alpha(t)\, w_\alpha(1)^{-1}, \quad w_\alpha(t) = x_\alpha(t)\, x_{-\alpha}(-t^{-1})\, x_\alpha(t).$$

Furthermore, since G is a simply connected group, the following relations hold in G (cf. [St67], Lemma 28 b), Lemma 20 c)):

(A) $T = T_{\alpha_1} \times \cdots \times T_{\alpha_n}$;

(B) for any two roots $\alpha,\, \beta \in \Sigma$ we have

$$h_\alpha(t)\, x_\beta(u)\, h_\alpha(t)^{-1} = x_\beta(t^{\langle\beta,\alpha\rangle} u)$$

where $\langle\beta, \alpha\rangle = 2\,(\beta, \alpha)/(\alpha, \alpha)$.

If $\Delta \subset \Sigma^+$ is a subset, we let G_Δ denote the subgroup generated by $U_{\pm\alpha}$, $\alpha \in \Delta$.

4.2 Galois descent data

We shall now describe explicitly the F-structure of G, i.e. the action of τ on the generators $\{x_\alpha(u),\ \alpha \in \Sigma\}$.

Lemma 4.1 *$\tau(\alpha) = -\alpha$ for any $\alpha \in \Sigma$.*

Proof. The character $\alpha + \tau(\alpha)$ of T is F-defined, hence it is zero, since by our assumption T is F-anisotropic. □

Lemma 4.2 *$\tau(B) = B^-$.*

Proof. The statement follows immediately from Lemma 4.1. □

Lemma 4.3 *$T_\alpha \simeq R^{(1)}_{K/F}(G_{m,K})$.*

Proof. T_α is a one-dimensional F-torus splitting over K. According to Lemma 4.1, τ acts on its character lattice by multiplication by -1. So the result follows. $\square$

Let $\alpha \in \Sigma$. Since, by Lemma 4.1, $\tau(\alpha) = -\alpha$, there exists a constant $c_\alpha \in K^\times$ such that $\tau(X_\alpha) = c_\alpha X_{-\alpha}$. It follows that the action of τ on $G(K)$ is determined completely by the family $\{c_\alpha,\, \alpha \in \Sigma\}$. We call these constants structure constants of G with respect to T. We summarize their properties in the following two lemmas.

Lemma 4.4 *Let $\alpha \in \Sigma$. Then we have*
(i) $c_{-\alpha} = c_\alpha^{-1}$*;*
(ii) $c_\alpha \in F^\times$*;*
(iii) *if $\beta \in \Sigma$ is a root such that $\alpha + \beta \in \Sigma$, then $c_{\alpha+\beta} = \pm c_\alpha\, c_\beta$; in particular, the family $\{c_\alpha,\, \alpha \in \Sigma\}$ is determined completely by its subfamily $\{c_{\alpha_1}, \ldots, c_{\alpha_n}\}$.*

Proof. (i) Apply τ to the equality $[X_\alpha, X_{-\alpha}] = H_\alpha$ and use the fact that $\tau(H_\alpha) = -H_\alpha$.
(ii) One has $X_\alpha = \tau^2(X_\alpha) = \tau(c_\alpha)c_{-\alpha}X_\alpha$, hence $\tau(c_\alpha)c_{-\alpha} = 1$. Substituting $c_{-\alpha} = c_\alpha^{-1}$ we obtain $\tau(c_\alpha) = c_\alpha$, as required.
(iii) Apply τ to the equality $[X_\alpha, X_\beta] = \pm(r+1)X_{\alpha+\beta}$. Here r is an integer depending on α, β only. $\square$

Remark 4.5 The number r above is the biggest integer such that

$$\beta,\ \beta - \alpha, \ldots, \beta - r\alpha$$

are roots, but $\beta - (r+1)\alpha$ is not a root. Therefore, this number is equal to 0 or 1, since, by our assumption, $\alpha + \beta$ is a root. It follows, in particular, that $r + 1 \neq 0$, since we assumed that $\mathrm{char}(F) \neq 2$.

Lemma 4.6 $\tau[\, x_\alpha(u)\,] = x_{-\alpha}(c_\alpha \tau(u))$ *for any $u \in K$ and $\alpha \in \Sigma$.*

Proof. This follows from the equality $x_\alpha(u) = \exp(uX_\alpha)$. $\square$

4.3 Comparison of different Galois descent data

The family $\{c_\alpha,\, \alpha \in \Sigma\}$ determining the action of τ on $G(K)$ depends on the chosen Borel subgroup B and the corresponding Chevalley basis. Given another Borel subgroup and Chevalley basis we get another family of constants and we want now to describe the relation between the old ones and the new ones.

Let $B' \subset G$ be a Borel subgroup over K such that the intersection $T' = B' \cap \tau(B')$ is a maximal and F-anisotropic torus. Both tori T and T' are isomorphic over F since, by Property (A) in 4.1 and Lemma 4.3, they are the direct products of n copies of the torus $R^{(1)}_{K/F}(G_{m,K})$. Furthermore, there exists an F-isomorphism $T \to T'$ preserving positive roots, i.e. which takes $(\Sigma')^+ = \Sigma(G,T')^+$ into $\Sigma^+ = \Sigma(G,T)^+$. Any such isomorphism can be extended to an inner automorphism

$$i_g : G \longrightarrow G, \quad x \to g\,x\,g^{-1}$$

for some $g \in G(F^s)$, which takes B into B' (see [Hum75], Theorem 32.1).

Lemma 4.7 *g can be chosen in $G(K)$.*

Proof. Since the restriction $i_g|_T$ is an F-defined isomorphism we easily get that $t_\sigma = g^{-1+\sigma} \in T(F^s)$ for any $\sigma \in \mathrm{Gal}\,(F^s/F)$. Consider the cocycle $\xi = (t_\sigma) \in Z^1(F,T)$. Since T splits over K, $res_K(\xi)$ viewed as a cocycle in T is trivial, by Hilbert's Theorem 90. It follows that there is $z \in T(F^s)$ such that $t_\sigma = z^{1-\sigma}$, $\sigma \in \mathrm{Gal}\,(F^s/K)$. Then the element $g' = gz$ is stable under $\mathrm{Gal}\,(F^s/K)$ and clearly $g'B(g')^{-1} = B'$. □

Let g be an element from Lemma 4.7 and let $t = g^{-1+\tau}$. Since t belongs to $T(K)$, it can be written (cf. 4.1) as a product $t = h_{\alpha_1}(t_1)\cdots h_{\alpha_n}(t_n)$, where $t_1,\ldots,t_n \in K^\times$ are some parameters. Using the equality $t\,\tau(t) = 1$ and the fact that τ acts on characters of T as multiplication by -1 one can easily see that $t_1,\ldots,t_n \in F^\times$. Consider the set

$$\{H'_{\alpha_1} = gH_{\alpha_1}g^{-1},\ldots,H'_{\alpha_n} = gH_{\alpha_n}g^{-1},\ X'_\alpha = gX_\alpha g^{-1},\ \alpha \in \Sigma\}$$

which is a Chevalley basis related to the pair (T',B'). Let $\{c'_\alpha,\ \alpha \in \Sigma\}$ be the corresponding structure constants.

Lemma 4.8 *For each $\alpha \in \Sigma$ one has $c'_\alpha = t_1^{-\langle\alpha,\alpha_1\rangle}\cdots t_n^{-\langle\alpha,\alpha_n\rangle}\cdot c_\alpha$.*

Proof. Apply τ to the equality $X'_\alpha = gX_\alpha g^{-1}$ and use relation (B) in 4.1. □

The converse is also true.

Lemma 4.9 *Let $g \in G(K)$ be an element such that $t = g^{-1+\tau} \in T(K)$. Then $T' = gTg^{-1}$ is an F-defined maximal torus splitting over K and the restriction of the inner automorphism i_g to T is an F-defined isomorphism. The structure constants $\{c'_\alpha\}$ related to T' are given by the formulas in Lemma 4.8.*

Proof. This is clear. □

Remark 4.10 The elements $g \in G(K)$ such that $g^{-1+\tau} \in T(K)$ correspond to the elements of the kernel of $\mu : H^1(K/F,T(K)) \to H^1(K/F,G(K))$. The exact sequence in Galois cohomology attached to the exact sequence

$$1 \longrightarrow T(K) \longrightarrow G(K) \longrightarrow (G/T)(K) \longrightarrow 1$$

shows that they come from F-points of the homogeneous variety G/T. It was shown in [Cher89] that G/T is an F-rational variety, hence all such elements can be parametrized by points from an open subset of an affine space.

Remark 4.11 The restriction of i_g to T induces a bijection between $H^1(K/F,T(K))$ and $H^1(K/F,T'(K))$. If we identify these two sets (recall that T and T' are isomorphic over F), then this bijection is the translation by the class of the cocycle $\xi = (t_\tau) \in Z^1(K/F,T(K))$, where $t_\tau = g^{-1+\tau}$.

4.4 Type A_n

It follows from Lemma 4.6 that, for each root $\alpha \in \Sigma$, the subgroup G_α of G is defined over F. Since it is a simple simply connected group of rank 1, we obtain that $G_\alpha \simeq SL(1,D_\alpha)$, where D_α is a quaternion algebra over F.

Lemma 4.12 *$D_\alpha \simeq (d,c_\alpha)$.*

Proof. Since $T_\alpha = R^{(1)}_{K/F}(G_{m,K}) \subset SL(1, D_\alpha)$, the algebra D_α splits over K. Hence it is of the form $D_\alpha = (d, f)$, where $f \in F^\times$, and we need to prove that

$$c_\alpha \equiv f \pmod{N_{K/F}(K^\times)}.$$

Let $i, j \in D^\times$ be elements such that $i^2 = d$, $j^2 = f$, $ij = -ji$. We may identify T_α with $R^{(1)}_{K/F}(F(i)^\times)$. A straightforward computation shows that the triple

$$H'_\alpha = \frac{1}{\sqrt{d}}\, i, \quad X'_\alpha = \frac{-\sqrt{d}+i}{-2f\sqrt{d}}\, j, \quad X'_{-\alpha} = \frac{\sqrt{d}+i}{2\sqrt{d}}\, j$$

belonging to $D \otimes_F K$ is a Chevalley basis with respect to T_α. Note that under the standard identification $D \otimes_F K \simeq M_2(K)$ the triple H'_α, X'_α, $X'_{-\alpha}$ corresponds to the matrices

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}.$$

From the above formulas for X_α and X'_α we easily get $\tau(X'_\alpha) = fX'_{-\alpha}$.

Let us now come back to our former Chevalley basis $H_\alpha, X_\alpha, X_{-\alpha}$. Recall that a Chevalley basis is unique up to an automorphism of the corresponding Lie algebra $sl_2(K)$. It follows that there is an inner automorphism i_d of D_K which takes $H'_\alpha, X'_\alpha, X'_{-\alpha}$ into $H_\alpha, X_\alpha, X_{-\alpha}$. Since H_α and H'_α are proportional (being elements of the Lie algebra of T_α), d lies in the Weyl group of T_α. Then X_α is proportional to either X'_α or $X'_{-\alpha}$. Without loss of generality we may assume that X_α is proportional to X'_α. Then we have $X_\alpha = zX'_\alpha$, $X_{-\alpha} = z^{-1}X'_{-\alpha}$ for some $z \in K^\times$ and hence

$$c_\alpha X_{-\alpha} = \tau(X_\alpha) = \tau(z)\tau(X'_\alpha) = \tau(z) f X'_{-\alpha} = z\tau(z) f X_{-\alpha},$$

implying $c_\alpha = z\tau(z)f$, as required. □

In conclusion of this subsection we consider outer forms of type ${}^2A_{n-1}$ splitting over a quadratic extension. Let

$$h = a_1 x_1 x_1^\tau - a_2 x_2 x_2^\tau + \ldots + (-1)^{n-1} a_n x_n x_n^\tau$$

be a hermitian form of dimension n relative to the quadratic extension K/F, where $a_1, \ldots, a_n$ are elements in $F^\times$. Let $T \subset \mathrm{SU}(h)$ be a maximal F-torus consisting of all diagonal matrices in $\mathrm{SU}(h)$. Clearly, T is F-anisotropic and splits over K. As above, we denote the corresponding structure constants related to T and the standard Chevalley basis of $\mathrm{SU}(h)_K \simeq \mathrm{SL}_{n,K}$ by $\{c_\alpha,\ \alpha \in \Sigma = \Sigma(SU(h), T)\}$.

Lemma 4.13 *One has the following:*

$$c_{\alpha_1} \equiv a_1/a_2,\ c_{\alpha_2} \equiv a_2/a_3,\ \ldots,\ c_{\alpha_{n-1}} \equiv a_{n-1}/a_n \pmod{N_{K/F}(K^\times)}.$$

Proof. The subgroup $G_{\alpha_i} \subset \mathrm{SU}(h)$ coincides with $\mathrm{SU}(h_i) \subset \mathrm{SU}(h)$, where

$$h_i = a_i x_i x_i^\tau - a_{i+1} x_{i+1} x_{i+1}^\tau.$$

Since $\mathrm{SU}\,(h_i) \simeq \mathrm{SL}\,(1, D_{\alpha_i})$ and $D_{\alpha_i} = (d, a_{\alpha_i}/a_{\alpha_{i+1}})$, the result follows from Lemma 4.12. □

4.5 A cohomological property

Proposition 4.14 *The natural map $H^1(K/F, T(K)) \to H^1(K/F, G(K))$ is surjective.*

Proof. We are under the conditions of Lemma 6.28 in [PR94], p. 369, so the result follows from that lemma. $\square$

5 *Groups E_6, E_7 splitting over cubic extensions.*

Throughout this section F denotes a field of characteristic $\neq 3$, K/F a cyclic extension of degree 3 and τ a non-trivial automorphism of K/F. We also assume that $\Gamma = Gal(F^s/F)$ is a pro-3-group. We let G_0 denote a simple simply connected split group over F of type E_6, E_7.

Theorem 5.1 *Any cocycle $\xi \in Z^1(K/F, G_0)$ is equivalent to a cocycle with coefficients in a standard simple simply connected F-subgroup $H < G_0$ of inner type A_2.*

Proof. We split our proof into a sequence of simple observations. The main ingredients are the classification of Tits indices [T66], Steinberg theorem [St65] and the fact that Γ is a pro-3-group; in particular there are no simple F-anisotropic groups of types A_1, A_3, B_n, C_n, ${}^{1,2}D_n, G_2$. We let $G = {}^{\xi}G_0$ denote the corresponding twisted group. Consider first the key case where G is an F-anisotropic group of type E_6.

5.1 Type E_6: anisotropic case

5.1.1 Construction of a special torus

Proposition 5.2 *G contains a maximal F-defined torus S splitting over K.*

Proof. We follow Harder's arguments [H65, H66] (cf. [PR94], Chapter 6). In this part G is not necessary a strongly inner form. Let us start with the construction of a simple simply connected F-subgroup of G of type ${}^3D_4$ splitting over K. Since G splits over K, we choose a K-split maximal torus T. Let $\Sigma = \Sigma(G,T)$ and let $\Pi = \{\alpha_1, \dots, \alpha_6\} \subset \Sigma$ be a basis. Let $\mathcal{P} \subset G$ be the standard parabolic subgroup over K corresponding to α_6.

Consider the connected component C of the intersection $\mathcal{P} \cap \tau(\mathcal{P}) \cap \tau^2(\mathcal{P})$. It is defined over F, hence reductive, since G is F-anisotropic. Denote the central torus of C by S_1 and let $C^{(1)} = [C,C] = C_1 \cdot \ldots \cdot C_s$ be the decomposition of the semisimple part of C into an almost direct product of the simple components over F^s. It easily follows from $\dim C \geq 30$ that $C^{(1)}$ contains a simple component, say C_1, of type not A_n (see Lemma 6.32 in [PR94], p. 380).

Lemma 5.3 *C_1 is defined over F.*

Proof. If C_1 is defined over L/F, then there is a canonical embedding $H_1 = R_{L/F}(C_1) \hookrightarrow C$, since C is F-defined. Consider a Levi subgroup $\mathcal{L} \subset \mathcal{P}$ over K containing C. The parabolic subgroup $\mathcal{P}$ corresponds to α_6, so the semisimple part $[\mathcal{L}, \mathcal{L}]$ of $\mathcal{L}$ has type D_5. It follows then from the inclusion $[C,C] \subset [\mathcal{L}, \mathcal{L}]$ that

$$\operatorname{rank} H_1 = [L : F] \cdot \operatorname{rank} C_1 \leq 5.$$

But $[L : F]$ is a power of 3 and C_1 is not of type A_n, hence $[L : F] = 1$. $\square$

Lemma 5.4 *C_1 has type ${}^3D_4$.*

Proof. The conditions C_1 is F-anisotropic and $\operatorname{rank} C_1 \leq 5$ imply that C_1 is of type either F_4 or D_4. A group of type F_4 being a group of dimension 52 can not be embedded into the group $[\mathcal{L}, \mathcal{L}]$ of type D_5, since $\dim [\mathcal{L}, \mathcal{L}] = 45$. So the result follows. $\square$

Lemma 5.5 *$C^{(1)} = C_1$.*

Proof. If $C^{(1)}$ contains another simple component C_2, then its rank is 1, since $C^{(1)}$ has rank at most 5. It follows that C_2 is defined over F and hence F-isotropic being a group of type A_1 — a contradiction. $\square$

Lemma 5.6 *$S_1 \simeq R^{(1)}_{K/F}(G_{m,K})$.*

Proof. We have $\dim C \geq 30$. On the other hand, $C^{(1)} = [C, C]$ is a group of dimension 28 and rank 4. Hence $\dim S_1 = 2$. According to the classification of 2-dimensional tori [V98] it suffices now to show that S_1 is K-split or, what is the same, K-isotropic, since Γ is a pro-3-group.

Let $\mathcal{L}$ be a Levi subgroup of $\mathcal{P}$ over K containing C. Both groups $\mathcal{L}$ and C are reductive and have the same rank 6. It follows that the central torus A of $\mathcal{L}$ is contained in C. Since it commutes with $[\mathcal{L}, \mathcal{L}]$ which contains $[C, C] = C_1$, we conclude that $A \subset S_1$. It remains to note that A is K-split. $\square$

Lemma 5.7 *C_1 contains a maximal torus S_2 isomorphic to $R^{(1)}_{K/F}(G_{m,K}) \times R^{(1)}_{K/F}(G_{m,K})$.*

Proof. Consider the following chain of inclusions:

$$C = S_1 \cdot C_1 \subset C_G(S_1) \subset C_G(A) = \mathcal{L}.$$

It gives

$$[C, C] \subset [C_G(S_1), C_G(S_1)] \subset [\mathcal{L}, \mathcal{L}].$$

Since $[C, C]$ and $[\mathcal{L}, \mathcal{L}]$ have type D_4 and D_5 respectively and $[C_G(S_1), C_G(S_1)]$ is a group of rank 4, we conclude that $[C_G(S_1), C_G(S_1)] = [C, C] = C_1$.

Since S_1 splits over K, so are $C_G(S_1)$ and $[C_G(S_1), C_G(S_1)] = C_1$. Thus C_1 is an F-group of type D_4 splitting over K. Then arguing just as in [PR94], p. 371–372, we obtain that C_1 contains a torus of the required form. $\square$

Lemmas 5.6 and 5.7 show that $S = S_1 \cdot S_2$ is an F-defined maximal torus of G splitting over K. Proposition 5.2 is proved. $\square$

Let S be the torus constructed in Proposition 5.2. According to Theorem 3.1 there exists an F-embedding $S \hookrightarrow G_0$ such that

$$[\xi] \in \operatorname{Im} [H^1(F, S) \longrightarrow H^1(F, G_0)].$$

We fix this embedding and starting from this point we may forget about the way it was constructed. The only fact we need to know is that S is an almost direct product of three copies of $R^{(1)}_{K/F}(G_{m,K})$. Based on this fact we are going to show that there exists a decomposition

$$S \simeq R^{(1)}_{K/F}(G_{m,K}) \times R^{(1)}_{K/F}(G_{m,K}) \times R^{(1)}_{K/F}(G_{m,K}) \tag{2}$$

and a new F-embedding $\eta : S \hookrightarrow G_0$ with the following properties:

(a) *the images of the first two components in decomposition (2) lie in an F-split standard subgroup of G_0 isomorphic to $SL_3 \times SL_3$,*

(b) ξ *is equivalent to a cocycle with coefficients in $\eta(S)$.*

5.1.2 The Weyl group W_{E_6}

Let $\Sigma = \Sigma(G_0, S)$ be the root system of G_0 with respect to S, $W = W(\Sigma)$ the Weyl group of Σ and $\Pi = \{\alpha_1, \ldots, \alpha_6\}$ a fixed basis of Σ.

Lemma 5.8 *Let $W_3 \subset W$ be a 3-Sylow subgroup. Then*

$$W_3 \simeq (\mathbb{Z}/3 \times \mathbb{Z}/3 \times \mathbb{Z}/3) \rtimes \mathbb{Z}/3,$$

where $\mathbb{Z}/3$ acts by permuting the components of $\mathbb{Z}/3 \times \mathbb{Z}/3 \times \mathbb{Z}/3$.

Proof. We have $\#(W_3) = 3^4$. Let Σ_1, Σ_2 and Σ_3 be the three subroot systems of Σ of type A_2 generated by roots $\langle \alpha_1, \alpha_3 \rangle$, $\langle \alpha_5, \alpha_6 \rangle$ and $\langle \alpha_2, -\beta \rangle$ respectively, where $\beta \in \Sigma$ is the positive root of maximal length with respect to the basis Π. Let $w_0, w_1 \in W$ be the elements of maximal length with respect to the basis $\{\alpha_1, \ldots, \alpha_6\}$ and $\{\alpha_1, \alpha_3, \alpha_4, \alpha_2, -\beta, \alpha_5\}$ respectively.

It is easy to see that $w = w_0 \cdot w_1$ has order 3 and takes the roots $\alpha_1, \alpha_3, \alpha_5, \alpha_6, \alpha_2, -\beta$ into $\alpha_6, \alpha_5, \alpha_2, -\beta, \alpha_3, \alpha_1$ respectively. Therefore w permutes the components of the subsystem $\Sigma' = \Sigma_1 \times \Sigma_2 \times \Sigma_3 \subset \Sigma$ and their Weyl groups. Let $v_1 \in W(\Sigma_1)$ be an arbitrary element of order 3. Then $v_2 = wv_1w^{-1} \in W(\Sigma_2)$ and $v_3 = wv_2w^{-1} \in W(\Sigma_3)$. It follows that v_1, v_2, v_3 commutes and w permutes them; in particular, v_1, v_2, v_3, w generate a subgroup $W_3 \subset W$ of order 3^4. □

Since S is an F-defined maximal torus splitting over K, the group $\mathrm{Gal}(K/F)$ acts on the root system Σ. Thus we have a natural embedding $\mathrm{Gal}(K/F) \hookrightarrow W$. Choosing an appropriate basis of Σ we may assume that the image of $\mathrm{Gal}(K/F)$ lies in the 3-Sylow subgroup W_3 constructed in Lemma 5.8.

Lemma 5.9 *The image of* $\mathrm{Gal}(K/F)$ *lies in a subgroup $\langle v_1, v_2, v_3 \rangle$ of W_3.*

Proof. Let $\tau = v_1^{i_1} v_2^{i_2} v_3^{i_4} w^{i_4}$, where $i_1, \ldots, i_4$ are integers. Since S is F-anisotropic, we have $\alpha_1 + \tau(\alpha_1) + \tau^2(\alpha_1) = 0$. On the other hand, assuming that $i_4 \neq 0$ we easily obtain that $\tau(\alpha_1) \in \Sigma_2$ and $\tau^2(\alpha_1) \in \Sigma_3$. But then $\alpha_1 + \tau(\alpha_1) + \tau^2(\alpha_1) \neq 0$ — a contradiction. □

5.1.3 Special embedding $S \hookrightarrow G_0$

Lemma 5.9 shows that $\Sigma_1, \Sigma_2, \Sigma_3$ are stable under the action of $\mathrm{Gal}(K/F)$, hence the subgroup $G_{\Sigma_1} \cdot G_{\Sigma_2} \cdot G_{\Sigma_3} \subset G_0$ is F-defined and of type $A_2 \times A_2 \times A_2$. Note also that the three intersections $S \cap G_{\Sigma_i}$ are 2-dimensional tori isomorphic to $R^{(1)}_{K/F}(G_{m,K})$. This follows from the facts that they are F-anisotropic, splitting over K and from the classification of 2-dimensional tori. Clearly, the tori $S \cap G_{\Sigma_i}$, $i = 1, 2, 3$, generate S.

We are now ready to construct a new embedding $S \hookrightarrow G_0$ with the required properties (a) and (b). Let $T \subset G_0$ be a maximal F-split torus and let $\{\beta_1, \ldots, \beta_6\}$ be a basis of the root system $\Sigma(G_0, T)$. We consider the subsystems $\Sigma_1', \Sigma_2', \Sigma_3'$ generated by

$\{\beta_1, \beta_3\}$, $\{\beta_5, \beta_6\}$, $\{\beta_2, -\beta'\}$ respectively. Here β' is the root of maximal length with respect to the basis $\{\beta_1, \ldots, \beta_6\}$. Since $G_{\Sigma'_1}, G_{\Sigma'_2}$ and $G_{\Sigma'_3}$ are isomorphic to SL_3 over F, there are F-embeddings $\phi_i : R^{(1)}_{K/F}(G_{m,K}) \hookrightarrow G_{\Sigma'_i}$, $i = 1, 2, 3$. Then the torus

$$S' = \operatorname{Im}\phi_1 \cdot \operatorname{Im}\phi_2 \cdot \operatorname{Im}\phi_3$$

is maximal in G_0 isomorphic to S over F.

Proposition 5.10 $[\xi] \in \operatorname{Im}[H^1(F, S') \longrightarrow H^1(F, G_0)]$.

Proof. It follows from the constructions of S and S' that there is an F-defined isomorphism $S \to S'$ which takes $\Sigma(G_0, S)$ into $\Sigma(G_0, S')$. Any such isomorphism can be extended to an inner automorphism $i_g : G_0 \to G_0$ over F^s, by Theorem 32.1 in [Hum75]. Since the restriction $i_g|_S$ is F-defined, we obtain that $\sigma(g)^{-1} \cdot g \in S$ for any $\sigma \in \operatorname{Gal}(F^s/F)$. Let $\xi = (a_\sigma)$, where $a_\sigma \in S$. Then the equivalent cocycle

$$\xi' = (g \cdot a_\sigma \cdot \sigma(g)^{-1}) = (g \cdot a_\sigma \cdot (\sigma(g)^{-1} g) \cdot g^{-1})$$

takes values in S' and we are done. □

5.1.4 The direct product decomposition

In view of Proposition 5.10 the torus S' satisfies condition (b). Let us prove that it satisfies condition (a) as well. We do not need the torus S any more and to ease notation we will denote S' by S. We also denote $\Sigma(G_0, S')$ by Σ and let $\Pi = \{\alpha_1, \ldots, \alpha_6\}$ be the corresponding basis of Σ.

For any root $\alpha \in \Sigma$ we have $\alpha + \tau(\alpha) + \tau^2(\alpha) = 0$, since S is F-anisotropic. It follows that the set $\{\pm\alpha, \pm\tau(\alpha)\}$ generates an F-defined subsystem of Σ of rank at most 2. This subsystem has the automorphism τ, which is of order 3, hence it has type A_2. In particular, the subgroup $G_{\{\alpha, \tau(\alpha)\}}$ is an F-defined inner form of type A_2 splitting over K. For $\alpha \in \Sigma$ we let

$$S_{\{\alpha, \tau(\alpha)\}} = S \cap G_{\{\alpha, \tau(\alpha)\}}.$$

Since $S_{\{\alpha, \tau(\alpha)\}}$ splits over K, we obtain that $S_{\{\alpha, \tau(\alpha)\}} \simeq R^{(1)}_{K/F}(G_{m,K})$.

Recall also that, by construction, the three subsystems of Σ generated by the roots $\{\alpha_1, \alpha_3\}$, $\{\alpha_5, \alpha_6\}$ and $\{\alpha_2, -\beta\}$ are stable under the action of $\operatorname{Gal}(K/F)$ and have type A_2. Hence

$$S_{\{\alpha_1, \tau(\alpha_1)\}} = S_{\{\alpha_1, \alpha_3\}}, \quad S_{\{\alpha_5, \tau(\alpha_5)\}} = S_{\{\alpha_5, \alpha_6\}}.$$

Proposition 5.11 *The product morphism $S_{\{\alpha_1, \alpha_3\}} \times S_{\{\alpha_5, \alpha_6\}} \times S_{\{\alpha_4, \tau(\alpha_4)\}} \longrightarrow S$ is an F-isomorphism.*

Proof. It suffices to show that it is an isomorphism over F^s. We use notation from Steinberg's book [St67]. Recall that given a root $\alpha \in \Sigma$, one can associate to it the one-parameter subgroup $S_\alpha = \langle\, h_\alpha(t) \mid t \in \overline{F}^\times \,\rangle \leq S$. By 4.1 (A), S is the direct product of such subgroups corresponding to $\alpha_1, \ldots, \alpha_6$. If $\alpha = m_1\alpha_1 + \cdots + m_6\alpha_6$, then

$$h_\alpha(t) = h_{\alpha_1}(t)^{m_1} \cdots h_{\alpha_6}(t)^{m_6}, \tag{3}$$

since all roots have the same length.

It is clear that $\tau(\alpha_4) \neq \pm\beta$, since otherwise in view of the fact that the root subsystem $\Sigma_3 = \langle\, \alpha_2, -\beta \,\rangle$ is F-defined we would have $\alpha_4 \in \Sigma_3$. Therefore $\tau(\alpha_4)$ is of the form

$$\tau(\alpha_4) = \pm(m_1\alpha_1 + m_3\alpha_3 + \cdots + m_6\alpha_6 + \alpha_2),$$

where $m_1, m_3, \ldots, m_6$ are positive integers. Then it follows from (3) that

$$S = S_{\alpha_1} \times S_{\alpha_3} \times \cdots \times S_{\alpha_6} \times S_{\tau(\alpha_4)} = S_{\{\alpha_1,\alpha_3\}} \times S_{\{\alpha_5,\alpha_6\}} \times S_{\{\alpha_4,\tau(\alpha_4)\}},$$

as required. $\square$

5.1.5 Concluding argument

Proof of Theorem 5.1 in anisotropic case. By Proposition 5.10 we may assume that $\xi \in Z^1(F, S)$. Let $\xi = (a_\sigma)$, where $a_\sigma \in S$. Applying Proposition 5.11 we split ξ into the product of three cocycles $\xi = \xi_1 \cdot \xi_2 \cdot \xi_3$ with coefficients in $S_{\{\alpha_1,\alpha_3\}}, S_{\{\alpha_5,\alpha_6\}}$ and $S_{\{\alpha_4,\tau(\alpha_4)\}}$ respectively. Since G_{Σ_1} and G_{Σ_2} are isomorphic to SL_3, ξ_1 and ξ_2 are trivial cocycles.

Let $g_1 \in G_{\Sigma_1}$ and $g_2 \in G_{\Sigma_2}$ be such that $\xi_1 = (g_1^{-1+\sigma})$ and $\xi_2 = (g_2^{-1+\sigma})$. Clearly, g_1 and g_2 commutes. It follows that the equivalent cocycle

$$\xi' = ((g_1g_2)\, a_\sigma\, (g_1g_2)^{-\sigma}) = (g_1g_2)^\sigma\, [(g_2^{-\sigma}g_2)(g_1^{-\sigma}g_1)a_\sigma]\, (g_1g_2)^{-\sigma}$$

has coefficients in

$$(g_1g_2)^\sigma\, S_{\{\alpha_4,\tau(\alpha_4)\}}\, (g_1g_2)^{-\sigma} \leq (g_1g_2)^\sigma\, G_{\{\alpha_4,\tau(\alpha_4)\}}\, (g_1g_2)^{-\sigma}.$$

The condition $(g_1g_2)^{-1}\,(g_1g_2)^\sigma \in S$ easily implies that

$$H = (g_1g_2)^\sigma\, G_{\{\alpha_4,\tau(\alpha_4)\}}\, (g_1g_2)^{-\sigma} \tag{4}$$

is an F-defined subgroup of type A_2 splitting over K, hence we are done.

Remark 5.12 Let $S \hookrightarrow G_0$ be the embedding constructed in 5.1.3. Proposition 5.10 says that the canonical map $H^1(K/F, S) \to H^1(K/F, G_0)$ is surjective. By Proposition 5.11, any cocycle $\xi \in Z^1(K/F, G_0)$ can be written as a triple

$$\xi = (a_1N_{K/F}(K^\times), a_2N_{K/F}(K^\times), a_3N_{K/F}(K^\times)),$$

where $a_1, a_2, a_3 \in F^\times$. One can show that the above subgroup (4) is isomorphic to $SL(1, T)$, where T is a cubic central simple algebra of the form $T = (K/F, a_1^{n_1}a_2^{n_2}c_{\alpha_4})$ for certain integers n_1, n_2 and a constant $c_{\alpha_4} \in F^\times$. These integers and the constant can be computed explicitly, but we omit details. As a result, we obtain the following formula for the Rost invariant:

$$R_{G_0}([\xi]) = T \cup (a_3).$$

5.1.6 Moving Lemma

The above argument will be used below several times. Let us formulate it for the future reference as follows.

Moving Lemma *Let G be a simple group over F and let T be a maximal torus of G over F. Let $\xi \in Z^1(F, T)$ be a cocycle. Assume that $\xi = \xi_1 \cdot \xi_2$ is the product of two cocycles* *with coefficients in T such that ξ_1 takes values in $T \cap H$, where H is a proper F-subgroup of G normalizing by T, and ξ_2 viewed as a cocycle with coefficients in G is trivial. Then ξ is equivalent to a cocycle with coefficients in a proper F-subgroup of G of the same type as H.*

Proof. Let $\xi_1 = (a_\sigma)$, $\xi_2 = (b_\sigma)$, where $\sigma \in \mathrm{Gal}\,(F^s/F)$, $a_\sigma \in T(F^s) \cap H(F^s)$ and $b_\sigma \in T(F^s)$. Since ξ_2 is trivial, there is $g \in G(F^s)$ such that $b_\sigma = g^{-1+\sigma}$ for all $\sigma \in \mathrm{Gal}\,(F^s/F)$. Then the equivalent cocycle $\xi' = (c_\sigma)$, where

$$c_\sigma = g(a_\sigma b_\sigma)g^{-\sigma} = g a_\sigma g^{-1},$$

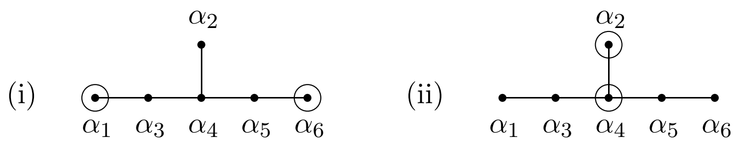
takes values in a proper F-subgroup gHg^{-1} which has the same type as H. $\square$

5.2 Type E_6: isotropic case

This case is much easier.

Lemma 5.13 *Let the twisted group $G = {}^\xi G_0$ be F-isotropic. Then it splits over F; in particular ξ is trivial.*

Proof. Assume the contrary. According to [T66] all admissible Tits' indices of type ${}^1E_6$ corresponding to isotropic groups are as follows:



(5)

In case (i) the semisimple anisotropic kernel of G is a classical group of type D_4. Since Γ is a pro-3-group, any such a group is F-split.

Consider case (ii). Applying Theorem 3.2 we obtain that ξ is equivalent to a cocycle with coefficients in $SL_3 \times SL_3$. Hence ξ is trivial and G is F-split. $\square$

5.3 Type E_7

Proposition 5.14 *There exists no F-anisotropic groups of type E_7 splitting over K.*

Proof. Assume the contrary. Let G be an F-anisotropic simple group of type E_7 splitting over K. To get a contradiction we can proceed as in case E_6. Namely, let $\mathcal{P} \subset G$ be the parabolic subgroup over K corresponding to the root α_7. Then we consider the connected component C of the intersection $\mathcal{P} \cap \tau(\mathcal{P}) \cap \tau^2(\mathcal{P})$. As in case E_6, it is easy to conclude that C is a reductive group of dimension at least 52 whose semisimple part $[C, C]$ contains an F-defined simple component C_1 of type not A_n.

Let $\mathcal{L} \subset \mathcal{P}$ be a Levi subgroup containing C_1. Its semisimple part has type E_6, hence C_1 is a group of type either ${}^3D_4, F_4$, or E_6. By a dimension argument, C_1 cannot be of type ${}^3D_4$. If C_1 is of type E_6, then C_1 is the semisimple part of $\mathcal{L}$. It follows that $C_G(C_1)$ is defined over F. But it coincides with the central torus A of $\mathcal{L}$ whose dimension is 1. Hence A is F-defined and F-isotropic being a torus of dimension 1.

Assume now that C_1 is a group of type F_4 and let us consider $C_G(C_1)$. Since it contains A, $C_G(C_1)$ is a nontrivial reductive group over F whose rank is either $1, 2$ or 3.

Let $S \subset C_G(C_1)$ be a maximal torus over F. It commutes with C_1, by construction, hence $C_1 \subset [C_G(S), C_G(S)]$.

If $\dim S = 1$, then S is F-isotropic. If $\dim S = 3$, then $C_1 = [C_G(S), C_G(S)]$ would be a standard subgroup of G of type F_4. But a root system of type E_7 does not contain a subsystem of type F_4.

Thus $\dim S = 2$ and $C_G(S)$ is a reductive group whose semisimple part $[C_G(S), C_G(S)]$ has rank 5 and contains the subgroup C_1 of type F_4. It follows that $[C_G(S), C_G(S)]$ contains another simple component over F of rank 1. But any such a group is F-isotropic. $\square$

We are now ready to complete the proof of Theorem 5.1 in the case of E_7 by reducing it to E_6. By Proposition 5.14, G is F-isotropic. Looking at Tits tables [T66] and taking into consideration the fact that Γ is a pro-3- group we obtain that the only possibility for the semisimple F-anisotropic kernel of G is to be a group of type E_6. Applying Theorem 3.2 we get that ξ is equivalent to a cocycle with coefficients in an F-split standard subgroup of G_0 of type E_6. So the result follows. $\square$

6 *The triviality of the kernel of R_G for E_6, E_7*

Theorem 6.1 *Let G_0 be a quasi-split simple simply connectedgroup of type E_6, E_7 defined over a field F of characteristic $\neq 2, 3$. Then* $\operatorname{Ker} R_{G_0} = 1$.

We split the proof into three parts considering inner forms of type E_6, outer forms of type E_6 and type E_7 separately. Let G_0 be the given quasi-split group and let $[\xi]$ be an element of $\operatorname{Ker} R_{G_0}$. Let $G = {}^{\xi}G_0$ be the corresponding twisted group. The triviality of ξ is clearly equivalent to saying that G is quasi-split over F.

6.1 Inner forms of type E_6

Our strategy is to reduce to the case where G is an F-isotropic group and then to apply Theorem 3.2 and Proposition 2.4.

6.1.1 Reduction to a pro-p-case

It is entirely based on the following theorem which is due to P. Gille [G93], [G97].

Theorem 6.2 *Let G be a simple simply connected group of type E_6 or E_7 over F. Assume that there exist finite field extensions $E_1, \ldots, E_s$ of F splitting G and such that the*

$$g.c.d.\{\, [E_1 : F], \ldots, [E_s : F] \,\} = 1.$$

Then G splits over F.

Let $\Gamma_p \subset \Gamma$ be a Sylow p-subgroup and let $F_p = (F^s)^{\Gamma_p}$ be fixed points of Γ_p. Assuming that Theorem 6.1 is proved over F_p we can find for each p a finite extension E_p/F contained in F_p and splitting G. Since the $g.c.d$ of all degrees $[E_p : F]$ is clearly 1, we obtain from Gille's theorem that G splits over F.

6.1.2 Reduction to the case $p = 2, 3$

By Theorem 3.1, we may assume that ξ takes values in an F-defined maximal torus $T \subset G_0$.

Lemma 6.3 *Any element of the group $H^1(F, T)$ has order of the form $2^n 3^m$.*

Proof. See Proposition 6.21 in [PR94], p. 375. □

Lemma 6.3 implies that in the case $p \neq 2, 3$ any cocycle from $Z^1(F, T)$ is trivial.

6.1.3 The case $p = 3$

Theorem 5.1 says that ξ is equivalent to a cocycle with coefficients in a standard simple simply connected F-subgroup of G_0 of type A_2. Then, by Theorem 2.1 and Proposition 2.4, ξ is trivial.

6.1.4 The case $p = 2$

Assume first that G be F-isotropic. According to [T66], we have two possibilities for an F-anisotropic kernel of G:

(i) an inner form of type $A_2 \times A_2$. But Γ is a pro-2-group, hence there are no anisotropic inner forms of type A_2 over F;

(ii) an inner form of type D_4. In this case, by Theorem 3.2, ξ is equivalent to a cocycle with coefficients in a standard simple simply connected F-split subgroup of G_0 of type D_4, hence it is trivial, by Propositions 2.2 and 2.4.

Let G be now F-anisotropic. Let E/F be a finite Galois extension which splits G and is minimal with this property. Since Γ is a pro-2-group, there is a chain of subfields

$$F = E_0 \subset E_1 \subset \ldots \subset E_s = E$$

such that $[E_{i+1} : E_i] = 2$ and $s \geq 1$. Since G is not split over E_{s-1} and the F-isotropic case has been already studied, G is anisotropic over that field. Thus it suffices to treat the case where G splits over a quadratic extension K/F. Then G has a maximal torus T defined over F and splitting over K (see § 4). Since G is a group of inner type, $\mathrm{Gal}\,(K/F)$ has the natural embedding into the Weyl group. We also know that the image of the nontrivial element of $\mathrm{Gal}\,(K/F)$ acts on the corresponding root system $\Sigma(G, T)$ by multiplication by -1. But the Weyl group of type E_6 does not contain -1: a contradiction.

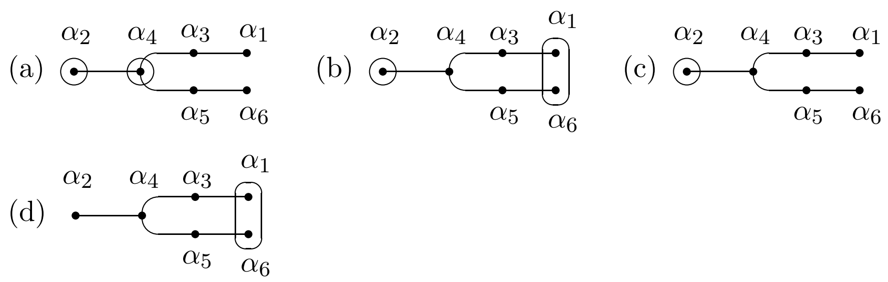
6.2 Outer forms of type E_6

Let G_0 be a quasi-split group of type E_6 and let $K = F(\sqrt{d})$ be the quadratic extension over which G_0 becomes split. Since the inner case has been already treated, we have $\mathrm{Res_K}([\xi]) = 1$, hence G splits over K.

6.2.1 Isotropic case

Proposition 6.4 *If G is F-isotropic, then $[\xi] = 1$.*

Proof. According to Tits' classification [T66] the F-index of G is one of the following:



Lemma 6.5 *The Tits index of G is not of the form* (a), (b) or (c)*.*

Proof. Let $T \subset G$ be a maximal F-torus containing a maximal F-split torus of G. We fix a basis $\Pi = \{\alpha_1, \dots, \alpha_6\}$ of $\Sigma(G, T)$ corresponding to the above pictures. According to [T66] the maximal F-split subtorus of T is the identity component of the subgroup of T defined by the following system of equations:

$$\begin{cases} \gamma(t) \;=\; \sigma^*(\gamma)(t) & \text{for all } \gamma \in \Pi \text{ and all } \sigma \in Gal(F^s/F), \\ \alpha_i(t) \;=\; 1 & \text{for all non-distinguished vertices } \alpha_i, \end{cases}$$

where $t \in T$ and σ^* denotes the $*$-action of Γ on Π (see [T66]). It follows from these equations and the above pictures that in all cases (a), (b) and (c) the maximal F-split subtorus of T contains the F-split one-dimensional subtorus $S_1 = \langle h_\beta(u) \mid u \in (F^s)^\times \rangle$ corresponding to the root β of maximal length. Then the semisimple part of the centralizer $C_G(S_1)$ is F-defined and coincides with the subgroup $G_{\Sigma_1} \subset G$ generated by roots $\Sigma_1 = \{\alpha_1, \alpha_3, \dots, \alpha_6\}$. Let $S_2 \subset G_{\Sigma_1}$ be an arbitrary maximal F-defined torus and let $S = S_1 \cdot S_2$.

Arguing as in Theorem 3.2 it is easy to see that there is an F-embedding $S \hookrightarrow G_0$ such that $[\xi] \in \operatorname{Im}[H^1(F, S) \to H^1(F, G_0)]$ and the image of S_2 lies in a standard quasi-split simple simply connected F-subgroup H of type ${}^2A_5$. Since S/S_2 is an F-split torus, any cocycle in $Z^1(F, S)$ is equivalent to a cocycle with coefficients in S_2. Thus ξ is equivalent to a cocycle with coefficients in H, hence ξ is trivial, by Propositions 2.3 and 2.4. $\square$

Lemma 6.6 *A group with the Tits index* (d) *can not split over a quadratic extension. In particular, the Tits index of G is not of the form* (d)*.*

Proof. Let H be an F-isotropic group with the Tits index of the form (d). If H splits over a quadratic extension K/F, then so is its semisimple F-anisotropic kernel L. In case (d) L is an almost simple simply connected F-anisotropic group of type ${}^2D_4$. Since L splits over a quadratic extension of the ground field, there are two possibilities.

Case I. $L \simeq \mathrm{Spin}\,(f)$, where f is an F-anisotropic quadratic form of dimension 8. Since L has type ${}^2D_4$, the discriminant of f is nontrivial. On the other hand, L is F-anisotropic and splits over K, hence f is of the form

$$f \simeq a_1(x_1^2 - dx_2^2) + a_2(x_1^3 - dx_4^2) + a_3(x_5^2 - dx_6^2) + a_4(x_7^2 - dx_8^2),$$

where $a_1, \dots, a_4 \in F^\times$. It follows that f has trivial discriminant — a contradiction.

Case II. $L \simeq \mathrm{Spin}\,(D, f)$, where D is a quaternion algebra over F and f is a skew-hermitian form over D (with respect to the standard involution on D). Let E be the function field of the Severi-Brauer variety corresponding to D. By a result of Parimala, Sridharan and Suresh [PSS99], L is still anisotropic over E and clearly has type ${}^2D_4$ over E. Then we can proceed to Case I to get a contradiction. $\square$

Lemmas 6.5 and 6.6 complete the proof of Proposition 6.4. $\square$

6.2.2 Anisotropic case

By Theorem 3.1, there is a maximal F-anisotropic torus $S \subset G_0$ splitting over K and such that

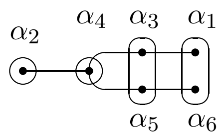
$$[\xi] \in \mathrm{Im}\,[H^1(F, S) \to H^1(F, G_0)]. \tag{6}$$

Then according to Proposition 4.14 for any maximal F-anisotropic torus of G_0 splitting over K, condition (6) still holds. We keep the notation introduced in Section 4. In particular, given a Chevalley basis of the Lie algebra of G_0 with respect to S we denote the corresponding structure constants by $\{c_\alpha,\, \alpha \in \Sigma = \Sigma(G_0, S)\}$.

Lemma 6.7 *There exists a maximal F-anisotropic torus $S \subset G_0$ splitting over K and such that the structure constants are of the form*

$$c_{\alpha_1} \equiv 1,\ c_{\alpha_2} \equiv 1,\ \ldots,\ c_{\alpha_6} \equiv 1 \pmod{N_{K/F}(K^\times)}.$$

Proof. Let $T \subset G_0$ be a centralizer of a maximal F-split torus in G_0. The Tits F-index of G_0 is of the form



(7)

Here $\{\alpha_1, \ldots, \alpha_6\}$ is a basis of $\Sigma(G_0, T)$. Let $\beta \in \Sigma(G_0, T)$ be the root of maximal length with respect to the basis $\{\alpha_1, \ldots, \alpha_6\}$. It follows from (7) that the subgroup $G_\beta \subset G_0$ corresponding to β is an F-split group of rank 1, hence $G_\beta \simeq \mathrm{SL}_2$. Let $S_1 \subset G_\beta$ be a maximal F-anisotropic torus of dimension 1 which is isomorphic to $R^{(1)}_{K/F}(G_{m,K})$.

The subgroup $H = G_{\Sigma_1} \subset G_0$ corresponding to the set $\Sigma_1 = \{\alpha_1, \alpha_3, \ldots \alpha_6\}$ is a quasi-split F-group of type ${}^2A_5$, hence it is F-isomorphic to $\mathrm{SU}\,(h)$, where

$$h = x_1 x_1^\tau - x_2 x_2^\tau + x_3 x_3^\tau - x_4 x_4^\tau + x_5 x_5^\tau - x_6 x_6^\tau. \tag{8}$$

We choose the F-anisotropic torus $S_2 \subset H = SU(h)$ consisting of all diagonal isometries of h and we let $S = S_1 \cdot S_2$. Since G_β commutes with H, S is a maximal F-anisotropic torus in G_0 splitting over K.

Let Σ be the root system of G_0 with respect to S. We may now forget about T and we work with the root system Σ related to S. In order to ease notation we denote a basis in Σ by the same letters $\{\alpha_1, \ldots, \alpha_6\}$. We choose a Chevalley basis (with respect to S) of the Lie algebra of G_0 and a basis $\{\alpha_1, \ldots, \alpha_6\}$ of Σ in such a way that its subset $\{\alpha_1, \alpha_3, \ldots, \alpha_6\}$ is a basis of the root system of $\mathrm{SU}\,(h)$ with respect to S_2. Then by Lemma 4.13,

$$c_{\alpha_1} \equiv 1,\ c_{\alpha_3} \equiv 1,\ \ldots,\ c_{\alpha_6} \equiv 1 \pmod{N_{K/F}(K^\times)}.$$

We now want to modify S (if necessary) in such a way that $c_{\alpha_2} \equiv 1 \pmod{N_{K/F}(K^\times)}$ as well.

Assume that $c_{\alpha_2} \not\equiv 1$. Consider the cocycle $\zeta = (b_\tau) \in Z^1(K/F, S_1(K))$, where $b_\tau = h_\beta(c_{\alpha_2})$ and β is the root of Σ of maximal length with respect to the ordering determined by the basis $\{\alpha_1, \ldots, \alpha_6\}$. Since $G_\beta \simeq \mathrm{SL}_2$, ζ viewed as a cocycle with coefficients in G_β is trivial.

Let $b_\tau = g^{-1+\tau}$, where $g \in G_\beta(K)$. We claim that the torus $S' = gSg^{-1}$ is as required. Indeed, by Lemma 4.9, S' is defined over F and splits over K. Since g commutes with H, Lemma 4.8 shows that the constants $c_{\alpha_1}, c_{\alpha_3}, \ldots, c_{\alpha_6}$ related to the tori S and S' coincide, hence are as required. Since $\langle \beta, \alpha_2 \rangle = 1$, Lemma 4.8 again shows that the constant c_{α_2} related to S' equals 1. $\square$

Applying the Moving Lemma 5.1.6 we want next to modify our cocycle ξ, i.e. take an equivalent one, in such a way that the new one has coefficients in a simple simply connected F-group of type D_5.

To do so, let S be the torus constructed in Lemma 6.7. Let $L \subset G_0$ be a subgroup generated by the simple roots $\alpha_2, \ldots, \alpha_6$ from the root system $\Sigma(G_0, S)$. Clearly, L is an F-defined group of type D_5 splitting over K. Since S splits over K, we have $H^1(F, S) = H^1(K/F, S(K))$. Hence ξ can be written in the form $\xi = (s_\tau)$, where

$$s_\tau = h_{\alpha_1}(u_1) \cdots h_{\alpha_6}(u_6),$$

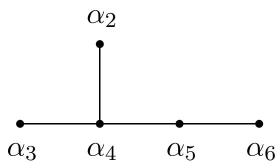
and τ is the nontrivial automorphism of K/F. It easily follows from $s_\tau \tau(s_\tau) = 1$ that $u_1, \ldots, u_6 \in F^\times$.

Since $c_{\alpha_1} \equiv 1$, we have $G_{\alpha_1} \simeq SL_2$ over F, by Lemma 4.12. Hence there is $g \in G_{\alpha_1}(K)$ such that $g^{-\tau+1} = h_{\alpha_1}(u_1)$. Consider the equivalent cocycle $\tilde{\xi} = (\widetilde{s_\tau})$, where

$$\widetilde{s_\tau} = g^\tau h_{\alpha_1}(u_1) \cdots h_{\alpha_6}(u_6) g^{-1} = g\, h_{\alpha_2}(u_2) \cdots h_{\alpha_6}(u_6)\, g^{-1}.$$

It has coefficients in $\widetilde{L} = g\, L\, g^{-1}$.

The group $\widetilde{L}$ is a simple simply connected group of type D_5 defined over F. It contains the maximal torus $\widetilde{S_2} = g\, S_2\, g^{-1}$ splitting over K. In order to stress that $\widetilde{L}$ sits inside G_0, we number simple roots in $\Sigma(\widetilde{L}, \widetilde{S_2})$ as follows.



Lemma 6.8 *The structure constants of $\widetilde{L}$ with respect to the torus $\widetilde{S_2}$ are as follows:*

$$c_{\alpha_2} \equiv c_{\alpha_4} \equiv c_{\alpha_5} \equiv c_{\alpha_6} \equiv 1 \pmod{N_{K/F}(K^\times)}, \quad c_{\alpha_3} \equiv u_1 \pmod{N_{K/F}(K^\times)};$$

in particular, $\widetilde{L}$ has F-rank at least 2.

Proof. The first statement follows from Lemma 4.8, the second one from the fact that the subgroups G_{α_2} and G_{α_5} of $\widetilde{L}$ corresponding to α_2 and α_5 split over F, by Lemma 4.12, and commutes. $\square$

Since $\widetilde{L}$ splits over the quadratic extension K/F, there are two possibilities for $\widetilde{L}$.

Lemma 6.9 *Assume that $\widetilde{L} \simeq \mathrm{Spin}\,(f)$, where f is a quadratic form over F of dimension* 10. *Then $\widetilde{L}$ is quasi-split.*

Proof. We have to exclude the possibilities for the Witt index i of f to be $i = 2, 3$.

Assume that $i = 2$. Then f is the direct sum of two hyperbolic planes and a certain F-anisotropic quadratic form of dimension 6. It follows that the dimension of a maximal F-split torus in $\widetilde{L}$ equals 2 and the semisimple part of its centralizer has type $A_3 = D_3$.

On the other hand, all maximal F-split tori in $\widetilde{L}$ are conjugate over F. Since G_{α_2} and G_{α_5} are split over F, they contain F-split tori of dimension 1, say T_2 and T_5. Then simple calculations with roots show that the semisimple part of the centralizer $C_{\widetilde{L}}(T_2 \cdot T_5)$ has type $A_1 \times A_1$ — a contradiction.

Assume that $i = 3$. Let f_{an} be the anisotropic part of f. It has dimension 4 and splits over K, in particular f_{an} has trivial discriminant. It follows that the function field E of the projective quadric $f_{an} = 0$ splits f. Hence G_0 has rank at least 5 over E which is impossible, since E does not contain K. □

Since $\widetilde{L}$ is quasi-split and $R_{G_0}([\xi]) = R_{\widetilde{L}}([\tilde{\xi}]) = 1$, Proposition 2.2 gives $[\tilde{\xi}] = 1$.

It remains to consider the case $\widetilde{L} \simeq \mathrm{Spin}\,(D, f)$, where D is a quaternion algebra over F and f is a skew-hermitian form over D (with respect to the standard involution on D). Let E be the function field of the Severi-Brauer variety of D. The extension E/F splits D and so we can reduce to the previous case if we show that the twisted group $G = {}^{\xi}G_0$ is still anisotropic over E.

Lemma 6.10 *G is anisotropic over E.*

Proof. Assume the contrary, i.e. G is E-isotropic. Then G is quasi-split over E, since the isotropic case has been already treated. Let U be the unipotent radical of a Borel subgroup $B \subset G$ over E. The twisted group ${}^{\tilde{\xi}}(\widetilde{L})$ being F-anisotropic is still anisotropic over E, by [PSS99]. Hence the intersection $U \cap {}^{\tilde{\xi}}(\widetilde{L})$ is trivial. On the other hand, we have $\dim {}^{\tilde{\xi}}(\widetilde{L}) = 45$, $\dim U = 36$, so $\dim U \cap {}^{\tilde{\xi}}(\widetilde{L})$ is at least 3. □

6.2.3 A formula for the Rost invariant

We keep the notation from the previous subsection. Using the above material one can easily produce a formula for the Rost invariant for any cocycle $\xi \in Z^1(K/F, G_0(K))$. Namely, let S be the torus from Lemma 6.7. By Proposition 4.14, we have the surjection

$$H^1(K/F, S(K)) \to H^1(K/F, G_0(K)).$$

Hence we may assume that ξ has coefficients in S.

Let $\xi = (a_\tau)$ and let $a_\tau = h_{\alpha_1}(t_1) \cdots h_{\alpha_6}(t_6)$, where $t_1, \ldots, t_6 \in F^\times$. We write ξ as the product $\xi = \xi_1 \cdot \xi_2$, where

$$\xi_1 = (h_{\alpha_1}(t_1) h_{\alpha_4}(t_4) h_{\alpha_6}(t_6)), \quad \xi_2 = (h_{\alpha_3}(t_3) h_{\alpha_2}(t_2) h_{\alpha_5}(t_5)).$$

Since, by Lemma 4.12, the subgroup of G_0 generated by the roots $\alpha_2, \alpha_3, \alpha_5$ splits over F, ξ_2 is a trivial cocycle. Then, by the Moving Lemma 5.1.6, ξ is equivalent to a cocycle with coefficients in an F-subgroup $H \subset G_0$ of type $A_1 \times A_1 \times A_1$.

According to Lemma 4.8 the three components of H correspond to the quaternion algebras $D_1 = (d, t_3)$, $D_4 = (d, t_2t_3t_5)$, $D_6 = (d, t_5)$. Then, by Proposition 2.4 and from the formula for the Rost invariant for groups of inner type A_n, we obtain that the cocycle $R_{G_0}(\xi)$ is given by

$$R_{G_0}(\xi) = (d) \cup (t_3) \cup (t_1) + (d) \cup (t_2t_3t_5) \cup (t_4) + (d) \cup (t_5) \cup (t_6).$$

6.3 Type E_7

This case is entirely similar to case E_6. By Gille's Theorem 6.2 and Lemma 6.3, we may assume that $\mathrm{Gal}\,(F^s/F)$ is a pro-p-group, where $p = 2, 3$. If $p = 3$, then in view of Theorem 5.1 ξ is equivalent to a cocycle with coefficients in a subgroup of G_0 of type A_2. Therefore ξ is trivial, by Theorem 2.1.

Let now $p = 2$. Then we may assume that G is split over a quadratic extension K/F. It is easy to see that G, and hence G_0, contains a maximal F-anisotropic torus S splitting over K. By Theorem 3.1, there is an embedding $S \hookrightarrow G_0$ such that ξ is equivalent to a cocycle with coefficients in the image of S. Arguing as in E_6 we may assume that all structure constants of S corresponding to all simple roots are 1 modulo norms $N_{K/F}(K^\times)$. After that we can modify ξ (as in Lemma 6.8) in such a way that the new cocycle lies in a simple simply connected F-subgroup H of G_0 of type E_6 with the following structure constants:

$$c_{\alpha_1} \equiv c_{\alpha_2} \equiv c_{\alpha_3} \equiv c_{\alpha_4} \equiv c_{\alpha_5} \equiv 1 \pmod{N_{K/F}(K^\times)}, \quad c_{\alpha_6} \equiv u_1 \pmod{N_{K/F}(K^\times)}.$$

It follows that F-rank of H is at least 3. Looking at the tables [T66], we see that H is either quasi-split or split over F. Hence the result follows from Proposition 2.4, since H is standard.

6.4 Type ${}^{3,6}D_4$

This case is known (see [KMRT98]). However in order to get a self-contained proof of Serre's Conjecture II for groups of exceptional types over (C_2)–fields (except E_8) let us show how this case follows from the above.

Let G_0 be a simple simply connected quasi-split trialitarian group over F. Denote the minimal extension of F over which G_0 becomes split by L and let $\Gamma = \mathrm{Gal}\,(L/F)$. If G_0 is a group of type ${}^3D_4$, then $[L : F] = 3$ and $\Gamma \simeq \mathbb{Z}/3$; otherwise we have $[L : F] = 6$ and $\Gamma \simeq S_3$. We start with the following

Proposition 6.11 *Let $\xi \in Z^1(F, G_0)$ be a cocycle such that the twisted group $G = {}^\xi G_0$ is quasi-split over a quadratic extension K/F. Assume that K and L are linearly disjoint over F. Then ξ is equivalent to a cocycle with coefficients in a standard simple simply connected F-subgroup of G_0 of type A_1.*

Proof. Let $\sigma \in \Gamma$ be an arbitrary element of order 3. We fix a subfield $P \subseteq L$ of degree 3 over F. If $[L : F] = 3$, the field P coincides with L. If $[L : F] = 6$, let λ be the non-trivial automorphism L/P. We have clearly $\lambda\sigma\lambda^{-1} = \sigma^2$. Let τ be the nontrivial automorphism of K/F. Since K and L are linearly disjoint over F, we can extend the automorphisms

$$\sigma,\, \lambda \in \mathrm{Gal}\,(L/F), \quad \tau \in \mathrm{Gal}\,(K/F)$$

in a natural way to the extension E/F, where $E = K \cdot L$. For simplicity we denote these extensions by the same letters σ, λ, τ.

Let $B \subset G$ be a Borel subgroup over K such that $S = B \cap \tau(B)$ is a maximal torus. S is split over E. Let $\Sigma = \Sigma(G, S)$ and let $\Pi = \{\alpha_1, \ldots, \alpha_4\} \subset \Sigma$ be the basis corresponding to the Borel subgroup B. The action of Γ on root subgroups was described in [ChT99] and is given by the formulas

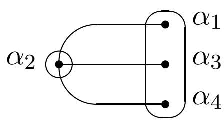
$$\begin{aligned}
&\sigma[x_{\pm\alpha_1}(u)] = x_{\pm\alpha_3}[\sigma(u)], && \sigma[x_{\pm\alpha_3}(u)] = x_{\pm\alpha_4}[\sigma(u)],\\
&\sigma[x_{\pm\alpha_4}(u)] = x_{\pm\alpha_1}[\sigma(u)], && \sigma[x_{\pm\alpha_2}(u)] = x_{\pm\alpha_2}[\sigma(u)],\\
&\lambda[x_{\pm\alpha_1}(u)] = x_{\pm\alpha_1}[\lambda(u)], && \lambda[x_{\pm\alpha_2}(u)] = x_{\pm\alpha_2}[\lambda(u)],\\
&\lambda[x_{\pm\alpha_3}(u)] = x_{\pm\alpha_4}[\lambda(u)], && \lambda[x_{\pm\alpha_4}(u)] = x_{\pm\alpha_3}[\lambda(u)],\\
&\tau([x_{\alpha_i}(u)] = x_{-\alpha_i}(\tau(u)).
\end{aligned} \tag{9}$$

Formulas (9) show that $S \simeq S_1 \times S_2$, where

$$S_1 = S \cap G_{\alpha_2} = \langle\, h_{\alpha_2}(u) \,\rangle \simeq R^{(1)}_{K/F}(G_{m,K}),$$

$$S_2 = S \cap G_{\{\alpha_1,\alpha_3,\alpha_4\}} = \langle\, h_{\alpha_1}(u_1)h_{\alpha_3}(u_3)h_{\alpha_4}(u_4) \,\rangle \simeq R_{P/F}\,[R^{(1)}_{P\cdot K/P}(G_{m,P\cdot K})].$$

The rest of the proof is the same as in Section 5.1.3. Namely, we construct the following embedding $\psi : S \hookrightarrow G_0$. Let $T \subset G_0$ be the centralizer of a maximal F-split torus of G_0. The Tits index of G_0 over F is of the form:



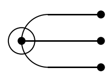
(10)

This picture shows that the subgroup $H_1 \subset G_0$ (respectively H_2) generated by α_2 (respectively $\alpha_1, \alpha_3, \alpha_4$) from the root system $\Sigma(G_0, T)$ is isomorphic to $SL_{2,F}$ (respectively $R_{P/F}(SL_{2,P})$). Hence there are natural embeddings $S_1 \hookrightarrow H_1$, $S_2 \hookrightarrow H_2$ which can be extended to $\psi : S \hookrightarrow G_0$. Arguing as in Proposition 5.10 we obtain that ξ is equivalent to a cocycle with coefficients in $\psi(S)$. Then it can be written as a product of two cocycles $\xi = \xi_1 \cdot \xi_2$ with coefficients in $\psi(S_1)$ and $\psi(S_2)$ respectively. Since ξ_2 has coefficients in H_2 which has trivial Galois cohomology, the Moving Lemma 5.1.6 completes the proof. □

Theorem 6.12 *If $\xi \in Z^1(F, G_0)$ is a cocycle such that $R_{G_0}([\xi]) = 1$, then ξ is trivial.*

Proof. The triviality of ξ is equivalent to saying that the twisted group $G = {}^{\xi}G_0$ is quasi-split over F. As usual we distinguish two cases: isotropic and anisotropic.

Let first G be F-isotropic. We claim that then G is quasi-split over F. Assume the contrary. Then the F-index of G is of the form



(11)

Let S_1 be a maximal F-split torus in G. It follows from the picture that the semisimple part of the centralizer $C_G(S_1)$ coincides with the subgroup $G_{\Sigma_2} \subset G$ generated by the non-distinguished roots $\Sigma_2 = \{\alpha_1, \alpha_3, \alpha_4\}$. Let $S_2 \subset G_{\Sigma_2}$ be an arbitrary maximal F-defined torus and let $S = S_1 \cdot S_2$.

Arguing as in Theorem 3.2 we obtain that there is an F-embedding $S \hookrightarrow G_0$ such that $[\xi] \in \mathrm{Im}\,[H^1(F,S) \to H^1(F,G_0)]$ and the image of S_2 lies in a standard quasi-split simple simply connected F-subgroup $H \subset G_0$ of type $A_1 \times A_1 \times A_1$. Since S/S_2 is a split torus over F, any cocycle in $Z^1(F,S)$ is equivalent to a cocycle with coefficients in S_2. It follows that ξ is equivalent to a cocycle with coefficients in H and H has trivial Galois cohomology.

Let G be F-anisotropic. Consider first the case $[L:F]=3$. Since $\mathrm{Ker}\, R^L_{G_0} = 1$, we obtain that $[\xi] \in H^1(L/F, G_0(L))$. Then the argument on p. 372–373 in [PR94] shows that ξ up to equivalence lies in a standard simple simply connected subgroup of G_0 of inner type A_2. Hence ξ is trivial, by Theorem 2.1 and Proposition 2.4.

The last case is $[L:F]=6$. Let $K_1 = F(\sqrt{d})$ be the quadratic extension contained in L. Since we have already proved that $\mathrm{Ker}\, R^{K_1}_{G_0} = 1$, we obtain that $\xi \in Z^1(K_1/F, G_0(K_1))$, in particular G is quasi-split over K_1. Then we can easily find as above (see also [PR94], p. 354) an F-subgroup H of G of type A_1. Let K/F be a quadratic extension splitting H and linearly disjoint with L. Then G is isotropic over K and hence quasi-split over K, for the isotropic case has been already treated. Since L and K are linearly disjoint, Proposition 6.11 and Theorem 2.1 show that ξ is trivial. □

7 *Serre's Conjecture* II *and the Hasse principle Conjecture* II

Conjecture II (Serre [S94]) Let F be a perfect field with $cd\,(F) \le 2$ and let G be a simply connected semisimple linear algebraic group over F. Then $H^1(F,G)=1$.

The Hasse Principle Conjecture II (Colliot-Thélène, Scheiderer [CT96, Sch96]) Let F be a field with $vcd\,(F) \le 2$ and let G be a simply connected semisimple linear algebraic group over F. Then the canonical map

$$\theta : \; H^1(F,G) \longrightarrow \prod_{\xi \in \Omega_F} H^1(F_\xi, G)$$

induced by the restriction maps has trivial kernel. Here Ω_F denotes the set of all orderings of F and F_ξ is a real closure of F at the ordering ξ.

Theorem 7.1 *Let G_0 be a quasi-split simple simply connected group over a perfect field F which is of type ${}^{3,6}D_4, E_6, E_7$. Assume that $cd_p\,(F) \le 2$, where $p = 2,3$. Then $H^1(F,G_0) = 1$.*

Proof. Let $\zeta \in Z^1(F,G_0)$. Since $cd_p\,(F) \le 2$, $p=2,3$, we get $R_{G_0}([\zeta]) = 1$. It follows then from Theorem 6.1 that $[\zeta]=1$. □

Theorem 7.2 *Let G_0 be a quasi-split simple simply connected algebraic group over F which is of type ${}^{3,6}D_4, E_6, E_7$. Assume that $vcd\,(F) \le 2$. Then*

$$\theta : \; H^1(F,G_0) \longrightarrow \prod_{\xi \in \Omega_F} H^1(F_\xi, G_0)$$

has trivial kernel.

Proof. Let $\zeta \in Z^1(F, G_0)$ be a locally trivial cocycle. Let $K = F(\sqrt{-1})$. By Theorem 7.1, the restriction of ζ at K is trivial. It follows that $R_{G_0}([\zeta])$ has coefficients in $\mathbb{Z}/2$. Hence the result follows from Theorem 6.1 and the following theorem which is due to Arason.

Theorem 7.3 *The Hasse principle holds for $H^3(F, \mathbb{Z}/2)$.*

Proof. Let $\eta \in Z^3(F, \mathbb{Z}/2)$ be a locally trivial cocycle. Then by Arason's theorem [A75], Satz 3, there is an integer r such that $\eta \cup (-1)^r = 0$. On the other hand from the exact sequence

$$H^i(K, \mathbb{Z}/2) \xrightarrow{cor} H^i(F, \mathbb{Z}/2) \xrightarrow{\cup(-1)} H^{i+1}(F, \mathbb{Z}/2) \xrightarrow{res} H^{i+1}(K, \mathbb{Z}/2)$$

([Ar75], Corollary 4.6) and from the equalities

$$H^i(K, \mathbb{Z}/2) = H^{i+1}(K, \mathbb{Z}/2) = 0, \quad i \geq 3$$

we conclude that the product $\cup(-1)$ is an isomorphism. Therefore, $\eta = 0$. $\square$

8 (C_2)-*fields*

A field F has (C_2)-property if every homogeneous equation $f(x_1, \ldots, x_n) = 0$ of degree d with coefficients in F has a nontrivial solution in F^n if $n > d^2$. Property (C_2) implies $cd(F) \leq 2$, but the converse is not true in general case. The main property of (C_2)-fields we are going to use is

Theorem 8.1 ([Art82]) *Every central simple algebra A over a (C_2)-field F of exponent p has index p if $p = 2, 3$.*

Theorem 8.2 *Let G be a simple simply connected algebraic group of type ${}^{3,6}D_4, E_6, E_7$ defined over a (C_2)-field F. Then $H^1(F, G) = 1$.*

Proof. Denote a simple simply connected (resp. adjoint) F-quasi-split group of the same type as G by G_0 (resp. $\overline{G}_0$). In the case ${}^{3,6}D_4$, as in 6.4, let L/F be the minimal Galois extension over which G_0 becomes split and P/F a cubic extension contained in L. We have the natural map $\varphi : H^1(F, \overline{G}_0) \longrightarrow H^2(F, Z)$, where Z is the center of G_0. Let $\xi \in Z^1(F, \overline{G}_0)$ be such that $G = {}^{\xi}G_0$. Then there is the natural bijection (see [S94])

$$\varphi^{-1}(\varphi([\xi])) \longrightarrow H^1(F, G)/\sim,$$

where $\sim$ is the equivalence relation given by multiplication on elements from $H^1(F, Z)$. It follows that we need only to show that the fiber $\varphi^{-1}(\varphi([\xi]))$ consists of one element, namely $[\xi]$, and any cocycle with coefficients in the centre of G is trivial, viewed as a cocycle in G.

8.1 Type ${}^{3,6}D_4$

Let $[\xi_1] \in \varphi^{-1}(\varphi([\xi]))$ and let $G_1 = {}^{\xi_1}G_0$ be the corresponding twisted group. It is known that

$$H^2(F, Z) \simeq \mathrm{Ker}\,[\,{}_2\mathrm{Br}\,P \longrightarrow {}_2\mathrm{Br}F\,].$$

Since exponent of an algebra over P coincides with its index, $\varphi([\xi])$ can be represented by a quaternion algebra over P. Then, by Proposition 43.9 in [KMRT98], there is a quadratic extension K/F which kills $\varphi([\xi]) = \varphi([\xi_1])$. This implies, by Theorem 7.1, that G and G_1 are quasi-split over K. Arguing as in Proposition 6.11 (see also [PR94], p. 354) we can easily see that each of G and G_1 contains a simple simply connected subgroup of outer type A_2 splitting over K. Since $cd_2(F) \leq 2$, any such subgroup is isotropic over F. Hence both groups G and G_1 are F-isotropic.

If one of G, G_1 is quasi-split over F, there is nothing to prove. Otherwise, both of them have the same Tits index (11). Denote by H_0 the subgroup in G_0 generated by the root subgroups corresponding to the roots α_1, α_3, α_4 from diagram (10). The group H_0 is a semisimple simply connected group of type $A_1 \times A_1 \times A_1$ containing the center Z. Let $\overline{H}_0 \subset \overline{G}_0$ be its image in the adjoint group. Taking into consideration the diagram (11) and arguing as in Theorem 3.2 we get immediately that up to equivalence the cocycles ξ and ξ_1 lies in $Z^1(F, \overline{H}_0)$. Hence $[\xi] = [\xi_1]$, since for groups of classical types Conjecture II holds by [BP95].

To show that

$$\mathrm{Im}\,[\,H^1(F,Z) \longrightarrow H^1(F,G)\,] = 1$$

it suffices to note that the center Z lies in the semisimple F-anisotropic kernel of G which has type $A_1 \times A_1 \times A_1$ (see diagram (11)) and hence has trivial Galois cohomology.

The above argument shows that we can apply the same proof for the other types E_6, E_7 if we find an F-split torus $S \subset G_0$ satisfying the following conditions:

(a) $[\xi]$, $[\xi_1] \in \mathrm{Im}\,[\,H^1(F, C_{\overline{G}_0}(\overline{S})) \longrightarrow H^1(F, \overline{G}_0)\,]$, *where* $\overline{S}$ *is the image of* S *in* $\overline{G}_0$,

(b) $H_0 = [\,C_{G_0}(S), C_{G_0}(S)\,]$ *is a semisimple simply connected group of classical type containing the center* Z *of* G_0,

(c) the centralizer $C_{G_0}(S)$ *is an almost direct product of* S *and* H_0.

8.2 Type $^1E_6$

We have $Z \simeq \mu_3$, hence there is a cubic cyclic extension E/F killing $\varphi([\xi]) = \varphi([\xi_1])$.

Lemma 8.3 *G and G_1 are F-isotropic.*

Proof. Assume the contrary. Let C_1 be a subgroup constructed in Lemma 5.3. It has type D_4, hence is F-isotropic by the argument above — a contradiction. $\square$

All admissible F-isotropic Tits indices are given by diagrams (5). Since G, G_1 are split over a cubic extension E/F we conclude that the only case which can occur is represented by diagram (5), index (ii). Then one can easily see that the torus S_1 constructed in Theorem 3.2 satisfies properties (a), (b) and (c).

8.3 Type $^2E_6$

Let K/F be the quadratic extension over which G_0 becomes a group of inner type and let τ be the nontrivial automorphism K/F.

Lemma 8.4 *G and G_1 are F-isotropic.*

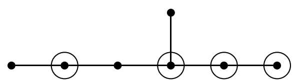
Proof. Assume the contrary. We have already proved that G is K-isotropic. If it splits over K, then it contains an F-defined subgroup of type A_2 splitting over the quadratic extension K/F. Since F has (C_2)-property, this subgroup is F-isotropic.

Thus G is not K-split, hence its K-Tits index is of the form (ii) in diagram (5) (note that the index (i) can not occur since its anisotropic kernel is a classical group of type D_4 and any such group is F-isotropic over a (C_2)-field). Let P be a minimal parabolic subgroup of G over K in generic position and let C be the connected component of $P \cap \tau(P)$. Since, by our assumption, G is F-anisotropic, C is a reductive F-group. By dimension argument, C_K is a Levi subgroup of P. This implies that $[C, C]$ is a semisimple K-anisotropic kernel of G. It follows then from picture (ii) in diagram (5) that the centraliser $C_G([C, C])$ is an F-defined subgroup of G of type A_2 splitting over K. But any such group is F-isotropic. $\square$

All admissible F-isotropic Tits indices of type ${}^2E_6$ are given by the diagrams in Proposition 6.4. Since the K-Tits indices of G, G_1 are of the form (ii) in (5), we conclude that over F they are of the form either (a) or (c) from the diagrams in Proposition 6.4. In both cases the subgroups in G, G_1 corresponding to the root of maximal length are isomorphic to SL_2 over F, hence contains a 1-dimensional split torus S. The rest of the proof is the same as for inner forms of type E_6.

8.4 Type E_7

As above one can easily see that both G, G_1 are F-isotropic. Looking at the Tits tables [T66] and taking into the consideration the fact (which has been already proved above) that all simple groups of type not A_n are F-isotropic we obtain that G, G_1 have the same Tits indices of the form



The rest of the proof is the same as for inner forms of type E_6. Thus we complete the proof of Theorem 8.2. $\square$

Remark 8.5 Note that under the proof of Theorem 8.2 we have showed that any simple group of type ${}^{3,6}D_4, E_6, E_7$ is isotropic and also described all admissible Tits indices of such groups.

References

[A75] J. Arason, Primideale im graduierten Wittring und im mod 2 Cohomologiering, Math. Z. **145** (1975), 139–143.

[Ar75] J. Arason, Cohomologische Invarianten quadratischer Formen, J. Algebra **36** (1975), 448–491.

[Art82] M. Artin, Brauer–Severi Varieties (Notes by A. Verschoren), Lecture Notes in Math.**917** (1982), 194–210.

[BP95] E. Bayer-Fluckiger, R. Parimala, Galois cohomology of the classical groups over fields of cohomological dimension ≤ 2, Invent. Math. **122** (1995), no. 2, 195–229.

[BP98] E. Bayer-Fluckiger, R. Parimala, Classical groups and the Hasse principle, Ann. of Math. **147** (1998), 1–43.

[Bourb68] N. Bourbaki, Groupes et Algèbres de Lie, Chapitres 4,5 et 6, Hermann, Paris 1968.

[Ch89] V. Chernousov, On the Hasse principle for groups of type E_8, Dokl. Akad. Nauk SSSR, **306** (1989), N 25, 1059-1063.

[Cher89] V. Chernousov, On projective simplicity of groups of rational points of some algebraic groups over algebraic number fields, Izvestiya Akad. Nauk SSSR, Ser. Math., **53** (1989), no 2, 398–410.

[Ch94] V. Chernousov, Remark on (mod 5)–Serre's invariant for groups of type E_8, Math. Zametki, **56** (1994), N 1, 116-121.

[Ch98] V. Chernousov, Letter to P. Gille, November, 1998.

[ChT99] V. Chernousov, L. Timoshenko, On the group of R-equivalence classes of semisimple groups over arithmetic fields, Algebra and Analis, **11** (1999), no 6, 191-221.

[Ch00] V. Chernousov, Letter to Garibaldi, October 2000.

[CT96] J–L. Colliot-Thélène, Groupes linéaires sur les corps de fonctions de courbes réelles, J. reine angew. Math. **474** (1996), 139–167.

[EKLV98] H. Esnault, B. Kahn, M. Levine, E. Viehweg, The Arason invariant and mod 2 algebraic cycles, J. Amer. Math. Soc. 11 (1998), no. 1, 73–118.

[Fer69] J. C. Ferrar, Lie algebras of type ${}^1E_6$, J. of Algebra 13 (1969), 57–72.

[Gar01] R. S. Garibaldi, The Rost invariant has trivial kernel for quasi-split groups of low rank, To appear in Commentarii Mathematici Helvetici.

[G93] P. Gille, R-équivalence et principe de norme en cohomologie galoisienne, C. R. Acad. Sci. Paris, Sér. I Math., **316** (1993), no. 4, 315–320.

[G97] P. Gille, La R-équivalence sur les groupes algébriques réductifs définis sur un corps global, Inst. Hautes Études Sci. Publ. Math., No. 86 (1997), 199–235 (1998).

[G00] P. Gille, Invariants cohomologiques de Rost en caractéristique positive, K-Theory, **21** (2000), no. 1, 57–100.

[G01] P. Gille, Cohomologie galoisienne des groupes quasi-déployés sur des corps de dimension cohomologique ≤ 2, Composito Math. **125** (2001), no. 3, 283–325.

[H65] G. Harder, Über die Galoiskohomologie halbeinfacher Matrizengruppen I, Math. Z. **90** (1965), no 5, 404–424.

[H66] G. Harder, Über die Galoiskohomologie halbeinfacher Matrizengruppen II, Math. Z. **92** (1966), no 5, 396–415.

[Hum75] J. Humphreys, Linear Algebraic Groups, Springer-Verlag 1975.

[KMRT98] M. Knus, A. Merkurjev, M. Rost, J–P. Tignol, The Book of Involutions, **44** Colloquium publications: American Mathematical Society 1998.

[L73] T.-Y. Lam, The Algebraic Theory of Quadratic Forms, Benjamin, MA, 1973.

[MS82] A. Merkurjev, A. Suslin, K-cohomology of Severi-Brauer varieties and the norm residue homomorphism, Izv. Akad. Nauk SSSR **46** (1982), 1011–1046.

[M01] A. Merkurjev, Unramified cohomology of classifying varieties for classical simply connected groups, Preprint 2001.

[PSS99] R. Parimala, R. Sridharan, V. Suresh, Hermitian analogue of a theorem of Springer, Preprint 1999.

[PR94] V. Platonov, A. Rapinchuk, Algebraic Groups and Number Theory, Academic Press 1994.

[R] M. Rost, Cohomological invariants, in preparation.

[S94] J.–P. Serre, Cohomologie Galoisienne, Springer, 1994.

[S93] J.–P. Serre, Cohomologie galoisienne: progrès et problèmes, Sém. Bourbaki 1993–1994, exposé 783.

[Sch96] C. Scheiderer, Hasse principles and approximation theorems for homogeneous spaces over fields of virtual cohomological dimension one, Invent. math. **125** (1996), 307–365.

[SGA3] Séminaire de Géométrie algébrique de l'I.H.E.S., 1963–1964, Schémas en groupes, dirigé par M. Demazure et A. Grothendieck, Lecture Notes in Math. 151–153, Springer (1970).

[St65] R. Steinberg, Regular elements of semisimple groups, Publ. Math. I.H.E.S. **25**, 281–312 (1965).

[St67] R. Steinberg, Lectures on Chevalley Groups, Yale University 1967.

[T66] J. Tits, Classification of algebraic semisimple groups, In Algebraic Groups and discontinuous Subgroups, (eds. A.Borel and G.D.Mostow), Proc. Symp. Pure Math. **9**, 33–62 (1966).

[V98] V. Voskresenskii, Algebraic Groups and their Birational Invariants, Translated from Russian by Boris E. Kunyavskii, Amer. Math. Soc., Providence, RI, 1998