Available at www.MATHEMATICSWEB.ORG
POWERED BY SCIENCE DIRECT

Journal of Algebra 266 (2003) 87–101

JOURNAL OF Algebra

www.elsevier.com/locate/jalgebra

Orthogonal groups containing a given maximal torus

Rosali Brusamarello,[a] Pascale Chuard-Koulmann,[b] and Jorge Morales [c,*]

[a] *Departamento de Matemática, Universidade Estadual de Maringá, Maringá, PR, 87020-900, Brazil*
[b] *Institut de Mathématiques, Université de Neuchâtel, Rue Emile Argand 11, CH-2007 Neuchâtel, Switzerland*
[c] *Department of Mathematics, Louisiana State University, Baton Rouge, LA 70808, USA*

Received 10 January 2002

Communicated by Eva Bayer-Fluckiger

Abstract

Let k be a field of characteristic different from 2 and let $\mathbf{T}$ be a fixed k-torus of dimension n. In this paper we study faithful k-representations $\rho:\mathbf{T}\to\mathbf{SO}(A,\sigma)$, where (A,σ) is a central simple algebra of degree $2n$ with orthogonal involution σ. Note that in this case $\rho(\mathbf{T})$ is a maximal torus in $\mathbf{SO}(A,\sigma)$. We are interested in describing the pairs (A,σ) for which there is such a representation. We compute invariants for these algebras (discriminant and Clifford algebra), which are sufficient to determine their isomorphism class when $I^3(k)=0$ by a theorem of Lewis and Tignol. The first part of the paper is devoted to the case where A is split over k and an application to a theorem of Feit on orthogonal groups over $\mathbf{Q}$ is given.

1. Introduction

Let k be a field of characteristic different from 2. Let V be a vector space of dimension $2n$ over k and let $\mathbf{T}$ be an algebraic torus of dimension n defined over k. Let $\rho:\mathbf{T}\to\mathbf{GL}(V)$ be a faithful self-dual representation defined over k.

* Corresponding author.
E-mail addresses: brusama@uem.br (R. Brusamarello), pascale.chuard@maths.unine.ch (P. Chuard-Koulmann), morales@math.lsu.edu (J. Morales).

0021-8693/03/$ – see front matter
doi:10.1016/S0021-8693(03)00287-4

We study nondegenerate quadratic forms on V that are $\mathbf{T}$-invariant under the representation ρ. These forms will be called $\mathbf{T}$-*forms* throughout the paper. Note that if q is such a form on V, then, for dimension reasons, $\rho(\mathbf{T})$ is a maximal torus in $\mathbf{SO}(V,q)$, hence the title of the paper.

The set W of weights of the representation ρ is naturally a $\mathrm{Gal}(k_{\mathrm{sep}}/k)$-set and carries the involution $\chi \mapsto \chi^{-1}$, since ρ is self-dual, so it determines a unique étale algebra E over k and an involution σ on E. We show that all $\mathbf{T}$-forms on V are equivariantly isomorphic to certain scaled trace forms on E (see Proposition 3.9). This allows us to compute the discriminant and the Hasse invariant of $\mathbf{T}$-forms in terms of invariants attached to the étale algebra E (see Corollary 4.2 and Theorem 4.3).

In the case where $I^3(k) = 0$, where $I(k)$ is the fundamental ideal of the Witt ring of k, we are able to classify the orthogonal groups that admit $\mathbf{T}$ as a maximal torus. If n is odd, and under some condition on E, there is only one orthogonal group containing $\mathbf{T}$ (see Corollary 4.8). As an application, we give a generalization of a theorem of Feit [3] on orthogonal groups over $\mathbf{Q}$ (Corollary 4.9).

In Section 5, we consider more generally representations $\mathbf{T} \to \mathbf{SO}(A,\sigma)$, where A is a central simple algebra of degree $2n$ over k and σ is an orthogonal involution on A. As in the case where A is split, we fix a set of weights W and ask for the isomorphism classes of algebras with involution (A,σ) for which there is a representation $\mathbf{T} \to \mathbf{SO}(A,\sigma)$ with set of weights W. We compute the discriminant and Clifford algebra of such pairs (A,σ) in terms of invariants attached to W. These computations lead to a complete classification when $I^3(k) = 0$, using a theorem of Lewis and Tignol [7, Proposition 6].

We are indebted to the referee for her/his careful reading and many useful and detailed comments.

2. Notation and definitions

Let k be a field. Throughout this paper, we shall denote by k_{sep} a separable closure of k and by Γ_k the Galois group $\mathrm{Gal}(k_{\mathrm{sep}}/k)$. If V is a vector space or an algebra over k, we shall denote by V_{sep} the tensor product $V \otimes_k k_{\mathrm{sep}}$.

Some algebraic groups

We shall denote by $\mathbf{G_m}$ the multiplicative group over k and by $\boldsymbol{\mu}_\ell$ the subgroup of $\mathbf{G_m}$ of ℓth roots of unity. If B is a k-algebra, we will denote by $\mathbf{GL_1}(B)$ the multiplicative group of B *as an algebraic group over* k. The general linear group of a vector space V over k will be denoted by $\mathbf{GL}(V)$.

If (B,σ) is an algebra over k equipped with an involution, the *unitary group* of (B,σ) is the group scheme over k given by

$$\mathbf{U}(B,\sigma)(R) = \bigl\{u \in B \otimes_k R\colon\ \sigma(u)u = 1\bigr\}$$

for any commutative k-algebra R.

In the particular case where (A, σ) is a central simple algebra over k equipped with an orthogonal involution, the unitary group of (A, σ) as above will be called the *orthogonal group* of (A, σ) and will be denoted by $\mathbf{O}(A, \sigma)$ instead of $\mathbf{U}(A, \sigma)$.

We shall denote by $\mathbf{GO}(A, \sigma)$ the group of similitudes of (A, σ) (see [5, Section 23]). The natural homomorphism $\mathrm{Int}: \mathbf{GO}(A, \sigma) \to \mathbf{Aut}(A, \sigma)$ given by $\mathrm{Int}(u)(x) = uxu^{-1}$ is an epimorphism and we have an exact sequence

$$1 \to \mathbf{G_m} \to \mathbf{GO}(A, \sigma) \xrightarrow{\mathrm{Int}} \mathbf{Aut}(A, \sigma) \to 1. \tag{1}$$

The quotient group $\mathbf{PGO}(A, \sigma) := \mathbf{GO}(A, \sigma)/\mathbf{G_m}$ is called the *projective orthogonal group* of (A, σ) and will be always identified with $\mathbf{Aut}(A, \sigma)$ via the above exact sequence.

We shall denote by $\mathbf{SO}(A, \sigma)$ the subgroup of $\mathbf{O}(A, \sigma)$ of elements of reduced norm 1 and by $\mathbf{PSO}(A, \sigma)$ the image of $\mathbf{SO}(A, \sigma)$ in $\mathbf{PGO}(A, \sigma)$. In the case where A has even degree over k, $\mathbf{PSO}(A, \sigma)$ has index 2 in $\mathbf{PGO}(A, \sigma)$.

In the particular case where $A = \mathrm{End}_k(V)$ and σ is the adjoint involution of a quadratic form q on V, we use the more standard notation $\mathbf{O}(V, q)$, $\mathbf{GO}(V, q)$, $\mathbf{SO}(V, q)$, $\mathbf{PSO}(V, q)$, $\mathbf{PGO}(V, q)$ for the groups above.

Galois cohomology

For an algebraic group $\mathbf{G}$ defined over k, we shall denote by $H^i(k, \mathbf{G})$ the profinite cohomology set $H^i(\Gamma_k, \mathbf{G}(k_{\mathrm{sep}}))$ as defined in [5, Chapter 7, Sections 28–29] ($i \leqslant 1$ if $\mathbf{G}$ is not abelian).

3. Maximal tori and étale algebras with involution

In this section, $\mathbf{T}$ denotes a fixed k-torus of dimension n and V a vector space of dimension $2n$ over k. For general facts about representations of algebraic tori and weight space decomposition, see [12, Chapter 2, Section 5], [4, Chapter VI, Section 16], or [1, Section 5].

Lemma 3.1. *Let $\rho: \mathbf{T} \to \mathbf{GL}(V)$ be a faithful self-dual representation. Then all weights of ρ are nonzero and are simple.*

Proof. Let $X(\mathbf{T}) := \mathrm{Hom}(\mathbf{T}, \mathbf{G_m})$. Recall that an element $\chi \in X(\mathbf{T})$ is a *weight* of ρ if there exists a nonzero vector $v \in V_{\mathrm{sep}}$ such that $\rho(t)v = \chi(t)v$ for all $t \in \mathbf{T}(k_{\mathrm{sep}})$. Let $W \subset X(\mathbf{T})$ be the set of nonzero weights of ρ. On the one hand, by faithfulness, W generates $X(\mathbf{T})$, and by self-duality we have $-W = W$. Hence one-half of the elements of W suffice to generate $X(\mathbf{T})$, so $|W| \geqslant 2n$. On the other hand, since $\dim_k(V) = 2n$, we also have $|W| \leqslant 2n$. Hence $|W| = 2n$ and the lemma follows. □

If (E, σ) is an algebra with involution, we shall denote by $\mathrm{Sym}(E, \sigma)$ the subspace of symmetric elements of E, i.e., $\mathrm{Sym}(E, \sigma) = \{x \in E\colon \sigma(x) = x\}$.

Lemma 3.2. *Let E be an étale algebra of dimension $2n$ over k equipped with an involution σ such that* $\dim \mathrm{Sym}(E,\sigma) = n$. *Then the unitary group $\mathbf{U}(E,\sigma)$ is an algebraic torus of dimension n.*

Proof. Let $e_1, e_2, \ldots, e_{2n}$ be the primitive idempotents of E_{sep}. Since $\dim \mathrm{Sym}(E,\sigma) = n$, none of the e_i is fixed by σ, so we can renumber them so that $\sigma(e_i) = e_{n+i}$ $(n = 1, \ldots, n)$. Then the elements of $\mathbf{U}(E,\sigma)(k_{\mathrm{sep}})$ are of the form $(t_1, \ldots, t_n, t_1^{-1}, \ldots, t_n^{-1})$ with $t_i \in k_{\mathrm{sep}}^\times$. Thus $\mathbf{U}(E,\sigma) \cong \mathbf{G_m} \times \cdots \times \mathbf{G_m}$ (n times) over k_{sep}. □

Let now q be a nondegenerate quadratic form on V and let σ be the adjoint involution of q.

Proposition 3.3. *Let $\mathbf{T} \subset \mathbf{SO}(V,q)$ be a maximal k-torus. Then there is a unique étale algebra $E \subset \mathrm{End}(V)$ stable by σ such that $\mathbf{T} = \mathbf{U}(E,\sigma)$. Moreover, E satisfies* $\dim E = 2n$ *and* $\dim \mathrm{Sym}(E,\sigma) = n$.

Conversely, for any étale algebra $E \subset \mathrm{End}(V)$ stable under σ and satisfying the dimension conditions above, the unitary group $\mathbf{U}(E,\sigma)$ is a maximal k-torus of $\mathbf{SO}(V,q)$.

Proof. Let $E = \mathrm{End}_{\mathbf{T}}(V) = \{f \in \mathrm{End}(V)\colon\ ft = tf \text{ for all } t \in \mathbf{T}(k_{\mathrm{sep}})\}$. It is clear that E is stable under σ. We shall show first that E is an étale algebra. Let $W \subset X(\mathbf{T})$ be the set of weights of $\mathbf{T}$ acting on V. For $\chi \in W$, we denote by V_χ the corresponding weight subspace of V and we consider the canonical decomposition $V_{\mathrm{sep}} = \bigoplus_{\chi \in W} V_\chi$. Notice that E_{sep} is the subalgebra of $\mathrm{End}(V_{\mathrm{sep}})$ that preserves the subspaces V_χ, thus $E_{\mathrm{sep}} = \prod_\chi \mathrm{End}(V_\chi)$. Since the subspaces V_χ are one-dimensional by Lemma 3.1, $\mathrm{End}(V_\chi) = k_{\mathrm{sep}}$ and therefore E is étale of dimension $2n$.

Let e_χ be the idempotent of E_{sep} corresponding to $\mathrm{End}(V_\chi)$ and let β be the symmetric bilinear form associated to q. For $t \in \mathbf{T}(k_{\mathrm{sep}})$ and $v, w \in V$, we have $\beta(t\sigma(e_\chi)v, w) = \beta(v, t^{-1}e_\chi w) = \beta(v, \chi^{-1}(t)e_\chi w) = \beta(\chi^{-1}(t)\sigma(e_\chi)v, w)$; so, by the nondegeneracy of β, we have $\sigma(e_\chi)v \in V_{\chi^{-1}}$ for all $v \in V$. It follows that $\sigma(e_\chi) = e_{\chi^{-1}}$, which proves in particular that $\dim \mathrm{Sym}(E,\sigma) = n$.

If $E' \subset \mathrm{End}(V)$ is another étale algebra with $\mathbf{U}(E',\sigma) = \mathbf{T}$, then, on the one hand, $E' \subset E$, since E' commutes with $\mathbf{T}$, and on the other hand $n = \dim \mathbf{U}(E',\sigma) \leqslant \frac{1}{2}\dim E'$, so $E' = E$ and uniqueness follows.

Conversely, if we start out with an étale subalgebra $E \subset \mathrm{End}(V)$ of dimension $2n$ preserved by σ and with $\dim \mathrm{Sym}(E,\sigma) = n$, then $\mathbf{U}(E,\sigma)$ is a torus of dimension n by Lemma 3.2 and is obviously contained in $\mathbf{O}(V,q)$. By connectedness, we have in fact $\mathbf{U}(E,\sigma) \subset \mathbf{SO}(V,q)$. □

It will be useful for later in the paper to have a description of the étale algebra $\mathrm{End}_{\mathbf{T}}(V)$ associated with $\mathbf{T}$ in terms of Galois sets. The Galois group Γ_k acts on the weight set W and we can consider the associated étale algebra[1] $E' := \mathrm{Map}_{\Gamma_k}(W, k_{\mathrm{sep}})$ of dimension $2n$ over k. The involution $\chi \mapsto \chi^{-1}$ on W induces an involution on E' that we shall denote by σ'.

[1] For the general correspondence between Γ_k-sets and étale algebras over k, see [5, Section 18].

Proposition 3.4. *There is a canonical isomorphism $\varphi : (E', \sigma') \xrightarrow{\sim} (\mathrm{End}_{\mathbf{T}}(V), \sigma)$ of k-algebras with involution. The map φ induces an isomorphism of k-algebraic tori $\bar{\varphi} : \mathbf{U}(E', \sigma') \xrightarrow{\sim} \mathbf{T}$ and the following diagram commutes:*

$$\begin{array}{ccc} E'_{\mathrm{sep}} & \overset{\overset{\varphi}{\cong}}{\longrightarrow} & \mathrm{End}_{\mathbf{T}}(V_{\mathrm{sep}}) \\ \cup & & \cup \\ \mathbf{U}\big(E', \sigma'\big)(k_{\mathrm{sep}}) & \overset{\overset{\bar{\varphi}}{\cong}}{\longrightarrow} & \mathbf{T}(k_{\mathrm{sep}}) \end{array}$$

Proof. For $v \in V_{\mathrm{sep}}$ we shall write $v = \sum_{\chi \in W} v_\chi$, where v_χ lies in the eigenspace V_χ corresponding to the weight χ. We define $\varphi : E'_{\mathrm{sep}} = \mathrm{Map}(W, k_{\mathrm{sep}}) \to \mathrm{End}_{\mathbf{T}}(V_{\mathrm{sep}})$ by

$$\varphi(f)v = \sum_{\chi \in W} f(\chi) v_\chi.$$

One verifies readily that φ commutes with the action of Γ_k and is an isomorphism. Indeed, the primitive idempotents of E'_{sep} are the maps e'_χ defined by $e'_\chi(\psi) = \delta_{\chi\psi}$ (Kronecker delta) for $\chi, \psi \in W$, and one sees immediately that $\varphi(e'_\chi) = e_\chi$, where e_χ is the idempotent of $\mathrm{End}_{\mathbf{T}}(V_{\mathrm{sep}})$ corresponding to V_χ. From the proof of Proposition 3.3, we have $\sigma(e_\chi) = e_{\chi^{-1}} = \varphi(e'_{\chi^{-1}}) = \varphi(\sigma'(e'_\chi))$, which proves that φ is an isomorphism of algebras with involution. □

Proposition 3.3 will allow us to compute the cohomology group $H^1(k, \mathbf{T})$ for a maximal torus $\mathbf{T} \subset \mathbf{SO}(V, q)$.

Keeping the notation of Proposition 3.3, we let $F = \mathrm{Sym}(E, \sigma)$ and define the norm map $N_{E/F} : \mathbf{GL_1}(E) \to \mathbf{GL_1}(F)$ by $x \mapsto x\sigma(x)$.

Corollary 3.5. $H^1(k, \mathbf{T}) = F^\times / N_{E/F}(E^\times)$.

Proof. By Proposition 3.3, we have $\mathbf{T} = \mathbf{U}(E, \sigma)$, so $\mathbf{T}$ fits into the exact sequence of algebraic groups

$$1 \to \mathbf{T} \to \mathbf{GL_1}(E) \xrightarrow{N_{E/F}} \mathbf{GL_1}(F) \to 1.$$

Taking cohomology we have

$$E^\times \xrightarrow{N_{E/F}} F^\times \xrightarrow{\partial} H^1(k, \mathbf{T}) \to H^1\big(k, \mathbf{GL_1}(E)\big).$$

By Hilbert's Theorem 90, we have $H^1(k, \mathbf{GL_1}(E)) = 0$. Hence $H^1(k, \mathbf{T}) = F^\times / N_{E/F}(E^\times)$. □

We shall now consider triples (V, ρ, q), where V is a vector space of dimension $2n$ over k, ρ is a faithful representation $\mathbf{T} \to \mathbf{GL}(V)$ defined over k, and q is a nondegenerate $\mathbf{T}$-form on V.

Two such triples (V, ρ, q) and (V', ρ', q') are said to be *isomorphic* if there is a k-linear map $\phi : V \to V'$ satisfying $\phi\rho(m) = \rho'(m)\phi$ for all $m \in \mathbf{T}$ and $q'\phi = q$.

An obvious invariant of the triple (V, ρ, q) is the character of the representation (V, ρ), or, equivalently, the set of weights W of ρ. If (V, ρ, q) and (V', ρ', q') are triples with the same set of weights, then they are isomorphic over k_{sep}. This can be seen as follows: Let $W = \{\chi_1, \dots, \chi_n, \chi_1^{-1}, \dots, \chi_n^{-1}\}$ be the set of weights of ρ and let V_{χ_i} denote the corresponding weight spaces. Then we have an orthogonal decomposition

$$V_{\mathrm{sep}} = (V_{\chi_1} \oplus V_{\chi_1^{-1}}) \perp \cdots \perp (V_{\chi_n} \oplus V_{\chi_n^{-1}}),$$

where each $V_{\chi_i} \oplus V_{\chi_i^{-1}}$ is a hyperbolic plane.

Hence, by standard descent theory, the triples (V', ρ', q') with given weight set are classified, up to isomorphism, by $H^1(k, \mathbf{Aut}(V, \rho, q))$, where $\mathbf{Aut}(V, \rho, q)$ denotes the automorphism group of (V, ρ, q) as an algebraic group over k.

Proposition 3.6. *Let (V, ρ, q) be a triple as above and let $E = \mathrm{End}_{\mathbf{T}}(V)$. Then $\mathbf{Aut}(V, \rho, q) = \mathbf{U}(E, \sigma) = \rho(\mathbf{T})$.*

Proof. By the very definition of $\mathbf{Aut}(V, \rho, q)$, we have

$$\mathbf{Aut}(V, \rho, q) = \mathbf{GL_1}(E) \cap \mathbf{SO}(V, q) = \mathbf{U}(E, \sigma).$$

The equality $\rho(\mathbf{T}) = \mathbf{U}(E, \sigma)$ follows from Proposition 3.3. □

Corollary 3.7. *The set of isomorphism classes of triples (V, ρ, q) with fixed set of weights W is in one-to-one correspondence with the elements of the group $H^1(k, \mathbf{T}) = F^\times / N_{E/F}(E^\times)$.*

Proof. This is an immediate consequence of Proposition 3.6 and Corollary 3.5. □

Remark 3.8. In fact, the correspondence of Corollary 3.7 can be made quite explicit as follows: Let β be the bilinear form on V such that $\beta(x, x) = q(x)$. For $a \in F^\times$ define $q_a(x) = \beta(ax, x)$. Then the correspondence is given by $a \mapsto (V, \rho, q_a)$.

For $a \in F^\times$ we define $B_a(x, y) = \mathrm{Tr}_{E/k}(ax\sigma(y))$ and we let $Q_a(x) = B_a(x, x) = \mathrm{Tr}_{E/k}(ax\sigma(x))$ be the associated quadratic form. Note that the group $\mathbf{U}(E, \sigma)$ acts by isometries on Q_a, and with the equality $\rho(\mathbf{T}) = \mathbf{U}(E, \sigma)$ given by Proposition 3.6, Q_a becomes a $\mathbf{T}$-form via ρ. For simplicity, we let $Q = Q_1$.

Proposition 3.9. $(V, \rho, q) \cong (E, \rho, Q_a)$ *for some $a \in F^\times$ uniquely determined modulo $N_{E/F}(E^\times)$.*

Proof. Since E and V have the same dimension and E acts faithfully on E, V is free of rank one over E, so we can assume that $V = E$. Let β be the symmetric bilinear form associated with q. The adjoint maps $\mathrm{ad}(\beta), \mathrm{ad}(B_1) : E \to E^*$ are isomorphisms, so $\mathrm{ad}(B_1)^{-1}\mathrm{ad}(\beta)$, being an E-automorphism of E, must be multiplication by a unit of $a \in E$. Hence $\mathrm{ad}(\beta)(x) = \mathrm{ad}(B_1)(ax) = \mathrm{ad}(B_a)(x)$. It follows that $\beta = B_a$. By the symmetry of β, we must have $a \in F$. The uniqueness of a modulo $N_{E/F}(E^{\times})$ follows from Corollary 3.7. □

4. Invariants of T-forms

Let V be a vector space of dimension $2n$ over k and let $\mathbf{T} \subset \mathbf{GL}(V)$ be a fixed algebraic torus of dimension n. We shall assume that V is self-dual as a representation of $\mathbf{T}$, so V can afford $\mathbf{T}$-invariant quadratic forms. In this section we shall investigate the low-dimensional invariants of these forms.

Proposition 4.1. *Let q be a nondegenerate quadratic form on V with $\mathbf{T} \subset \mathbf{SO}(V, q)$. The isomorphism classes of quadratic forms q' on V such that $\mathbf{T} \subset \mathbf{SO}(q')$ are in one-to-one correspondence with the elements in the image of the map $H^1(k, \mathbf{T}) \xrightarrow{\iota_*} H^1(k, \mathbf{SO}(V, q))$ induced by the natural inclusion $\mathbf{T} \xhookrightarrow{\iota} \mathbf{SO}(V, q)$. In particular, all the $\mathbf{T}$-forms have the same determinant.*

Proof. We already know by Corollary 3.7 that the triples (V, ι, q') are classified by $H^1(k, \mathbf{T})$. It is clear that the natural map $H^1(k, \mathbf{T}) \xrightarrow{\iota_*} H^1(k, \mathbf{SO}(V, q))$ sends the class of a triple (V, ι, q') to the class of q'. □

Corollary 4.2. *Let E and F be as in Section* 3 *and write $E = F[t]/(t^2 - d)$ with $d \in F^{\times}$. Then all $\mathbf{T}$-forms q on V have determinant $N_{F/k}(-d)$.*

Proof. By Proposition 3.9, we can assume $V = E$ and $q = Q_1$, since all the $\mathbf{T}$-forms have the same determinant. Let $x \in E$ and write $x = r + ts$ with $r, s \in F$. Then $x\sigma x = r^2 - ds^2$ and $Q_1(x) = \mathrm{Tr}_{E/k}(x\sigma(x)) = 2\mathrm{Tr}_{F/k}(r^2) + 2\mathrm{Tr}_{F/k}(-ds^2)$. Hence

$$\det Q_1 = 2^n \delta_{F/k} \cdot 2^n N_{F/k}(-d)\delta_{F/k} \equiv N_{F/k}(-d) \pmod{k^{\times 2}},$$

where $\delta_{F/k}$ is the discriminant of F/k. □

The next step is to determine the Hasse invariant of the $\mathbf{T}$-forms as above. For this, we consider the étale algebra E of the previous section and identify $\mathbf{T}$ with $\mathbf{U}(E, \sigma)$. We can assume, without loss of generality that $V = E$ and $q = Q$.

Theorem 4.3. *Let $a \in F^{\times}$ and $E = F[t]/(t^2 - d)$ with $d \in F^{\times}$. Then*

$$h(Q_a) = h(Q) + \mathrm{Cor}_{F/k}(a, d), \tag{2}$$

where h denotes the Hasse invariant and $\mathrm{Cor}_{F/k} : H^2(k, \mathbf{GL_1}(F)) \to H^2(k, \mathbf{G_m})$ is the corestriction map, that is, the map induced by the norm $N_{F/k} : \mathbf{GL_1}(F) \to \mathbf{G_m}$.

As the referee has kindly pointed out, one can obtain a complete formula for $h(Q_a)$ combining (2) with Serre's formula [10, Théorème 1] for the Hasse invariant of the trace form. Even though Theorem 4.3 is sufficient for our purposes, we work out below the details of this relation.

Let $\mathfrak{S}_{2n}$ be the symmetric group in $2n$ letters, identified with the group of permutations of the set of primitive idempotents of E_{sep}. Let $\varphi_E : \Gamma_k \to \mathfrak{S}_{2n}$ be the homomorphism defined by the action of Γ_k on this set. Let $s_{2n} \in H^2(\mathfrak{S}_{2n}, \mathbb{Z}/2\mathbb{Z})$ be the canonical class defined in [10, 1.5]. We denote by $\delta_{E/k}$ the discriminants of E/k.

Theorem 4.4. *With the notation above, we have*

$$\begin{aligned} h(Q_a) = {} & \varphi_E^*(s_{2n}) + \big(\delta_{E/K}, (-1)^{n-1}2\big) + (\delta_{F/k}, -1) + \frac{n(n-1)}{2}(-1,-1) \\ & + \mathrm{Cor}_{F/k}(a, d). \end{aligned}$$

Proof. We first relate $h(Q)$ to the Hasse invariant of the usual trace form $q_{E/k}(x) = \mathbf{tr}_{E/k}(x^2)$ using an argument similar to one used by D.W. Lewis in [6, Theorem 2].

Let q^0 be the restriction of $q_{E/K}$ to F and let q^1 be the restriction of $q_{E/K}$ to the subspace of antisymmetric elements $\{x \in E\colon\ \sigma(x) = -x\}$. Then $q_{E/K} = q^0 \perp q^1$ and $Q = q^0 \perp (-q^1)$. Hence

$$\delta_{E/k} = \det q_{E/k} = \det\big(q^0\big)\det\big(q^1\big) = (-1)^n \det Q \quad \text{and} \quad \det\big(q^0\big) = 2^n \delta_{F/k}.$$

We have $Q \perp q_{E/K} \cong q^0 \perp q^0 \perp H$, where H is a hyperbolic form of rank $2n$, so applying the formula for the Hasse invariant of an orthogonal sum [9, 12.6] to both sides of this equality, we get, after some manipulation:

$$h(Q) = h(q_{E/K}) + (n-1)(\delta_{E/K}, -1) + (\delta_{F/k}, -1) + \frac{n(n-1)}{2}(-1,-1). \tag{3}$$

We obtain the desired expression for $h(Q_a)$ by putting together (2), (3), and Serre's formula $h(q_{E/K}) = \varphi_E^*(s_{2n}) + (\delta_{E/k}, 2)$ [10, Théorème 1]. $\square$

In order to prove Theorem 4.3 we need some preliminaries. Consider the exact sequence

$$0 \to \mathbf{GL_1}(F) \to \mathbf{GL_1}(E) \xrightarrow{p} \mathbf{T} \to 0,$$

with $p(u) = u\sigma(u)^{-1}$. Note that p is surjective by dimension reasons. Denote by $\mathbf{M}_{F/k}$ (respectively $\mathbf{M}_{E/k}$) the kernel of the norm map $N_{F/k} : \mathbf{GL_1}(F) \to \mathbf{G_m}$ (respectively $N_{E/k} : \mathbf{GL_1}(E) \to \mathbf{G_m}$). We have the following commutative diagram with exact rows and columns

$$\begin{tikzcd}
 & & 0 \arrow[d] & 0 \arrow[d] & & \\
 & 0 \arrow[r] & \mathbf{M}_{F/k} \arrow[r] \arrow[d] & \mathbf{M}_{E/k} \arrow[r, "f"] \arrow[d] & \widetilde{\mathbf{T}} \arrow[r] \arrow[d] & 0 \\
 & 0 \arrow[r] & \mathbf{GL_1}(F) \arrow[r] \arrow[d, "N_{F/k}"] & \mathbf{GL_1}(E) \arrow[r, "p"] \arrow[d, "N_{E/k}"] & \mathbf{T} \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \boldsymbol{\mu}_2 \arrow[r] & \mathbf{G_m} \arrow[r, "2"] \arrow[d] & \mathbf{G_m} \arrow[r] \arrow[d] & 0 & \\
 & & 0 & 0 & &
\end{tikzcd} \tag{4}$$

where $\widetilde{\mathbf{T}} := \mathbf{M}_{E/k}/\mathbf{M}_{F/k}$ and $f : \mathbf{M}_{E/k} \to \widetilde{\mathbf{T}}$ is the canonical projection. By the Snake lemma, we get an exact sequence

$$0 \to \boldsymbol{\mu}_2 \to \widetilde{\mathbf{T}} \to \mathbf{T} \to 0, \tag{5}$$

which shows that $\widetilde{\mathbf{T}}$ is a two-fold cover of $\mathbf{T}$.

Lemma 4.5. *There exists a map $\tilde{i} : \widetilde{\mathbf{T}} \to \mathbf{Spin}(Q)$ such that the following diagram commutes*

$$\begin{tikzcd}
\mathbf{M}_{E/k} \arrow[r, "f"] \arrow[d, "j"'] & \widetilde{\mathbf{T}} \arrow[r, "\tilde{i}"] \arrow[d] & \mathbf{Spin}(Q) \arrow[d, "\pi"] \\
\mathbf{GL_1}(E) \arrow[r, "p"] & \mathbf{T} \arrow[r, "i"] & \mathbf{SO}(Q).
\end{tikzcd}$$

Proof. Since $\mathbf{T}$ is connected, if a lifting $\tilde{i}$ exists, it is unique and hence it is defined over k. Thus it is enough to show the existence of $\tilde{i}$ over the separable closure k_{sep}. Let $\{e_1, \dots, e_n, f_1, \dots, f_n\}$ be the set of primitive idempotents of E_{sep}, numbered so that $\sigma(e_i) = f_i$. We shall first define a map $\varphi : \mathbf{M}_{E/k} \to \mathbf{Spin}(Q)$ and see that it factors through $\widetilde{\mathbf{T}}$.

We denote by $\mathrm{Cliff}(Q)$ the Clifford algebra of Q and by $\mathrm{Cliff}^+(Q)$ its even subalgebra. The canonical involution on $\mathrm{Cliff}(Q)$ will be denoted by $*$.

Define $\eta_i = \frac{1}{2} e_i f_i$ in $\mathrm{Cliff}^+(Q)$. One verifies easily from the definition of the Clifford algebra that the η_i satisfy the following relations:

(i) $\eta_i^2 = \eta_i$,
(ii) $\eta_i \eta_i^* = 0$ and $\eta_i + \eta_i^* = 1$,
(iii) the elements $\eta_1, \eta_2, \dots, \eta_n, \eta_1^*, \eta_2^*, \dots, \eta_n^*$ commute with each other.

Let $x \in \mathbf{M}_{E/k}$ and write $x = \sum_{i=1}^{n}(x_i e_i + y_i f_i)$ with $x_1 \cdots x_n y_1 \cdots y_n = 1$. Define

$$\varphi(x) = \prod_{i=1}^{n}\bigl(x_i \eta_i + y_i \eta_i^*\bigr)$$

in $\mathrm{Cliff}^+(Q)$. It follows from the properties (i)–(iii) above that φ is a homomorphism.

We also verify readily the relations $e_i\eta_j = \eta_j e_i$, $f_i\eta_j = \eta_j f_i$ for $i \neq j$, and $e_i\eta_i = 0$, $\eta_i e_i = e_i$, $f_i\eta_i = f_i$, $\eta_i f_i = 0$, and the relations obtained from these by applying the canonical involution $*$: $\eta_j^* e_i = e_i\eta_j^*$, $\eta_j^* f_i = f_i\eta_j^*$ for $i \neq j$, and $\eta_i^* e_i = 0$, $e_i\eta_i^* = e_i$, $\eta_i^* f_i = f_i$, $f_i\eta_i^* = 0$. Using all these relations, we have:

$$\begin{cases} \varphi(x)e_i\varphi(x)^{-1} = x_i y_i^{-1} e_i, \\ \varphi(x) f_i \varphi(x)^{-1} = y_i x_i^{-1} f_i \end{cases} \quad \text{and} \quad \varphi(x)\varphi(x)^* = \prod_{i=1}^{n} x_i y_i. \tag{6}$$

Hence $\varphi(x)E_{\mathrm{sep}}\varphi(x)^{-1} \subset E_{\mathrm{sep}}$ and $\varphi(x)\varphi(x)^* = 1$, so $\varphi(x) \in \mathbf{Spin}(Q)$.

If $x \in \mathbf{M}_{F/k}$, we have $x = \sum_{i=1}^{n} x_i(e_i + f_i)$ with $\prod_{i=1}^{n} x_i = 1$, so $\varphi(x) = \prod_{i=1}^{n} x_i(\eta_i + \eta_i^*) = 1$. Hence φ factors through $\widetilde{\mathbf{T}}$. We call $\tilde{i}$ the induced map $\widetilde{\mathbf{T}} \to \mathbf{Spin}(Q)$. $\square$

Now we are ready to prove Theorem 4.3.

Proof of Theorem 4.3. From Lemma 4.5 we get the following commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \boldsymbol{\mu}_2 & \longrightarrow & \widetilde{\mathbf{T}} & \longrightarrow & \mathbf{T} & \longrightarrow & 0 \\ & & \| & & \big\downarrow \tilde{i} & & \big\downarrow i & & \\ 0 & \longrightarrow & \boldsymbol{\mu}_2 & \longrightarrow & \mathbf{Spin}(Q) & \longrightarrow & \mathbf{SO}(Q) & \longrightarrow & 0. \end{array}$$

Taking cohomology we have

$$\begin{array}{ccc} H^1(k, \mathbf{T}) & \xrightarrow{\partial_{\mathbf{T}}} & H^2(k, \boldsymbol{\mu}_2) \\ \big\downarrow i_* & & \| \\ H^1\bigl(k, \mathbf{SO}(Q)\bigr) & \xrightarrow{\partial_1} & H^2(k, \boldsymbol{\mu}_2). \end{array}$$

By Springer's interpretation of the coboundary map [11, Formula 4.7], we have $\partial_1(Q_a) = h(Q_a) - h(Q)$. Thus, by the commutativity of the diagram, $\partial_{\mathbf{T}}(a) = h(Q_a) - h(Q) \in H^2(k, \boldsymbol{\mu}_2)$.

Now we take cohomology in (4), so the diagram

$$\begin{tikzcd} 0 \arrow[r] & H^1(k,\mathbf{T}) \arrow[r, "\partial'"] \arrow[d, "\partial_{\mathbf{T}}"] & H^2\big(k,\mathbf{GL_1}(F)\big) \arrow[r] \arrow[d, "\mathrm{Cor}_{F/k}"] & H^2\big(k,\mathbf{GL_1}(E)\big) \arrow[d, "\mathrm{Cor}_{E/k}"] \\ 0 \arrow[r] & H^2(k,\boldsymbol{\mu}_2) \arrow[r] & H^2(k,\mathbf{G_m}) \arrow[r, "2"] & H^2(k,\mathbf{G_m}) \end{tikzcd} \tag{7}$$

commutes. Identifying $H^1(k,\mathbf{T})$ with $F^\times/N_{E/F}(E^\times)$ we have $\partial'(a) = (a,d) \in H^2(k,\mathbf{GL_1}(F))$, where (a,d) is the cup product of the classes of a and d in $H^1(k,\boldsymbol{\mu}_{2,F}) = F^\times/F^{\times 2}$. From the commutativity of the diagram, which follows from the commutativity of (4), we have $h(Q_a) - h(Q) = \mathrm{Cor}_{F/k}(a,d)$. □

Corollary 4.6. *If $I^3(k) = 0$ (that is, the quadratic forms over k are classified by discriminant and Hasse invariant), then Q_a is k-isomorphic to Q_b if and only if $\mathrm{Cor}_{F/k}(a,d) = \mathrm{Cor}_{F/k}(b,d)$.*

Corollary 4.7. *If $I^3(k) = 0$ then the similarity classes of quadratic forms on V whose orthogonal group admits $\mathbf{T}$ as a maximal torus are in one-to-one correspondence with the elements of the group*

$$\frac{\{\mathrm{Cor}_{F/k}(a,d)\colon\ a \in F^\times\}}{\{(\lambda, N_{F/k}(d))\colon\ \lambda \in k^\times\}}.$$

This correspondence is given by $Q_a \mapsto \mathrm{Cor}_{F/k}(a,d)$.

Proof. Observe that for $\lambda \in k^\times$ we have $\mathrm{Cor}_{F/k}(\lambda,d) = (\lambda, N_{F/k}(d))$. Thus, if

$$\mathrm{Cor}_{F/k}(a,d) = \mathrm{Cor}_{F/k}(b,d) + \big(\lambda, N_{F/k}(d)\big)$$

for some $\lambda \in k^\times$, then $\mathrm{Cor}_{F/k}(a,d) = \mathrm{Cor}_{F/k}(\lambda b,d)$, which, by Corollary 4.6, implies $Q_a \cong Q_{\lambda b} = \lambda Q_b$. □

Corollary 4.8. *If $I^3(k) = 0$, n is odd and $d \in k^\times(F^\times)^2$, then all $\mathbf{T}$-forms are k-similar to Q. Consequently, there is only one orthogonal group of rank n, up to isomorphisms, containing $\mathbf{T}$ as a maximal torus.*

Proof. We may assume without loss of generality that $d \in k^\times$. For $a \in F^\times$, we have $\mathrm{Cor}_{F/k}(a,d) = (N_{F/k}(a), d) = (N_{F/k}(a), N_{F/k}(d))$, the last equality using the fact that n is odd. Hence the group of Corollary 4.7 is trivial. □

Corollaries 4.6–4.8 can be easily restated in the more general situation where $I^3(k)$ is torsion-free, since in this case, by Pfister's local-global principle [9, Chapter 3, Theorem 6.2], quadratic forms over k are classified by discriminant, Hasse invariant and signatures. We shall only give a version of Corollary 4.8 in this situation.

Corollary 4.9. *If $I^3(k)_{\mathrm{tors}} = 0$, n is odd, $d \in k^\times$, and Q is positive-definite, then all positive-definite* $\mathbf{T}$*-forms are k-similar to Q. Consequently, the orthogonal groups of such forms are all in the same k-isomorphism class.*

Corollary 4.9 is in fact a generalization of the following theorem of Feit [3] (see also [8]) for positive-definite quadratic forms over $\mathbf{Q}$.

Proposition 4.10 (Feit, [3]). *Let p be a prime number congruent to* 3 *modulo* 4. *Let q and q' be positive-definite quadratic forms over $\mathbf{Q}$ of rank $p - 1$. If both q and q' admit a rational autometry of order p, then they are similar, and consequently they have isomorphic orthogonal groups.*

Proof. Let $E = \mathbf{Q}(\zeta)$, where ζ is a primitive pth root of unity. Let τ be complex conjugation and let $\mathbf{T} = \mathbf{U}(E, \tau)$. Note that if $t \in \mathbf{SO}(V, q)(\mathbf{Q})$ is an element of order p, there is a unique representation $\mathbf{T} \to \mathbf{SO}(V, q)$ with $\zeta \mapsto t$, so q becomes a $\mathbf{T}$-form. Since E is an abelian extension of $\mathbf{Q}$, and $[F : \mathbf{Q}] = n = (p - 1)/2$ is odd, we have $E = F[t]/(t^2 - d)$ with $d \in \mathbf{Q}^\times$. We conclude by Corollary 4.9. □

5. Algebras with orthogonal involution

In this section, we generalize the results of the previous section to central simple algebras with orthogonal involution.

As before, $\mathbf{T}$ denotes an algebraic k-torus of dimension n and we consider faithful k-representations $\rho : \mathbf{T} \to \mathbf{SO}(A, \sigma)$, where A is a central simple algebra of degree $2n$ equipped with an orthogonal involution σ. The main question we shall deal with is to describe, for fixed $\mathbf{T}$, the isomorphism classes of algebras with involution (A, σ) for which there is such a representation.

We fix $\mathbf{T}$ and a set of weights $W \subset X(\mathbf{T})$ generating $X(\mathbf{T})$ with $|W| = 2n$, stable under both the action of Γ_k and the involution $\chi \mapsto \chi^{-1}$. This is equivalent to fixing an étale algebra with involution (E, τ) of dimension $2n$ and an isomorphism $\mathbf{T} \cong \mathbf{U}(E, \tau)$. We shall study the isomorphism classes of algebras with orthogonal involution (A, σ) such that there is a representation $\rho : \mathbf{T} \to \mathbf{SO}(A, \sigma)$ with weight system W. As in the case when A is split, E is identified with the elements of A that commute with $\rho(\mathbf{T})$ and with this identification we have $\rho(\mathbf{T}) = \mathbf{U}(E, \tau)$ as in Proposition 3.3. Studying such representations is equivalent to studying the embeddings of $(E, \tau) \hookrightarrow (A, \sigma)$ as algebras with involution.

We first have the existence problem, which is discussed in [2] in the more general context of Frobenius algebras.

Proposition 5.1 (see [2, Proposition 5.7]). *Let (E, τ) be as above and let A be a central simple algebra with $\dim_k(A) = \dim_k(E)^2$. There is an orthogonal involution σ on A and an embedding $(E, \tau) \hookrightarrow (A, \sigma)$ as algebras with involution if and only if $A \cong A^{\mathrm{op}}$ and A splits over $E/\mathfrak{m}$ for all maximal ideals $\mathfrak{m}$ of E.*

The existence question having been addressed, we fix a central simple algebra A satisfying the conditions of Proposition 5.1 and an embedding $E \hookrightarrow A$ and we describe the conjugacy classes of involutions on A that extend the involution τ on E. Following the notation of the previous section, we denote by F the subalgebra of E of points fixed under τ and we let $\mathbf{T} = \mathbf{U}(E, \tau)$. We also write $E = F[t]/(t^2 - d)$ and $\delta = N_{F/k}(d)$.

Lemma 5.2. *Let σ be a fixed orthogonal involution on A extending τ. Then for all $a \in F^\times$, the map $\sigma_a := \operatorname{Int}(a)\sigma$ is an orthogonal involution extending τ. All orthogonal involutions on A that extend τ are of the form σ_a for some $a \in F^\times$.*

Proof. An easy application of Skolem–Noether shows that all k-involutions on A are of the form $\sigma_a = \operatorname{Int}(a)\sigma$, with $a \in A^\times$ and $\sigma(a) = \pm a$. Since $\sigma_a|_E = \sigma|_E = \tau$, we have that $a \in Z_A(E) = E$, and the fact that σ_a is orthogonal implies that $\tau(a) = a$. □

Let σ be a fixed orthogonal involution on A extending τ. Let $C(A, \sigma)$ be its Clifford algebra (see [5, Chapter II, 8B] for the definition) and let $Z = Z(C(A, \sigma))$. It is known that Z is an étale quadratic extension of k (see [5, Chapter II, Theorem 8.10]).

Recall that the cohomology set $H^1(k, \mathbf{PSO}(A, \sigma))$ classifies triples (A', σ', ϕ'), where A' is a central simple algebra over k of degree $2n$, σ' is an orthogonal involution on A' and $\phi' : Z \to Z(C(A', \sigma'))$ is a k-isomorphism (see [5, Chapter VII, 29.F]). We shall denote by $[A', \sigma', \phi']$ the element of $H^1(k, \mathbf{PSO}(A, \sigma))$ that corresponds to the isomorphism class of (A', σ', ϕ'). The triple $[A, \sigma, \mathrm{id}_Z]$ corresponds to the trivial class in $H^1(k, \mathbf{PSO}(A, \sigma))$.

Once an isomorphism $\phi' : Z \to Z(C(A', \sigma'))$ has been chosen, one of the two possible choices, the Clifford algebra of (A', σ') becomes a Z-algebra, which will be denoted by $C(A', \sigma', \phi')$.

We shall be interested in the triples (A', σ', ϕ') that arise from the image of the natural map $j_* : H^1(k, \mathbf{T}) \to H^1(k, \mathbf{PSO}(A, \sigma))$ induced by the composite map $\mathbf{T} \xrightarrow{\text{incl.}} \mathbf{SO}(A, \sigma) \xrightarrow{\text{proj.}} \mathbf{PSO}(A, \sigma)$.

Using the identification $H^1(k, \mathbf{T}) = F^\times / N_{E/F}(E^\times)$ of Corollary 3.5, the elements of $\operatorname{Im}(j_*)$ are, by Lemma 5.2, of the form

$$j_*(a) = [A, \sigma_a, \phi_a] \in H^1\bigl(k, \mathbf{PSO}(A, \sigma)\bigr)$$

for $a \in F^\times / N_{E/F}(E^\times)$. The isomorphism $\phi_a : Z \to Z(C(A, \sigma_a))$ can be described explicitly as follows: Let $u \in E_{\mathrm{sep}}^\times$ be such that $u\sigma(u) = a$. Then $\operatorname{Int}(u) : (A_{\mathrm{sep}}, \sigma) \to (A_{\mathrm{sep}}, \sigma_a)$ is an isomorphism and induces an isomorphism $\operatorname{Int}(u)_* : C(A, \sigma)_{\mathrm{sep}} \to C(A, \sigma_a)_{\mathrm{sep}}$. We define $\phi_a := \operatorname{Int}(u)_*|_{Z_{\mathrm{sep}}}$. It is easy to verify that ϕ_a is defined over k and is independent of the choice of u.

We can now state the main result of this section:

Proposition 5.3. *For $a \in F^\times / N_{E/F}(E^\times)$, the equality*

$$\bigl[C(A, \sigma_a, \phi_a)\bigr] = \bigl[C(A, \sigma, \mathrm{id}_Z)\bigr] + \operatorname{Res}_{Z/k} \operatorname{Cor}_{F/k}(a, d)$$

holds in $\operatorname{Br}(Z) = H^2(k, \mathbf{GL_1}(Z))$.

Proof. Let $\mathbf{Spin}(A,\sigma)$ be the universal cover of $\mathbf{SO}(A,\sigma)$ and let $C = \ker[\mathbf{Spin}(A,\sigma) \to \mathbf{PSO}(A,\sigma)]$. It is known that $C = \boldsymbol{\mu}_{4[Z]}$ if n is odd, and $C = R_{Z/k}(\boldsymbol{\mu}_{2,Z})$ if n is even (see [5, Chapter VII, 31.A]). In any case, $C \subset \mathbf{GL_1}(Z)$, and we have a natural map $H^2(k,C) \to H^2(k,\mathbf{GL_1}(Z))$. Notice that $H^2(k,\mathbf{GL_1}(Z)) = H^2(Z,\mathbf{G_m}) = \mathrm{Br}(Z)$ by the Faddeev–Shapiro lemma [5, Lemma 29.6].

From the exact sequence $1 \to C \to \mathbf{Spin}(A,\sigma) \to \mathbf{PSO}(A,\sigma) \to 1$, we get a connecting homomorphism $\partial : H^1(k,\mathbf{PSO}(A,\sigma)) \to H^2(k,C)$. Let ∂' be the composite map

$$H^1\big(k,\mathbf{PSO}(A,\sigma)\big) \xrightarrow{\partial} H^2(k,C) \to \mathrm{Br}(Z).$$

On the one hand, it follows from the Tits class computations in [5, Chapter VII, Example 31.11] that for $[A',\sigma',\phi'] \in H^1(k,\mathbf{PSO}(A,\sigma))$ we have

$$\partial'\big[A',\sigma',\phi'\big] = \big[C\big(A',\sigma',\phi'\big)\big] - \big[C(A,\sigma,\mathrm{id_Z})\big]. \tag{8}$$

On the other hand, from the exact sequence $1 \to \boldsymbol{\mu}_2 \to \widetilde{\mathbf{T}} \to \mathbf{T} \to 1$ of (5), we get a map $\partial_{\mathbf{T}} : H^1(k,\mathbf{T}) \to H^2(k,\boldsymbol{\mu}_2)$, which by diagram (7) is given by

$$\partial_{\mathbf{T}}(a) = \mathrm{Cor}_{F/k}(a,d) \tag{9}$$

for $a \in H^1(k,\mathbf{T}) = F^\times/N_{E/F}(E^\times)$. The diagram

$$\begin{tikzcd}
1 \arrow[r] & \boldsymbol{\mu}_2 \arrow[r] \arrow[d, "i"'] & \widetilde{\mathbf{T}} \arrow[r] \arrow[d] & \mathbf{T} \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & C \arrow[r] & \mathbf{Spin}(A,\sigma) \arrow[r] & \mathbf{PSO}(A,\sigma) \arrow[r] & 1
\end{tikzcd} \tag{10}$$

commutes, so taking cohomology we have $i_*\partial_{\mathbf{T}}(a) = \partial[A,\sigma_a,\phi_a]$ in $H^2(k,C)$. Taking the image of this equality under the natural map $H^2(k,C) \to \mathrm{Br}(Z)$ and using (9), we get

$$\partial'[A,\sigma_a,\phi_a] = \mathrm{Res}_{Z/k}\,\mathrm{Cor}_{F/k}(a,d). \tag{11}$$

The combination of (8) and (11) proves the desired result. □

Corollary 5.4. *If $I^3(k) = 0$, then $(A,\sigma_a) \cong (A,\sigma)$ if and only if $\mathrm{Res}_{Z/k}\,\mathrm{Cor}_{F/k}(a,d)$ is in the subgroup (of order at most 2) generated by $\mathrm{Res}_{Z/k}[A]$.*

Proof. Let $*$ be the nontrivial k-automorphism of Z. We begin by noting the equality

$$\big[C(A,\sigma,*)\big] - \big[C(A,\sigma,\mathrm{id}_Z)\big] = \mathrm{Res}_{Z/k}[A] \tag{12}$$

in $\mathrm{Br}(Z)$. This is an immediate consequence of [5, (9.9)].

If $(A,\sigma_a) \cong (A,\sigma)$, then $C(A,\sigma_a,\phi_a)$ is isomorphic to either $C(A,\sigma,\mathrm{id}_Z)$ or to $C(A,\sigma,*)$. By Proposition 5.3, we have in the first case $\mathrm{Res}_{Z/k}\,\mathrm{Cor}_{F/k}(a,d) = 0$ and in the second case $\mathrm{Res}_{Z/k}\,\mathrm{Cor}_{F/k}(a,d) = \mathrm{Res}_{Z/k}[A]$, using (12).

Conversely, if $\mathrm{Res}_{Z/k}\,\mathrm{Cor}_{F/k}(a,d) = 0$ or $\mathrm{Res}_{Z/k}\mathrm{Cor}_{F/k}(a,d) = \mathrm{Res}_{Z/k}[A]$, then $[C(A,\sigma_a,\phi_a)] = [C(A,\sigma,\mathrm{id}_Z)]$ or $[C(A,\sigma_a,\phi_a)] = [C(A,\sigma,*)]$, that is, in either case, $C(A,\sigma_a) \cong C(A,\sigma)$ as k-algebras. Under the hypothesis $I^3(k) = 0$, this condition implies $(A,\sigma_a) \cong (A,\sigma)$ by a theorem of Lewis and Tignol [7]. $\square$

Corollary 5.5. *If $I^3(k) = 0$, $d \in k^\times F^{\times 2}$ and n is odd, then, up to conjugacy, there is exactly one involution on A that extends τ.*

Proof. We can assume without loss of generality that $d \in k^\times$. Then $\delta = N_{F/k}(d) = d^n \equiv d \pmod{k^\times)^2}$ and $Z \subset E$, so $\mathrm{Res}_{Z/k}\,\mathrm{Cor}_{F/k} = \mathrm{Cor}_{E/Z}\,\mathrm{Res}_{E/F}$. Since d is a square in E, $\mathrm{Res}_{E/F}(a,d) = 0$. We conclude by Corollary 5.4. $\square$

Acknowledgments

R. Brusamarello and J. Morales gratefully acknowledge the hospitality of IMPA, Rio de Janeiro, during the preparation of this paper. J. Morales is also indebted to the Universidade Estadual de Maringá, Maringá, Brazil, for its hospitality and support.

References

[1] R. Brusamarello, J. Morales, On the second Stiefel–Whitney class of scaled trace forms of central simple algebras, J. London Math. Soc. (2) 61 (2) (2000) 335–348, MR 2001c:11051.
[2] P. Chuard-Koulmann, J. Morales, Extending involutions on Frobenius algebras, Manuscripta Math. 108 (4) (2002) 439–451, MR 1 923 532.
[3] W. Feit, On certain rational quadratic forms, Linear and Multilinear Algebra 3 (1–2) (1975/76) 25–32. Collection of articles dedicated to Olga Taussky-Todd, MR 52 #10593.
[4] J.E. Humphreys, Linear Algebraic Groups, in: Grad. Texts in Math., Vol. 21, Springer-Verlag, New York, 1975, MR 53 #633.
[5] M.-A. Knus, A. Merkurjev, M. Rost, J.-P. Tignol, The Book of Involutions, American Mathematical Society, Providence, RI, 1998; with a preface in French by J. Tits, MR 2000a:16031.
[6] D.W. Lewis, A note on trace forms and involutions of the first kind, Exposition. Math. 15 (3) (1997) 265–272, MR 98d:16033.
[7] D.W. Lewis, J.-P. Tignol, Classification theorems for central simple algebras with involution, Manuscripta Math. 100 (3) (1999) 259–276; with an appendix by R. Parimala, MR 2000m:16027.
[8] J. Morales, J.-M. Piveteau, Quadratic forms invariant under group actions, Illinois J. Math. 36 (1) (1992) 145–154, MR 93e:11046.
[9] W. Scharlau, Quadratic and Hermitian forms, Springer-Verlag, Berlin, 1985, MR 86k:11022.
[10] J.-P. Serre, L'invariant de Witt de la forme $\mathrm{tr}(x^2)$, Comment. Math. Helv. 59 (4) (1984) 651–676, MR 86k:11067.
[11] T.A. Springer, On the equivalence of quadratic forms, Nederl. Akad. Wetensch. Proc. Ser. A 62 (1959) 241–253; = Indag. Math. 21, MR 21 #7184.
[12] T.A. Springer, Linear Algebraic Groups, in: Progr. Math., Vol. 9, Birkhäuser, Boston, MA, 1981, MR 84i:20002.