An Elementary Approach to the Serre-Rost Invariant of Albert Algebras

Holger P. Petersson[1]
Fachbereich Mathematik, FernUniversität, Lützowstraße 125, D-58084 Hagen, Deutschland

Michel L. Racine[2]
Department of Mathematics, University of Ottawa, 585 King Edward, K1N 6N5 Ottawa, Ontario, Canada

Dedicated to Nathan Jacobson on the occasion of his 85*th birthday*

Introduction

Let k be a field remaining fixed throughout this paper. Following a suggestion of Serre [27], Rost [21] has shown that, assuming char $k \neq 2, 3$, every Albert algebra over k admits a cohomological invariant belonging to $H^3(k, \mathbf{Z}/3\mathbf{Z})$ and called its *invariant* mod 3 which is stable under base change and characterizes Albert division algebras.

In the present paper, we give a proof for the existence of this invariant, called the *Serre-Rost invariant* in the sequel, that is more elementary than Rost's. Our approach takes up another suggestion of Serre [26] and is inspired by the concept of chain equivalence [23, p. 143] in the algebraic theory of quadratic forms (see 4.2, 4.13 for details). The proof we obtain in this way works uniformly in all characteristics except 3. (In characteristic 3, Serre has shown how to define the invariant in a different way; see 4.24 for comments). In order to make our presentation comparatively selfcontained, we include without proof some preliminary material from elementary Galois cohomology (Sec. 1) and the theory of algebras of degree 3 (Sec. 2) that will be needed in the subsequent development. Rather than striving for maximum generality, we confine ourselves to what is indispensable for

[1]Supported by Deutsche Forschungsgemeinschaft. The hospitality of the University of Ottawa is gratefully acknowledged.
[2]Supported in part by a grant from NSERC.

the intended applications. The existence and uniqueness theorem for the Serre-Rost invariant is presented in Sec. 3, where we also show uniqueness and, with respect to existence, carry out some easy reductions. Existence is then firmly established in Sec. 4, where a broad outline of the proof may be found in 4.2. Finally, in Sec. 5, we discuss possibilities of answering the question as to whether Albert algebras are classified by their invariants mod 2 and 3. The conscientious reader will notice that we manage to define the Serre-Rost invariant without recourse to the second Tits construction of Albert algebras.

The authors would like to express their gratitude to the participants of the Jordan term held at the University of Ottawa in the fall of 1994 for their lively interest and stimulating discussions. Special thanks are due to O. Loos, M. Rost and, in particular, to J.-P. Serre for valuable comments.

1. Galois Cohomology [4, 24, 25, 29]

1.1. The general setup. We write k_s for the separable closure and $G = \mathrm{Gal}(k_s/k)$ for the absolute Galois group of k, its action on k_s being symbolized exponentially by $(\sigma, a) \mapsto {}^{\sigma}a$. With respect to the Krull topology, G is a compact group. Given a Galois module M (of k) (i.e., an ordinary G-module such that the group action $G \times M \to M$ becomes continuous when M is endowed with the discrete topology), we denote by $H^*(G, M)$ the corresponding cohomology. For a closed subgroup $H \subset G$ and $\sigma \in G$, there is a natural map

$$\sigma^* : H^*(H, M) \longrightarrow H^*(\sigma H \sigma^{-1}, M)$$

extending the action of σ on M in dimension 0.

1.2. Restriction and corestriction. Let $H \subset G$ be an open subgroup (corresponding to a finite intermediate field extension of k_s/k) and M a Galois module. Then there are natural maps

$$\mathrm{res} = \mathrm{res}_{G/H} : H^*(G, M) \longrightarrow H^*(H, M) \qquad \text{(restriction)},$$

$$\mathrm{cor} = \mathrm{cor}_{G/H} : H^*(H, M) \longrightarrow H^*(G, M) \qquad \text{(corestriction)}$$

satisfying

$$\mathrm{cor} \circ \mathrm{res} = [G : H]\mathbf{1}. \tag{1.2.1}$$

In particular, *if p is a prime not dividing $[G:H]$ and M is a p-group*, res *must be injective.*

Suppose now that H is normal in G (and hence corresponds to a finite Galois extension of k). Choosing a full set R of representatives of G/H in G, we then have

$$\text{res} \circ \text{cor} = \sum_{\rho \in R} \rho^*. \tag{1.2.2}$$

1.3. The cup product. Given Galois modules M, M', M'' and integers $p, q, r \geq 0$, there are natural maps

$$\cup : H^p(G, M) \times H^q(G, M') \longrightarrow H^{p+q}(G, M \otimes M'),$$

the tensor product being taken over $\mathbf{Z}$, such that, for all $\alpha \in H^p(G, M), \alpha' \in H^q(G, M'), \alpha'' \in H^r(G, M'')$, the following holds.

(1.3.1) $\cup$ is $\mathbf{Z}$-bilinear.

(1.3.2) $\cup$ is associative, i.e.,

$$(\alpha \cup \alpha') \cup \alpha'' = \alpha \cup (\alpha' \cup \alpha'')$$

after identifying $(M \otimes M') \otimes M'' = M \otimes (M' \otimes M'')$ canonically.

(1.3.3) $\cup$ is *graded* commutative, i.e.,

$$\alpha \cup \alpha' = (-1)^{pq} \alpha' \cup \alpha$$

after identifying $M \otimes M' = M' \otimes M$ canonically.

(1.3.4) $\cup$ is stable under base change, i.e.,

$$\text{res}_{G/H}(\alpha \cup \alpha') = \text{res}_{G/H}(\alpha) \cup \text{res}_{G/H}(\alpha')$$

for any closed subgroup $H \subset G$.

1.4. Commutative group schemes. The cohomological formalism just described applies in particular to commutative affine group schemes of finite type over k [3, 31], i.e., to covariant functors $\mathbf{\Gamma}$ from k-algebras to abelian groups represented, as set-valued functors, by finitely generated k-algebras. We then observe that

$$H^*(k, \mathbf{\Gamma}) := H^*(G, \mathbf{\Gamma}(k_s))$$

depends functorially on k; in fact, given any field extension l/k, there is a natural map

$$\mathrm{res} = \mathrm{res}_{l/k} : H^*(k, \mathbf{\Gamma}) \longrightarrow H^*(l, \mathbf{\Gamma})$$

generalizing the restriction of 1.2 and preserving its major properties, e.g., (1.3.4). For any finite (abelian) group Γ, we denote the associated constant group scheme [31, 2.3] by Γ as well. If $\mathbf{\Gamma}, \mathbf{\Gamma}'$ are commutative affine group schemes of finite type over k, we write $\mathbf{\Gamma} \otimes \mathbf{\Gamma}'$ instead of $\mathbf{\Gamma}(k_s) \otimes \mathbf{\Gamma}'(k_s)$.

1.5. Cyclic field extensions. Fix a positive integer n. Then

$$H^1(k, \mathbf{Z}/n\mathbf{Z}) = \mathrm{Hom}(G, \mathbf{Z}/n\mathbf{Z}),$$

where the right-hand side refers to *continuous* homomorphisms from G to the discrete group $\mathbf{Z}/n\mathbf{Z}$. Using this, one finds a natural bijection between nonzero elements of $H^1(k, \mathbf{Z}/n\mathbf{Z})$ and (isomorphism classes of) pairs (E, σ) consisting of a cyclic field extension E/k of degree n and a generator σ of its Galois group. The element of $H^1(k, \mathbf{Z}/n\mathbf{Z})$ corresponding to (E, σ) will be denoted by $[E, \sigma]$.

1.6. The Brauer group. We write $\mathbf{G}_\mathrm{m}$ for the group scheme attaching to any k-algebra its group units and

$$\mathrm{Br}(k) = H^2(k, \mathbf{G}_\mathrm{m})$$

for the Brauer group of k. The Brauer group allows a canonical interpretation as the group of similarity classes of central simple associative algebras (always assumed to be finite-dimensional over k) under the tensor product; given a central simple associative k-algebra D, the corresponding element of $\mathrm{Br}(k)$ will be denoted by $[D]$.

$\mathrm{Br}(k)$ is an abelian torsion group. For a positive integer n which is prime to the characteristic exponent of k, i.e., to the maximum of 1 and the characteristic, the n-torsion part of $\mathrm{Br}(k)$, i.e.,

$${}_n\mathrm{Br}(k) = \{\alpha \in \mathrm{Br}(k) : n\alpha = 0\},$$

may be described cohomologically as follows. Writing $\boldsymbol{\mu}_n$ for the group scheme of n-th roots of 1, exponentiation by n yields a short exact sequence

$$1 \longrightarrow \boldsymbol{\mu}_n \longrightarrow \mathbf{G}_\mathrm{m} \xrightarrow{n} \mathbf{G}_\mathrm{m} \longrightarrow 1$$

whose associated long exact cohomology sequence, in view of Hilbert's Theorem 90, looks like this:

$$\cdots \longrightarrow k^\times \xrightarrow{n} k^\times \longrightarrow H^1(k, \boldsymbol{\mu}_n) \longrightarrow 1 \longrightarrow H^2(k, \boldsymbol{\mu}_n) \longrightarrow \mathrm{Br}(k) \xrightarrow{n} \mathrm{Br}(k) \longrightarrow \cdots.$$

Hence we have a canonical identification

$$ {}_n\mathrm{Br}(k) = H^2(k, \boldsymbol{\mu}_n). $$

In particular, $[D] \in H^2(k, \boldsymbol{\mu}_n)$ *for every central simple associative* k*-algebra* D *of degree* n. Also, the image of $a \in k^\times$ in $H^1(k, \boldsymbol{\mu}_n)$ will be denoted by $[a]$.

1.7. Example. Let E/k be a cyclic field extension of degree n, σ a generator of its Galois group and $c \in k^\times$. Then the cyclic algebra

$$ D = (E/k, \sigma, c) = E \oplus Ew \oplus \cdots \oplus Ew^{n-1}, w^n = c \cdot 1, wu = {}^\sigma uw \quad (u \in E) $$

is central simple of degree n. Therefore, if n is prime to the characteristic exponent of k, we have $[D] \in H^2(k, \boldsymbol{\mu}_n)$ by 1.6; more precisely,

$$ [D] = [E, \sigma] \cup [c] $$

in the sense of 1.3, 1.5, 1.6 after identifying $\mathbf{Z}/n\mathbf{Z} \otimes \boldsymbol{\mu}_n = \boldsymbol{\mu}_n$ canonically.

Recall that D is a division algebra iff no element of the form c^i $(0 < i < n)$ belongs to the norm group of E [7, Exercise 8.5.3]. Recall further that central associative division algebras of degree 3 are always cyclic, by a theorem of Albert [1, XI Theorem 5].

In the context of this work, only one truly deep result will be needed, namely the following.

1.8. Theorem. (Merkurjev-Suslin [12, 12.2]). *Let* D *be a central simple associative* k*-algebra whose degree* r *is squarefree and prime to the characteristic exponent of* k. *Then for* $a \in k^\times$ *the following statements are equivalent.*

(i) *a is the reduced norm of an element of D.*

(ii) $[D] \cup [a] = 0$ *in* $H^3(k, \boldsymbol{\mu}_r \otimes \boldsymbol{\mu}_r)$. □

In fact, the implication (i) ⇒ (ii) is quite easy to prove (cf. 4.3 below for the special case $r = 3$) whereas (ii) ⇒ (i) constitutes the hard part.

2. Algebras of Degree 3 [6, 10, 11, 14, 17, 18]

2.1. Field extensions. By an *étale* k*-algebra* (*of rank* n) we mean a separable commutative associative k-algebra (of dimension n). (Such an algebra was called a

torus in [14–20].) Let E/k be a separable cubic field extension. Then there exists an étale k-algebra K of rank 2 such that E/k is Galois iff K/k splits. In particular, if E/k is not Galois, K is a field and $E \otimes_k K/K$ is Galois.

2.2. Associative algebras with involution. Let $(D, *)$ be an associative algebra of degree 3 with involution which is central simple over k *as an algebra with involution*, assume that $*$ is of the second kind, and let $A = \mathrm{H}(D, *)$ be the corresponding Jordan algebra of symmetric elements. Then $K = \mathrm{Cent}(D)$, the center of D, is étale of rank 2 over k, and we have the following possibilities.

Case I. K splits, i.e., $K \cong k \oplus k$. Then $D \cong D' \oplus D'^{\mathrm{op}}$ for some central simple associative k-algebra D' of degree 3 and $A \cong D'^{+}$, the Jordan algebra determined by D'.

Case II. K/k is a separable quadratic field extension. Then $A \otimes_k K \cong D^{+}$.

2.3. Jordan algebras. All Jordan algebras of degree 3 over k arise as follows. Let $(V, N, \sharp, 1)$ be a cubic form with adjoint and base point over k, so

- V is a vector space over k (always assumed to be finite-dimensional),
- $N : V \longrightarrow k$ is a cubic form,
- $\sharp : V \longrightarrow V$ is a quadratic map,
- $1 \in V$ is a point

such that, writing $T = -(D^2 \log N)(1)$ for the associated trace form, the relations $x^{\sharp\sharp} = N(x)x, N(1) = 1, T(x^{\sharp}, y) = (DN)(x)y, 1^{\sharp} = 1, 1 \times y = T(y)1 - y$ ($\times$ the bilinearization of $\sharp, T(y) := T(1, y)$) hold under all scalar extensions. Then the U-operator

$$U_x y = T(x, y)x - x^{\sharp} \times y \tag{2.3.1}$$

and the base point 1 give V the structure of a unital quadratic Jordan algebra, written as $\mathcal{J}(V, N, \sharp, 1)$. The following formula will be needed later on.

$$N(x^{\sharp}) = N(x)^2. \tag{2.3.2}$$

Conversely, given any Jordan algebra $\mathcal{J}$ of degree 3 over k, we have $\mathcal{J} = \mathcal{J}(V, N, \sharp, 1)$ where V is the underlying vector space, $N = N_{\mathcal{J}}$ is the generic norm, $\sharp$ is the adjoint, i.e., the numerator of the inversion map, and $1 = 1_{\mathcal{J}}$ is the unit element. Also, $T = T_{\mathcal{J}}$ becomes the generic trace.

2.4. Cyclic algebras. The preceding set-up in particular applies to the Jordan algebras $\mathcal{J} = R^+$ where R is an associative k-algebra of degree 3. For example, let

$$D = (E/k, \sigma, c) = E \oplus Ew \oplus Ew^2,\ w^3 = c1_D, wu = {}^{\sigma}uw \quad (u \in E)$$

be a cyclic algebra of degree 3 over k as in 1.7. Then

$$D^+ = \mathcal{J}(V, N_D, \sharp, 1_D)$$

where V is the vector space underlying D, $N_D : D \longrightarrow k$ is the reduced norm given by

$$(2.4.1)\quad N_D(u_0 + u_1w + u_2w^2) = N_E(u_0) + cN_E(u_1) + c^2N_E(u_2) - cT_E(u_0\,{}^{\sigma}u_1\,{}^{\sigma^2}u_2)$$

for $u_i \in E$ $(i = 0, 1, 2)$, N_E, T_E being the norm, trace, respectively, of E/k, and $\sharp : D \longrightarrow D$ is the adjoint given by

$$(2.4.2)\qquad (u_0 + u_1w + u_2w^2)^{\sharp} = ({}^{\sigma}u_0\,{}^{\sigma^2}u_0 - c\,{}^{\sigma}u_1\,{}^{\sigma^2}u_2) + (c\,{}^{\sigma^2}u_2u_2 - {}^{\sigma^2}u_0u_1)w + (u_1\,{}^{\sigma}u_1 - u_2\,{}^{\sigma}u_0)w^2.$$

We also record an explicit formula for the reduced trace $T_D : D \times D \longrightarrow k$:

$$(2.4.3)\quad T_D(u_0 + u_1w + u_2w^2, u_0' + u_1'w + u_2'w^2) = T_E(u_0, u_0') + cT_E({}^{\sigma}u_1, {}^{\sigma^2}u_2') + cT_E({}^{\sigma^2}u_2, {}^{\sigma}u_1')$$

for $u_i, u_i' \in E$ $(i = 0, 1, 2)$. Finally, the bilinearization of the adjoint reads

$$(2.4.4)\qquad \begin{aligned}(u_0 + u_1w + u_2w^2) \times (u_0' + u_1'w + u_2'w^2) = \\ ({}^{\sigma}u_0\,{}^{\sigma^2}u_0' + {}^{\sigma}u_0'\,{}^{\sigma^2}u_0 - c\,{}^{\sigma}u_1\,{}^{\sigma^2}u_2' - c\,{}^{\sigma}u_1'\,{}^{\sigma^2}u_2) + \\ (c\,{}^{\sigma^2}u_2u_2' + c\,{}^{\sigma^2}u_2'u_2 - {}^{\sigma^2}u_0u_1' - {}^{\sigma^2}u_0'u_1)w + \\ (u_1\,{}^{\sigma}u_1' + u_1'\,{}^{\sigma}u_1 - u_2\,{}^{\sigma}u_0' - u_2'\,{}^{\sigma}u_0)w^2.\end{aligned}$$

2.5. The first Tits construction. Consider an associative k-algebra D of degree 3 and $a \in k^{\times}$. Writing N_D for the norm, $\sharp$ for the adjoint, 1_D for the unit, T_D for the trace of D (or, what amounts to the same, of D^+), 2.3 may be specialized as follows. We define

$$V = D_0 \oplus D_1 \oplus D_2,\ D_i = D \text{ for } i = 0, 1, 2,$$

as a vector space over k, $N : V \longrightarrow k$ by

$$(2.5.1)\qquad N(x) = N_D(x_0) + aN_D(x_1) + a^{-1}N_D(x_2) - T_D(x_0x_1x_2)$$

for $x = (x_0, x_1, x_2) \in V,\ \sharp : V \longrightarrow V$ by

$$x^\sharp = (x_0^\sharp - x_1x_2, a^{-1}x_2^\sharp - x_0x_1, ax_1^\sharp - x_2x_0) \tag{2.5.2}$$

and

$$1 = (1_D, 0, 0).$$

Then $(V, N, \sharp, 1)$ is a cubic form with adjoint and base point whose associated Jordan algebra will be written as

$$\mathcal{J} = \mathcal{J}(D, a) = \mathcal{J}(V, N, \sharp, 1).$$

The bilinearization of $\sharp$ and the associated trace form on $\mathcal{J}$ are given by

$$\begin{aligned} x \times y = (&x_0 \times y_0 - x_1y_2 - y_1x_2, a^{-1}x_2 \times y_2 - x_0y_1 - y_0x_1, \\ &ax_1 \times y_1 - x_2y_0 - y_2x_0), \end{aligned} \tag{2.5.3}$$

$$T(x, y) = T_D(x_0, y_0) + T_D(x_1, y_2) + T_D(x_2, y_1) \tag{2.5.4}$$

for $x = (x_0, x_1, x_2),\ y = (y_0, y_1, y_2) \in V$. Taking orthogonal complements relative to T, (2.5.2), (2.5.4) yield

$$D_0^\perp = D_1 \oplus D_2, \tag{2.5.5}$$

$$D_1^\sharp \subset D_2,\ D_2^\sharp \subset D_1. \tag{2.5.6}$$

The following propositions are well known and easy to prove.

2.6. Proposition. *Let D be a separable associative k-algebra of degree 3 and $a \in k^\times$. Then*

a) *$\mathcal{J} = \mathcal{J}(D, a)$ is a division algebra iff $a \notin N_D(D^\times)$.*

b) *The map*

$$\iota : D^+ \longrightarrow \mathcal{J},\ x_0 \longmapsto \iota(x_0) := (x_0, 0, 0)$$

is an imbedding of (unital) quadratic Jordan algebras with image D_0. □

2.7. Proposition. *Let*

$$D = (E/k, \sigma, c) = E \oplus Ew \oplus Ew^2,\ w^3 = c1,\ wu = {}^\sigma uw\ (u \in E)$$

be a cyclic k-algebra of degree 3 as in 1.7 and 2.4. Then the assignment

$$u_0 + u_1w + u_2w^2 \longmapsto (u_0, {}^\sigma u_1,\ c\,{}^{\sigma^2}u_2)$$

for $u_0, u_1, u_2 \in E$ gives an isomorphism $D^+ \xrightarrow{\sim} \mathcal{J}(E, c)$. □

2.8. The first Tits construction and Albert algebras. Let D be a central simple associative k-algebra of degree 3 and $a \in k^\times$. Then the first Tits construction $\mathcal{J}(D, a)$ is an *Albert algebra*, i.e., a k-form of the Jordan algebra of 3-by-3 hermitian matrices having diagonal entries in k and off-diagonal entries in the split octonion algebra over k. Since D is central simple we have, using the notations of 2.5 and the map ι of 2.6 b),

$$D_1 = \{x \in D_0^\perp : \iota(v) \times \big(\iota(v') \times x\big) = -\iota(vv') \times x \quad (v, v' \in D)\} \tag{2.8.1}$$

$$D_2 = \{x \in D_0^\perp : \iota(v) \times \big(\iota(v') \times x\big) = -\iota(v'v) \times x \quad (v, v' \in D)\}. \tag{2.8.2}$$

2.9. Albert algebras and the first Tits construction. Conversely, let $\mathcal{J}$ be any Albert algebra over k. Then $\mathcal{J}$ contains a subalgebra A as in 2.2. If A has the form D^+ for some central simple associative k-algebra D of degree 3, $\mathcal{J}$ is a first Tits construction; more precisely, there exist a scalar $a \in k^\times$ and an isomorphism $\mathcal{J} \xrightarrow{\sim} \mathcal{J}(D, a)$ which extends the canonical imbedding $\iota : D^+ \longrightarrow \mathcal{J}(D, a)$ of 2.6 b).
Consequently, if $\mathcal{J}$ is not a first Tits construction, it will become one after a suitable separable quadratic field extension (2.2, Case II).

2.10. Subalgebras of Albert division algebras. Let $\mathcal{J}$ be an Albert *division* algebra and $\mathcal{J}' \subset \mathcal{J}$ a subalgebra. Then either $\mathcal{J}'/k$ is a purely inseparable field extension of exponent 1 and characteristic 3, or one of the following holds.

- $\mathcal{J}' = k1,\ \dim \mathcal{J}' = 1.$
- $\mathcal{J}' = E^+$ for E as in 2.1, $\dim \mathcal{J}' = 3.$
- $\mathcal{J}' = A$ for A as in 2.2, $\dim \mathcal{J}' = 9.$
- $\mathcal{J}' = \mathcal{J},\ \dim \mathcal{J}' = 27.$

3. The Serre-Rost Invariant

3.1. *Throughout this section we assume that our base field k has characteristic not* 3. This allows us to use 1.6, 1.7 for $n = 3$. Choosing a primitive third root of unity $\zeta \in k_s$, it is important to note that the assignment

$$\zeta^i \otimes \zeta^j \longmapsto ij \bmod 3 \qquad (i, j \in \mathbf{Z})$$

defines an isomorphism $\boldsymbol{\mu}_3 \otimes \boldsymbol{\mu}_3 \xrightarrow{\sim} \mathbf{Z}/3\mathbf{Z}$ which is independent of the choice of ζ. Thus $\boldsymbol{\mu}_3 \otimes \boldsymbol{\mu}_3$ and $\mathbf{Z}/3\mathbf{Z}$ *canonically* identify as Galois modules (where G acts canonically on $\boldsymbol{\mu}_3$, diagonally on $\boldsymbol{\mu}_3 \otimes \boldsymbol{\mu}_3$ and trivially on $\mathbf{Z}/3\mathbf{Z}$). Our principal aim in the sequel is to give an elementary proof of the following result.

3.2. Theorem. (Rost [21]). *There exists a cohomological invariant assigning to each Albert algebra $\mathcal{J}$ over k a unique element*

$$g_3(\mathcal{J}) \in H^3(k, \mathbf{Z}/3\mathbf{Z})$$

which only depends on the isomorphism class of $\mathcal{J}$ and satisfies the following two conditions.

SR1 *If $\mathcal{J} \cong \mathcal{J}(D, a)$ for some central simple associative algebra D of degree 3 over k and some $a \in k^\times$, then*

$$g_3(\mathcal{J}) = [D] \cup [a] \in H^3(k, \boldsymbol{\mu}_3 \otimes \boldsymbol{\mu}_3) = H^3(k, \mathbf{Z}/3\mathbf{Z}).$$

SR2 *g_3 is invariant under base change, i.e.,*

$$g_3(\mathcal{J} \otimes_k l) = \mathrm{res}_{l/k}(g_3(\mathcal{J}))$$

for any field extension l/k.

Moreover, we have

SR3 *g_3 characterizes division algebras, i.e., $\mathcal{J}$ is a division algebra iff $g_3(\mathcal{J}) \neq 0$.*

3.3. Our principal objective in this paper is to give an elementary proof of this result. To do so, we proceed in two steps. The first step, which will occupy the rest of this section, consists in reducing 3.2 to the assertion that defining g_3 for first Tits constructions as in SR1 makes sense, i.e., is independent of the choices made.

As in Rost [21], we first dispose of SR3, assuming the validity of the rest. Incidentally, this will be the only place where we use the Merkurjev - Suslin Theorem 1.8. Since the property of a cubic form to be anisotropic is preserved under quadratic extensions [9, VII Exercise 7], we may assume that $\mathcal{J} \cong \mathcal{J}(D, a)$ is a first Tits construction as in SR1 (2.9). But then $\mathcal{J}$ is not a division algebra iff $a \in N_D(D^\times)$ (2.6 a)) iff $g_3(\mathcal{J}) = [D] \cup [a] = 0$ (1.8).

3.4. Next we prove uniqueness. By SR1, this will be no problem if $\mathcal{J}$ is a first Tits construction. If not there exists a separable quadratic field extension K/k such

that $\mathcal{J} \otimes_k K$ is a first Tits construction (2.9), forcing $g_3(\mathcal{J} \otimes_k K)$ to be uniquely determined. But then, by SR2 and (1.2.1), so is

$$g_3(\mathcal{J}) = -\mathrm{cor}_{K/k}(g_3(\mathcal{J} \otimes_k K))$$

since $2 = -1$ in $\mathbf{Z}/3\mathbf{Z}$.

3.5. We will try to establish the existence of $g_3(\mathcal{J})$ by reading 3.4 backwards. So let $\mathcal{J}$ be an Albert algebra over k. If $\mathcal{J} \cong \mathcal{J}(D, a)$ is a first Tits construction as in SR1, we define

$$g_3(\mathcal{J}) := [D] \cup [a] \in H^3(k, \mathbf{Z}/3\mathbf{Z}). \tag{3.5.1}$$

Let us assume for time being that this definition makes sense. (This assumption will be justified in Sec. 4.) Then (3.5.1) is stable under base change, by (1.3.4). Also, if $\mathcal{J}$ is not a first Tits construction, we choose any separable quadratic field extension K/k such that $\mathcal{J} \otimes_k K$ is a first Tits construction and *claim that*

$$g_3(\mathcal{J}) := -\mathrm{cor}_{K/k}(g_3(\mathcal{J} \otimes_k K)) \tag{3.5.2}$$

does not depend on the choice of K. Indeed, if K'/k is another separable quadratic field extension such that $\mathcal{J} \otimes_k K'$ is a first Tits construction, the composite extension $L = KK'$ has degree 4 over k, which implies

$$\begin{aligned} \mathrm{cor}_{L/k}(g_3(\mathcal{J} \otimes_k L)) &= \mathrm{cor}_{K/k}\mathrm{cor}_{L/K}\mathrm{res}_{L/K}(g_3(\mathcal{J} \otimes_k K)) \\ &= -\mathrm{cor}_{K/k}(g_3(\mathcal{J} \otimes_k K)) \qquad \text{(by (1.2.1))}, \end{aligned}$$

so the right-hand side does not change when replacing K by K', as desired. Observe that (3.5.2), by (1.2.1) and (1.3.4), holds automatically if $\mathcal{J}$ is a first Tits construction.

3.6. Lemma. *Assuming that* (3.5.1) *makes sense and defining the Serre-Rost invariant as in* 3.5, *condition* SR2 *of* 3.2 *will follow once we have shown*

$$\mathrm{res}_{K/k}\mathrm{cor}_{K/k}(g_3(\mathcal{J} \otimes_k K)) = -g_3(\mathcal{J} \otimes_k K) \tag{3.6.1}$$

for every Albert algebra $\mathcal{J}$ *over* k *and every separable quadratic field extension* K/k *making* $\mathcal{J}$ *a first Tits construction.*

Proof. Let $\mathcal{J}$ be an Albert algebra over k and l/k an arbitrary field extension. Choose any separable quadratic field extension K/k such that $J \otimes_k K$ becomes a first Tits construction. Assume first that K is a subfield of l. Then $\mathcal{J} \otimes_k l$ is a first Tits construction as well and satisfies

$$g_3(\mathcal{J} \otimes_k l) = \mathrm{res}_{l/K}(g_3(\mathcal{J} \otimes_k K))$$

since (3.5.1) is stable under base change. On the other hand, (3.5.2) and (3.6.1) yield

$$\begin{aligned}\mathrm{res}_{l/k}(g_3(\mathcal{J})) &= -\mathrm{res}_{l/K}\mathrm{res}_{K/k}\mathrm{cor}_{K/k}(g_3(\mathcal{J}\otimes_k K))\\ &= \mathrm{res}_{l/K}(g_3(\mathcal{J}\otimes_k K)),\end{aligned}$$

as claimed. We are left with the case that $L = K \otimes_k l$ is a quadratic separable field extension of l, forcing $(\mathcal{J}\otimes_k l)\otimes_l L$ to be a first Tits construction. Hence (3.5.2) gives

$$\begin{aligned}\mathrm{res}_{L/l}(g_3(\mathcal{J}\otimes_k l)) &= -\mathrm{res}_{L/l}\mathrm{cor}_{L/l}(g_3((\mathcal{J}\otimes_k l)\otimes_l L))\\ &= g_3(\mathcal{J}\otimes_k L) && \text{(by (3.6.1))}\\ &= \mathrm{res}_{L/K}(g_3(\mathcal{J}\otimes_k K))\\ &= -\mathrm{res}_{L/K}\mathrm{res}_{K/k}\mathrm{cor}_{K/k}(g_3(\mathcal{J}\otimes_k K)) && \text{(by (3.6.1))}\\ &= \mathrm{res}_{L/k}(g_3(\mathcal{J})) && \text{(by (3.5.2))}\\ &= \mathrm{res}_{L/l}\mathrm{res}_{l/k}(g_3(\mathcal{J})).\end{aligned}$$

But since $\mathrm{res}_{L/l}$ is injective on $H^3(l, \mathbf{Z}/3\mathbf{Z})$ (1.2), this implies SR2. □

3.7. We continue to assume that (3.5.1) makes sense and wish to derive (3.6.1). To do so we extend the nontrivial k-automorphism of K in any way to an element $\sigma \in G$. Then (1.2.2) gives

$$\mathrm{res}_{K/k}\mathrm{cor}_{K/k}(g_3(\mathcal{J}\otimes_k K)) = g_3(\mathcal{J}\otimes_k K) + \sigma^* g_3(\mathcal{J}\otimes_k K).$$

Writing $\mathcal{J}\otimes_k K \cong \mathcal{J}(D, a)$ for some central simple associative K-algebra D of degree 3 as well as some $a \in K^\times$ and observing that σ^* commutes with cup products, we conclude

$$\sigma^* g_3(\mathcal{J}\otimes_k K) = (\sigma^*[D]) \cup (\sigma^*[a]) = [\sigma^* D] \cup [{}^\sigma a]$$

where $\sigma^* A$, for any K-algebra A, agrees with A as a ring but has scalar multiplication twisted by σ. From the assumed validity of (3.5.1) we conclude

$$\sigma^* g_3(\mathcal{J}\otimes_k K) = g_3(\sigma^*(\mathcal{J}\otimes_k K)) = g_3(\mathcal{J}\otimes_k K)$$

since $\mathcal{J}\otimes_k K$, being extended from k, must be isomorphic with $\sigma^*(\mathcal{J}\otimes_k K)$. Combining relations, we end up with (3.6.1).

Summarizing, we may state as our final conclusion *that, in order to prove* 3.2., *it suffices to show that* (3.5.1) *is well defined.*

4. Existence and Uniqueness of the Serre-Rost Invariant

Unless stated otherwise, the base field in this section will be arbitrary. We now perform the second step in the proof of 3.2 by establishing the following result.

4.1. Key Lemma. *Assume* $\operatorname{char} k \neq 3$ *and let* $\mathcal{J}$ *be an Albert algebra over* k*. Given any central simple associative* k*-algebra* D *of degre* 3 *and any scalar* $a \in k^\times$ *satisfying* $\mathcal{J} \cong \mathcal{J}(D, a)$*, the element*

$$[D] \cup [a] \in H^3(k, \mathbf{Z}/3\mathbf{Z})$$

only depends on $\mathcal{J}$ *and not on the choice of* D, a*.*

4.2. We begin by giving a broad outline of the proof. After having easily reduced to the case that $\mathcal{J}$ is a division algebra (4.3), we proceed in the following steps.

Step I. Let $\mathfrak{R}$ be the totality of k-subalgebras $A \subset \mathcal{J}$ having $A \cong D^+$ for some central associative division algebra D of degree 3 over k. Given $A \in \mathfrak{R}$, we are going to define the Serre-Rost invariant of $\mathcal{J}$ *relative to* A, written as $g_3(\mathcal{J}, A)$, in such a way that, for any D as above and any $a \in k^\times$, using notations of 2.5.,

$$g_3\big(\mathcal{J}(D, a), D_0\big) = [D] \cup [a].$$

It then remains to prove that $g_3(\mathcal{J}, A)$ in fact does not depend on A. Hence we must show

$$g_3(\mathcal{J}, A) = g_3(\mathcal{J}, A') \text{ for all } A, A' \in \mathfrak{R}. \tag{4.2.1}$$

Step II. In order to establish (4.2.1), we next reduce to the case that A and A' contain a common cyclic cubic subfield. Therefore, fixing any cyclic cubic subfield E/k in $\mathcal{J}$ and putting

$$\mathfrak{R}_E := \{A \in \mathfrak{R} : E \subset A\},$$

it remains to prove

$$g_3(\mathcal{J}, A) = g_3(\mathcal{J}, A') \text{ for all } A, A' \in \mathfrak{R}_E. \tag{4.2.2}$$

Step III. In order to establish (4.2.2), we follow a suggestion of Serre [26] and introduce a neighboring relation between elements of $\mathfrak{R}_E$ which is motivated by the notion of chain equivalence in the algebraic theory of quadratic forms. In keeping with this motivation, we then perform the following two substeps.

Step III.1. The Serre-Rost invariants of $\mathcal{J}$ relative to neighbors in $\mathfrak{R}_E$ are the same (4.14).

Step III.2. Any two elements of $\mathfrak{R}_E$ can be linked by a finite chain any two successive members of which are neighbors in $\mathfrak{R}_E$; in fact, we will produce such a chain of length at most 4 (4.16). In its final stage, the proof of this requires a somewhat lengthy computation.

We now turn to the proof of 4.1 and begin by reducing to the case that $\mathcal{J}$ is a division algebra. That this reduction is, in fact, allowed follows from the easy direction of the Merkurjev-Suslin Theorem 1.8, whose proof we include for the sake of completeness:

4.3. Lemma. *Assume* $\operatorname{char} k \neq 3$, *let* D *be a central simple associative* k*-algebra of degree* 3 *and* $b \in N_D(D^\times)$. *Then*

$$[D] \cup [b] = 0.$$

Proof. We may assume that D is a division algebra and write $b = N_D(u)$ for some $u \in D^\times$. If $u \in k1$, then $b \in k^{\times 3}$, forcing $[b] = 0$ (1.6). Hence we may assume that $E = k[u] \subset D$ is étale of rank 3. By passing if necessary to an appropriate quadratic extension, which we are allowed to do because of (1.2.1), (1.3.4), we may assume further that E/k is cyclic (2.1), so $D \cong (E/k, \sigma, c)$ as in 1.7 for $n = 3$. Hence

$$\begin{aligned} [D] \cup [b] &= [E, \sigma] \cup [c] \cup [b] && \text{(by 1.7)} \\ &= -[E, \sigma] \cup [b] \cup [c] && \text{(by (1.3.3))} \\ &= [(E/k, \sigma, b)] \cup [c] \\ &= 0 \end{aligned}$$

since b is a norm of E, forcing $(E/k, \sigma, b)$ to be split by 1.7. □

4.4. In view of 4.3, we assume from now on *that* $\mathcal{J}$ *is a division algebra.* As in 2.5, orthogonal complementation is to be understood relative to the trace form of $\mathcal{J}$. Given $M \subset \mathcal{J}$, the set

$$M^{\perp\!\!\!\perp} := \{x \in \mathcal{J} : x \in M^\perp, x^\sharp \in M^\perp\}$$

is called the *strong orthogonal complement of* M *in* $\mathcal{J}$. Notice that $M^{\perp\!\!\!\perp}$ will *not* be a linear space in general. For $A \in \mathfrak{R}$, choose any central associative division algebra D of degree 3 over k and any isomorphism $\eta : D^+ \xrightarrow{\sim} A$. Then an element x is said to be *associated with* (D, η) if $x \in A^{\perp\!\!\!\perp} \cap \mathcal{J}^\times$ and

$$\eta(v) \times \big(\eta(v') \times x\big) = -\eta(vv') \times x \quad \text{for all } v, v' \in D.$$

We denote by $\mathrm{Ass}(D,\eta)$ the collection of all elements associated with (D,η). The standard example illuminating these concepts is the following.

4.5. Example. Let D be a central associative division algebra of degree 3 over k, $a \in k^\times$, $\mathcal{J} = \mathcal{J}(D,a)$ as in 2.5, $A = D_0$, $\eta = \iota$ as in 2.6 b), viewed as an isomorphism $D^+ \xrightarrow{\sim} D_0$. Then (2.5.1 - 6) yield

$$D_0^{\amalg} \cap \mathcal{J}^\times = (D_1 \cup D_2) \cap \mathcal{J}^\times,$$
$$\mathrm{Ass}(D,\iota) = D_1 \cap \mathcal{J}^\times,$$
$$\mathrm{Ass}(D^{\mathrm{op}},\iota) = D_2 \cap \mathcal{J}^\times.$$

These relations are instrumental in proving the following results.

4.6. Lemma. *Given $A \in \mathfrak{R}$, a central associative division algebra D of degree 3 over k and an isomorphism $\eta : D^+ \xrightarrow{\sim} A$, we have*:

a) $\mathrm{Ass}(D,\eta) \neq \emptyset \neq \mathrm{Ass}(D^{\mathrm{op}},\eta)$.

b) $A^{\amalg} \cap \mathcal{J}^\times$ *is the disjoint union of* $\mathrm{Ass}(D,\eta)$ *and* $\mathrm{Ass}(D^{\mathrm{op}},\eta)$.

c) *For all* x, $x \in \mathrm{Ass}(D,\eta)$ *iff* $x^\sharp \in \mathrm{Ass}(D^{\mathrm{op}},\eta)$.

d) *For* $x \in \mathrm{Ass}(D,\eta)$, $N(x) \in k^\times$ *is unique modulo* $N_D(D^\times)$.

Proof. By 2.9, we may assume $\mathcal{J} = \mathcal{J}(D,a), A = D_0, \eta = \iota$ as in 4.5. Then the assertions follow from (2.5.1), (2.8.1,2) and 4.5. □

4.7. We can now carry out Step I of 4.2: Assume $\mathrm{char}\, k \neq 3$, fix $A \in \mathfrak{R}$ and choose any central associative division algebra D of degree 3 over k, any isomorphism $\eta : D^+ \xrightarrow{\sim} A$ as well as any element $x \in \mathrm{Ass}(D,\eta)$ to define

$$g_3(\mathcal{J},A) := [D] \cup [N(x)].$$

4.8. Lemma. *Assume* $\mathrm{char}\, k \neq 3$. *Then, for* $A \in \mathfrak{R}$, $g_3(\mathcal{J},A)$ *as given in* 4.7 *is well defined.*

Proof. Independence of the choice of x follows from 4.6 d) and 4.3. Now suppose D' is another central associative division algebra of degree 3 over k and $\eta' : D'^+ \xrightarrow{\sim} A$ is an isomorphism. Then $\eta' = \eta \circ \varphi$ for some isomorphism $\varphi : D'^+ \xrightarrow{\sim} D^+$. Hence $\varphi : D' \longrightarrow D$ is an isomorphism or an anti-isomorphism. In the former case, we have $x \in \mathrm{Ass}(D',\eta')$, and the assertion follows. In the latter case, we have $x \in \mathrm{Ass}(D'^{\mathrm{op}},\eta')$, forcing $x^\sharp \in \mathrm{Ass}(D',\eta')$ by 4.6 c), and we conclude

$$[D'] \cup [N(x^\sharp)] = (-[D]) \cup [N(x)^2] \qquad \text{(by (2.3.2))}$$

$$= (-[D]) \cup (-[N(x)])$$
$$= [D] \cup [N(x)],$$

which completes the proof. □

Having thus completed Step I of 4.2, it remains to prove (4.2.1).

4.9. Lemma. *Assume* $\operatorname{char} k \neq 3$. *In order to prove* (4.2.1), *we may assume that* A, A' *have a common cyclic cubic subfield.*

Proof. Let $F \subset A, F' \subset A'$ be any cubic subfields and write A'' for the subalgebra of $\mathcal{J}$ generated by F, F'. By passing to a tower of appropriate quadratic field extensions, which we are allowed to do by 1.2.1, 1.3.4, we may assume that F, F' are both cyclic (2.1) and $A'' \in \mathfrak{K}$ (2.2, 2.10). But then we may apply (4.2.1) to A, A'' and to A'', A'. □

In view of 4.9, we have completed Step II of 4.2. We are left with the task of proving (4.2.2). To do so we first provide tools to carry out Step III.

4.10. Lemma. *Let* $x \in E^{\amalg} \cap \mathcal{J}^{\times}$, *and denote by* A *the subalgebra of* $\mathcal{J}$ *generated by* E *and* x. *Let* σ *be a generator of* $\operatorname{Gal}(E/k)$, *put* $c = N(x)$ *and consider the cyclic algebra*

$$D = (E/k, \sigma, c) = E \oplus Ew \oplus Ew^2, w^3 = c1, wu = {}^{\sigma}uw \quad (u \in E)$$

as in 1.7, 2.4.

a) *The rule*

$$\eta(u_0 + u_1 w + u_2 w^2) := u_0 - {}^{\sigma}u_1 \times x - {}^{\sigma^2}u_2 \times x^{\sharp}$$

for $u_0, u_1, u_2 \in E$ *defines an isomorphism* $\eta : D^+ \xrightarrow{\sim} A$ *extending the identity on* E *and satisfying* $\eta(w) = x$.

b) $A = E \oplus (E \times x) \oplus (E \times x^{\sharp}) \in \mathfrak{K}_E$.

c) $E^{\amalg} \cap A^{\times} = (E^{\times} \times x) \cup (E^{\times} \times x^{\sharp})$.

Proof. The proof of [14, Prop. 2.2] yields an isomorphism

$$\mathcal{J}(E, c) \xrightarrow{\sim} A, \ (u_0, u_1, u_2) \longmapsto u_0 - u_1 \times x - c^{-1} u_2 \times x^{\sharp}.$$

Composing with the isomorphism $D^+ \xrightarrow{\sim} \mathcal{J}(E, c)$ of 2.7 implies a). Now b) and c) follow from a) and (2.4.2,3), respectively. □

4.11 Lemma. *If $A \in \mathfrak{R}_E$, then $E^{\perp\!\!\!\perp} \cap A^\times$ is not empty and A is generated by E and any $x \in E^{\perp\!\!\!\perp} \cap A^\times$.*

Proof. Matching A with D^+ for some central associative division algebra D of degree 3 over k, $D = (E/k, \sigma, c)$ must be cyclic as in 2.4, and the assertion follows from (2.4.2,3) and 2.10. □

Part c) of the next lemma is an adaptation of [16, Theorem 2′] to the present set-up.

4.12. Lemma. *Let $A \in \mathfrak{R}_E$, $x' \in A^{\perp\!\!\!\perp} \cap \mathcal{J}^\times$, and write A' for the subalgebra of $\mathcal{J}$ generated by E and x'. Then*

a) $A' \in \mathfrak{R}_E$.

b) $E^{\perp\!\!\!\perp} \cap A \subset A'^{\perp\!\!\!\perp}$.

c) *If* $\operatorname{char} k \neq 3$, *then* $g_3(\mathcal{J}, A) = g_3(\mathcal{J}, A')$.

Proof. a) follows from 4.10 b). In b) we pick any $x \in E^{\perp\!\!\!\perp} \cap A^\times$ (4.11) and conclude from 4.10 b), c) that

$$A = E \oplus (E \times x) \oplus (E \times x^\sharp),\ A' = E \oplus (E \times x') \oplus (E \times x'^\sharp)$$

and $E^{\perp\!\!\!\perp} \cap A = (E \times x) \cup (E \times x^\sharp)$. But since the expression $T(u \times v, w)$ is totally symmetric in u, v, w, we conclude $x, x^\sharp \in A'^\perp$, and b) follows.
c) Choose a central simple associative k-algebra D of degree 3 and an isomorphism $\eta : D^+ \xrightarrow{\sim} A$. Then either $x' \in \operatorname{Ass}(D, \eta)$ or $x' \in \operatorname{Ass}(D^{\mathrm{op}}, \eta)$ (4.6 b)). Since the latter implies $x'^\sharp \in \operatorname{Ass}(D, \eta)$ (4.6 c)) and A' is also generated by E and $x'^\sharp \in E^{\perp\!\!\!\perp} \cap A'^\times$ (4.11), we may assume $x' \in \operatorname{Ass}(D, \eta)$. As usual we write

$$D = (E/k, \sigma, c) = E \oplus Ew \oplus Ew^2, w^3 = c1, wu = {}^\sigma uw \quad (u \in E)$$

where $\mathbf{1} \neq \sigma \in \operatorname{Gal}(E/k), c \in k^\times$. Furthermore, using 2.9, we may identify $\mathcal{J} = \mathcal{J}(D, a)$, for some $a \in k^\times$, in such a way that $A = D_0$ and η is induced by ι as in 2.6 b). Then $x := \eta(w) \in E^{\perp\!\!\!\perp} \cap A^\times \subset A'^{\perp\!\!\!\perp} \cap \mathcal{J}^\times$ (by b)) satisfies $N(x) = c$, and $x' \in \operatorname{Ass}(D, \eta)$ implies

$$x' = (0, x'_1, 0) \text{ for some } x'_1 \in D^\times \qquad \text{(by 4.5)},$$

forcing

$$c' := N(x') = aN_D(x'_1) \qquad \text{(by (2.5.1))}.$$

Now consider the cyclic algebra

$$D' := (E/k, \sigma, c') = E \oplus Ew' \oplus Ew'^2, w'^3 = c'1, w'u = {}^{\sigma}uw' \quad (u \in E)$$

and use 4.10 a) to produce an isomorphism $\eta' : D'^{+} \xrightarrow{\sim} A'$ extending the identity on E and satisfying $\eta'(w') = x'$. For $u \in E$ this yields

$$\begin{aligned}
\eta'(u) \times \big(\eta'(w') \times x\big) &= u \times (x' \times x) \\
&= u \times \big((w,0,0) \times (0, x'_1, 0)\big) \\
&= -(u,0,0) \times (0, wx'_1, 0) \qquad \text{(by (2.5.3))} \\
&= (0, uwx'_1, 0),
\end{aligned}$$

whereas

$$\begin{aligned}
\eta'(uw') \times x &= -({}^{\sigma}u \times x') \times x \qquad \text{(by (4.10 a))} \\
&= (w,0,0) \times (0, {}^{\sigma}ux'_1, 0) \\
&= -(0, w{}^{\sigma}ux'_1, 0) = -(0, {}^{\sigma^2}uwx'_1, 0).
\end{aligned}$$

Hence $x \in A'^{\perp\!\!\!\perp} \cap \mathcal{J}^{\times}$ does not belong to $\mathrm{Ass}(D', \eta')$ and so must belong to $\mathrm{Ass}(D'^{\mathrm{op}}, \eta')$ (4.6 b)). From this we conclude

$$\begin{aligned}
g_3(\mathcal{J}, A') &= [D'^{\mathrm{op}}] \cup [N(x)] \qquad \text{(by 4.7)} \\
&= -[E, \sigma] \cup [c'] \cup [c] \qquad \text{(by 1.7)} \\
&= [E, \sigma] \cup [c] \cup [c'] \qquad \text{(by (1.3.2,3))} \\
&= [D] \cup [N(x')] = g_3(\mathcal{J}, A). \qquad \square
\end{aligned}$$

We can now proceed with Step III.

4.13. Definition. Elements $A, A' \in \mathfrak{R}_E$ are said to be *neighbors*, written as $A \sim A'$, if

$$(A \cup A^{\perp\!\!\!\perp}) \cap (A' \cup A'^{\perp\!\!\!\perp}) - E \neq \emptyset. \qquad \square$$

Obviously, the neighboring relation thus defined is reflexive and symmetric on $\mathfrak{R}_E$. We can now easily perform Step III.1.

4.14. Lemma. *If* $\operatorname{char} k \neq 3$ *and* $A, A' \in \mathfrak{R}_E$ *are neighbors, then*

$$g_3(\mathcal{J}, A) = g_3(\mathcal{J}, A').$$

Proof. Choose $y \in (A \cup A^{\perp\!\!\!\perp}) \cap (A' \cup A'^{\perp\!\!\!\perp}) - E$. If $y \in A \cap A'$ then $A = A'$ by 2.10. If $y \in A \cap A'^{\perp\!\!\!\perp}$ or $y \in A^{\perp\!\!\!\perp} \cap A'$ then $g_3(\mathcal{J}, A) = g_3(\mathcal{J}, A')$ by 4.11, 4.12. If $y \in A^{\perp\!\!\!\perp} \cap A'^{\perp\!\!\!\perp}$ write B for the subalgebra generated by E and y. Then 4.12 implies $B \in \mathfrak{R}_E$ and $g_3(\mathcal{J}, A) = g_3(\mathcal{J}, B) = g_3(\mathcal{J}, A')$. □

We finally turn to Step III.2, which will be more difficult.

4.15. Lemma. *For* $A, A' \in \mathfrak{R}_E$ *we have*

$$A^\perp \cap A'^{\perp\!\!\!\perp} \neq \{0\}.$$

Proof. We may assume $A \neq A'$ and then simply count dimensions: $\dim_k A'^\perp = 18$, and $A^\perp \cap A'^\perp \subset A'^\perp$ is a subspace satisfying

$$\dim_k(A^\perp \cap A'^\perp) = \dim_k(A + A')^\perp = 27 - 9 - 9 + 3 = 12.$$

On the other hand, if we use 2.9 to identify $\mathcal{J} = \mathcal{J}(D', a')$ for some central associative division algebra D' of degree 3 over k and some $a' \in k^\times$ such that $A' = D'_0$ (in the notation of 2.5 adapted to the present set-up), we have $D'_1 \subset A'^{\perp\!\!\!\perp}$ (by (2.5.2, 4)) $\subset A'^\perp$ and $\dim_k D'_1 = 9$. Hence D'_1 intersects $A^\perp$ nontrivially, and the assertion follows. □

4.16. Proposition. *For all* $A, A' \in \mathfrak{R}_E$ *there are* $B, C \in \mathfrak{R}_E$ *such that*

$$A \sim B \sim C \sim A'.$$

4.17. In order to prove 4.16, we begin by defining C as the subalgebra $\mathcal{J}$ generated by E and a nonzero element $z \in A^\perp \cap A'^{\perp\!\!\!\perp}$ (4.15). Indeed, we then have $C \in \mathfrak{R}_E$ (4.12 a)) and $C \sim A'$ (4.13). Also, $z \in E^{\perp\!\!\!\perp}$.

4.18. The construction of B is more troublesome. We identify $\mathcal{J} = \mathcal{J}(D, a)$ for some central associative division algebra D of degree 3 over k and some $a \in k^\times$ in such a way that $A = D_0$. As usual, we write

$$D = (E/k, \sigma, c) = E \oplus Ew \oplus Ew^2, w^3 = c1, wu = {}^\sigma uw \quad (u \in E)$$

as a cyclic algebra, where σ is a generator of $\operatorname{Gal}(E/k)$, and 4.17 yields

$$z = (0, z_1, z_2) \text{ for some } z_1, z_2 \in D.$$

4.19. Lemma. *In* 4.18 *we may assume*

$$z = (0, 1_D, w + tw^2), \ \textit{for some } t \in E.$$

Proof. If $z_1 = 0$ or $z_2 = 0$, then $z \in A^{\perp\!\!\!\perp}$ (4.5), forcing $A \sim C$ by 4.13. Hence we may assume $z_1 \neq 0 \neq z_2$. Setting $a' = N(z_1)a$, the map

$$\varphi : \mathcal{J} \longrightarrow \mathcal{J}(D, a'), \ (v_0, v_1, v_2) \longmapsto (v_0, v_1 z_1^{-1}, z_1 v_2),$$

is an isomorphism inducing the identity on D_0, so $\varphi(C)$ is generated by E and $\varphi(z) = (0, 1_D, z_1 z_2)$. Hence we may assume $z_1 = 1_D$. Furthermore, by (2.5.2) and (4.17),

$$z^\sharp = (-z_2, a^{-1} z_2^\sharp, a1_D) \in E^\perp,$$

which implies $z_2 \in E^\perp \cap D = Ew + Ew^2$. Therefore $z_2 = sw + tw^2$ for some $s, t \in E$. If $s = 0$, we replace w by tw^2, σ by σ^2 and reduce to $z_2 = w$. If $s \neq 0$, we replace w by sw and reduce to $z_2 = w + tw^2$. 4.19 follows. □

4.20. Lemma. *We have* $C = F_0 \oplus F_1 \oplus F_2$ *where*

$$\begin{aligned}
F_0 &= E, \\
F_1 &= \{(0, u, {}^{\sigma}uw + {}^{\sigma^2}utw^2); u \in E\}, \\
F_2 &= \{({}^{\sigma^2}uw + {}^{\sigma}utw^2, a^{-1}cu\,{}^{\sigma^2}t - a^{-1}cu\,{}^{\sigma^2}ttw - a^{-1}uw^2, -au); u \in E\}.
\end{aligned}$$

Proof. From 4.10 b) we obtain

$$C = E \oplus (E \times z) \oplus (E \times z^\sharp).$$

Now let $u \in E$. Then (2.5.3) and 4.19 yield

$$\begin{aligned}
u \times z &= (u, 0, 0) \times (0, 1_D, w + tw^2) \\
&= (0, -u, -wu - tw^2 u) = (0, -u, -{}^{\sigma}uw - {}^{\sigma^2}utw^2).
\end{aligned}$$

Hence $E \times z = F_1$. On the other hand, by (2.5.2), (2.4.2),

$$\begin{aligned}
z^\sharp &= (-w - tw^2, a^{-1}(w + tw^2)^\sharp, a1_D) \\
&= (-w - tw^2, a^{-1}(-c\,{}^{\sigma^2}t + c\,{}^{\sigma^2}ttw + w^2), a1_D),
\end{aligned}$$

which by (2.5.3) implies

$$u \times z^\sharp = (-u \times (w + tw^2), a^{-1}cu\,{}^{\sigma^2}t - a^{-1}cu\,{}^{\sigma^2}ttw - a^{-1}uw^2, -au).$$

But since $u \times (w + tw^2) = -\,{}^{\sigma^2}uw - {}^{\sigma}utw^2$ by (2.4.4), we conclude $E \times z^\sharp = F_2$, and the proof is complete. □

4.21. Lemma. *Setting*

$$x_1 := a^{-1}c(1_D - tw + t\,{}^{\sigma}tw^2) \in D,$$

we have

$$x := (w^2, x_1, 0) \in C^{\perp\!\!\!\perp}$$

and

$$x^\sharp = (cw, -w^2x_1, ax_1^\sharp).$$

Proof. (2.4.3), (2.5.4) yield $T(F_0, x) = T(E, x) = 0$. Moreover, for $u \in E$,

$$\begin{aligned}
T\big((0, u, {}^{\sigma}uw + {}^{\sigma^2}utw^2), x\big) &= a^{-1}cT_D({}^{\sigma}uw + {}^{\sigma^2}utw^2, 1_D - tw + t\,{}^{\sigma}tw^2) && \text{(by (2.5.4))}\\
&= a^{-1}c\big(cT_E({}^{\sigma^2}u, {}^{\sigma^2}tt) + cT_E({}^{\sigma}u\,{}^{\sigma^2}t, -{}^{\sigma}t)\big) && \text{(by (2.4.3))}\\
&= a^{-1}c^2T_E(u, t\,{}^{\sigma}t - {}^{\sigma}tt)\\
&= 0,
\end{aligned}$$

forcing $T(F_1, x) = 0$. Similarly,

$$\begin{aligned}
&T\big((\,{}^{\sigma^2}uw + {}^{\sigma}utw^2, a^{-1}cu\,{}^{\sigma^2}t - a^{-1}cu\,{}^{\sigma^2}ttw - a^{-1}uw^2, -au), x\big) &=\\
&T_D({}^{\sigma^2}uw + {}^{\sigma}utw^2, w^2) + T_D\big(-au, a^{-1}c(1_D - tw + t\,{}^{\sigma}tw^2)\big) &=\\
&cT_E(u, 1_E) - cT_E(u, 1_E) &= \quad 0,
\end{aligned}$$

forcing $T(F_2, x) = 0$. Summing up, 4.20 gives $x \in C^\perp$. Next consider

$$x^\sharp = (w^{2\sharp}, -w^2x_1, ax_1^\sharp) \qquad \text{(by (2.5.2))},$$

where

$$\begin{aligned}
w^{2\sharp} &= cw && \text{(by (2.4.2))}\\
w^2x_1 &= a^{-1}c(-c\,{}^{\sigma^2}t + c\,{}^{\sigma^2}ttw + w^2) && \text{(by 4.21)}\\
ax_1^\sharp &= a^{-1}c^2\big((1_E + c\,{}^{\sigma}t\,{}^{\sigma^2}tt) + (c\,{}^{\sigma^2}ttt\,{}^{\sigma}t + t)w + (t\,{}^{\sigma}t - t\,{}^{\sigma}t1_E)w^2\big) && \text{(by (2.4.2))}\\
&= a^{-1}c^2\big(1 + cN_E(t)\big)(1_E + tw),
\end{aligned}$$

from which we conclude

$$x^\sharp = \big(cw, a^{-1}c(c\,{}^{\sigma^2}t - c\,{}^{\sigma^2}ttw - w^2), a^{-1}c^2(1 + cN_E(t))(1_E + tw)\big).$$

This yields $T(F_0, x^\sharp) = 0$ and, for $u \in E$,

$$\begin{aligned} T\big((0, u, {}^\sigma uw + {}^{\sigma^2}utw^2), x^\sharp\big) &= T_E\big(u, a^{-1}c^2(1 + cN_E(t))1_E\big) + cT_E({}^{\sigma^2}u, -a^{-1}c1_E) \\ &\quad + cT_E({}^\sigma u\, {}^{\sigma^2}t, -a^{-1}c^2 t\, {}^\sigma t) \qquad \text{(by (2.5.4), (2.4.3))} \\ &= \big(a^{-1}c^2 + a^{-1}c^3N_E(t) - a^{-1}c^2 - a^{-1}c^3N_E(t)\big)T_E(u) \\ &= 0, \end{aligned}$$

forcing $T(F_1, x^\sharp) = 0$, as well as

$$\begin{aligned} &T\big(({}^{\sigma^2}uw + {}^\sigma utw^2, a^{-1}cu\, {}^{\sigma^2}t - a^{-1}cu\, {}^{\sigma^2}ttw - a^{-1}uw^2, -au), x^\sharp\big) \qquad = \\ &cT_E(u\, {}^{\sigma^2}t, c1_E) + T_E\big(a^{-1}cu\, {}^{\sigma^2}t, a^{-1}c^2(1 + cN_E(t))1_E\big) + \\ &\quad cT_E\big(-a^{-1}\, {}^{\sigma^2}u, a^{-1}c^2(1 + cN_E(t))\, {}^\sigma t\big) + T_E(-au, a^{-1}c^2\, {}^{\sigma^2}t) \qquad = \\ &T_E\big(u, c^2\, {}^{\sigma^2}t + a^{-2}c^3(1 + cN_E(t))\, {}^{\sigma^2}t - a^{-2}c^3(1 + cN_E(t))\, {}^{\sigma^2}t - c^2\, {}^{\sigma^2}t\big) \;=\; 0, \end{aligned}$$

forcing $T(F_2, x^\sharp) = 0$. By 4.20, all this sums up to $x \in C^{\perp\!\!\!\perp}$. □

4.22. Lemma. *The subalgebra B of $\mathcal{J}$ generated by E and*

$$y = (0, 0, x_1^{-1}w^2) \in A^{\perp\!\!\!\perp}$$

belongs to $\mathfrak{R}_E$, and we have $x \in B^{\perp\!\!\!\perp}$, hence $A \sim B \sim C$.

Proof. We have $y \in A^{\perp\!\!\!\perp}$ by 4.5 and

$$B = E \oplus (E \times y) \oplus (E \times y^\sharp) \in \mathfrak{R}_E$$

by 4.10 b). From (2.5.2), (2.5.3) we conclude first

$$y^\sharp = (0, a^{-1}w^{2\sharp}x_1^{-1\sharp}, 0) = (0, a^{-1}cN_D(x_1)^{-1}wx_1, 0)$$

and then

$$B = \{(u_0, u_1wx_1, x_1^{-1}u_2w^2); u_0, u_1, u_2 \in E\}.$$

Given $u_0, u_1, u_2 \in E$, we now obtain

$$T\big((u_0, u_1wx_1, x_1^{-1}u_2w^2), x\big) = T_D(u_0, w^2) + T_D(x_1^{-1}u_2w^2, x_1) = 0$$

from (2.5.4), (2.4.3) and 4.21, which implies $x \in B^\perp$. On the other hand, 4.21 yields

$$x^\sharp = (cw, -w^2x_1, ax_1^\sharp),$$

so

$$\begin{aligned} T\big((u_0, u_1wx_1, x_1^{-1}u_2w^2), x^\sharp\big) &= cT_D(u_0, w) + T_D(u_1wx_1, ax_1^\sharp) - T_D(x_1^{-1}u_2w^2, w^2x_1) \\ &= aN_D(x_1)T_D(u_1, w) - cT_D(u_2, w) \\ &= 0 \end{aligned}$$

gives $x^\sharp \in B^\perp$ and hence $x \in B^{\perp\perp}$. Moreover, $A \sim B$ by the construction of B and $B \sim C$ by 4.21 and the relation just proved. □

4.23. Combining 4.17 with 4.22 not only completes the proof of 4.16 but also Step III.2 and hence the proof of the Key Lemma 4.1 as well. The authors have not checked whether a result similar to 4.16 holds for associative division algebras of degree 3 or higher.

4.24. Remark. In a letter to the first-named author, Serre has recently shown how to do define the Serre-Rost invariant in characteristic 3. We sketch his construction. Assume $\operatorname{char} k = 3$ and consider the group $H_3^3(k)$ of [28, §10] (with $p = 3$), which is a quotient of the k-vector space Ω^2 of differential 2-forms over k. Let $\mathcal{J} = \mathcal{J}(D, a)$ be a first Tits construction Albert algebra over k as in 2.8. Then there are elements $x \in k, y \in k^\times$ such that D is the central simple associative k-algebra of degree 3 defined by generators X, Y and relations $X^3 - X = x,\ Y^3 = y,\ YXY^{-1} = X + 1$. This being so, Serre has shown, using Rost's Theorem [21] combined with Kato's Galois cohomology of local fields, that the image of

$$x\frac{dy}{y} \wedge \frac{da}{a} \in \Omega^2$$

in $H_3^3(k)$ is independent of the choices made. It should thus be regarded as the Serre-Rost invariant of $\mathcal{J}$ in characteristic 3, the more so since also 3.2 SR3 carries over to this particular setting. We intend to come back to the question whether the approach adopted in the present paper works in characteristic 3 as well.

5. Vista

5.1. Besides the invariant mod 3, there are two other cohomological invariants that may be attached to Albert algebras: The *invariants* mod 2, belonging to $H^3(k, \mathbf{Z}/2\mathbf{Z}), H^5(k, \mathbf{Z}/2\mathbf{Z})$, respectively, and intimately tied up with the trace form

(cf. Serre [27, 28] and Rost [22]). A description relating them explicitly to the Tits process [17] is due to the authors [19, 20].

5.2. Serre [28] has raised the question as to whether Albert algebras are classified by their invariants mod 2 and 3. To get an idea of how one could possibly deal with this question, we consider the corresponding situation for octonion algebras.

5.3. The invariant mod 2 of an octonion algebra. Assume $\operatorname{char} k \neq 2$ and let C be an octonion algebra over k. Then $C \cong \operatorname{Cay}(D, c)$, the octonion algebra arising from some quaternion algebra D over k and some $c \in k^\times$ by means of the Cayley-Dickson doubling process, and, observing $\boldsymbol{\mu}_2(k_s) = \mathbf{Z}/2\mathbf{Z}$ as well as 1.6,

$$g_2(C) := [D] \cup [c] \in H^3(k, \mathbf{Z}/2\mathbf{Z})$$

is called the *invariant* mod 2 *of* C. Of course, one has to show that

(5.3.1) $\qquad g_2(C)$ *is well defined*,

i.e., does not depend on the choice of D and c, which is fairly easy, certainly much easier than the corresponding result for Albert algebras; furthermore, that

(5.3.2) $\qquad g_2(C)$ *is stable under base change*,

which is obvious, in view of (1.3.4); and, finally, that

(5.3.3) $\qquad g_2(C)$ *characterizes division algebras*,

which is a deep result, depending as it does on the Merkurjev-Suslin Theorem 1.8: C splits iff c is a reduced norm of D iff $g_2(C) = [D] \cup [c] = 0$. Using these properties, particularly (5.3.3), one obtains a short proof of the following result which was derived by Arason [2, Proposition 2] using a theorem of Merkurjev.

5.4. Theorem. *Two octonion algebras over k are isomorphic if and only if they have the same invariants* mod 2.

Proof. Let C, C' be octonion algebras over k satisfying $g_2(C) = g_2(C')$. Since a field extension l/k splits C iff $\operatorname{res}_{l/k}(g_2(C)) = 0$ (by (5.3.3)), C and C' have the same splitting fields. But then they are isomorphic, by a theorem of Ferrar [5]. □

5.5. One is tempted to try the same approach for Albert algebras. In what follows, we assume $\operatorname{char} k \neq 3$ and focus attention on first Tits constructions, which are known to have trivial invariants mod 2. Then Serre's original question 5.2 reduces to the following:

(5.5.1) *Are two first Tits construction Albert algebras over k isomorphic if and only if they have the same invariants* mod 3?

Arguing as in the proof of 5.4, we conclude that two first Tits construction Albert algebras having the same invariants mod 3 also have the same splitting fields. Unfortunately, however, Ferrar's aforementioned theorem does not carry over to Albert algebras. In fact, generalizing [13, Theorem 6.1], we have the following class of counter examples.

5.6. Examples. Let D be a central simple associative k-algebra of degree 3 and $a \in k^\times$. Then, as the norm groups of D and D^{op} are the same, $\mathcal{J} = \mathcal{J}(D, a)$ and $\mathcal{J}' = \mathcal{J}(D^{\mathrm{op}}, a)$ have the same splitting fields (2.6a)). On the other hand, $g_3(\mathcal{J}) = -g_3(\mathcal{J}')$, so $\mathcal{J}$ and $\mathcal{J}'$ cannot be isomorphic unless they are split (3.2, SR3).

5.7. In view of 5.5, 5.6 it is natural to ask the following question:

(5.7.1) *Given nonisomorphic first Tits construction Albert algebras $\mathcal{J}, \mathcal{J}'$ over k having the same splitting fields, are there a central simple associative k-algebra D of degree* 3 *and a scalar $a \in k^\times$ satisfying $\mathcal{J} \cong \mathcal{J}(D, a)$ as well as $\mathcal{J}' \cong \mathcal{J}(D^{\mathrm{op}}, a)$*?

Obviously, an affirmative answer to (5.7.1) would also settle (5.5.1). Furthermore, *$\mathcal{J}$ and $\mathcal{J}'$ as in* (5.7.1) *must have the same cubic subfields* [15, Corollary 3]. Hence, in trying to prove (5.7.1), the theory of twisted compositions, due to Springer [30] and, in a more general form, to Knus-Merkurjev-Rost-Tignol [8], might turn out to be useful.

References

1. Albert, A. A.: "Structure of Algebras" . Amer. Math. Soc. Coll. Publ. **24**, Providence, R. I., 1961.

2 Arason, J.: *A proof of Merkurjev's Theorem*. Can. Math. Soc. Conference Proc. **4** (1984), 121 – 130.

3. Demazure, M., Gabriel, P.: "Groupes Algébriques". Paris Amsterdam: Masson & Cie 1970.

4. Evens, L.: "The cohomology of groups". Oxford New York Tokyo: Clarendon Press 1991.

5. Ferrar, J. C.: *Generic splitting fields for composition algebras.* Trans. Amer. Math. Soc. **128** (1967), 506 – 514.

6. Ferrar, J. C., Petersson, H. P.: *Exceptional simple Jordan algebras and Galois cohomology.* Arch. Math. **61** (1993), 517 – 520.

7. Jacobson, N.: "Basic Algebra II". Second Edition. New York: W. H. Freeman 1989.

8. Knus, M.-A., Merkurjev, A. S., Rost, M., Tignol, J.-P.: A forthcoming book.

9. Lang, S.: "Algebra". Reading: Addison-Wesley 1965.

10. McCrimmon, K.: *The Freudenthal-Springer-Tits constructions of exceptional Jordan algebras.* Trans. Amer. Math. Soc. **139** (1969), 495 – 510.

11. – *The Freuenthal-Springer-Tits constructions revisited.* Trans. Amer. Math. Soc. **148** (1970), 293 – 314.

12. Merkurjev, A. S., Suslin, A. A.: *K-Cohomology of Severi-Brauer varieties and the norm residue homomorphism.* Math. USSR Izvestiya **21** (1983), 307 – 340.

13. Petersson, H. P.: *Generic reducing fields of Jordan pairs.* Trans. Amer. Math. Soc. **285** (1984), 825 – 843.

14. Petersson, H. P., Racine, M. L.: *Springer forms and the first Tits construction of exceptional Jordan division algebras.* Manuscripta math. **45** (1984), 249 – 272.

15. – *Cubic subfields of exceptional simple Jordan algebras.* Proc. Amer. Math. Soc. **91** (1) (1984), 31 – 36.

16. – *A norm theorem for central simple algebras of degree* 3. Arch. Math. **42** (1984), 224 – 228.

17. – *Jordan Algebras of degree* 3 *and the Tits process.*. J. Algebra **98** (1) (1986), 211 – 243.

18. – *Classification of algebras arising from the Tits process.* J. Algebra **98** (1986), 244 – 279.

19. – *On the invariants* mod 2 *of Albert algebras.* J. Algebra **174** (1995), 1049 – 1072.

20. – *Reduced models of Albert algebras.* To appear in Math. Z.

21. Rost, M.: *A* (mod 3) *invariant for exceptional Jordan algebras.* C. R. Acad. Sci. Paris Sér. I Math. **315** (1991), 823 – 827.

22. – *A descent property for Pfister forms.* Preprint, 1991.

23. Scharlau, W.: "Quadratic and hermitian forms". (Grundlehren Math. Wiss. Bd. 270) Berlin Heidelberg New York Tokyo: Springer 1985.

24. Serre, J. – P.: "Cohomologie Galoisienne". LNM **5**. Berlin Heidelberg New York: Springer 1965.

25. – "Corps locaux". Paris: Hermann 1962.

26. – Letter to M. L. Racine, April 25, 1991.

27. – *Résumé des cours de l'année* 1990 – 91. Annuaire du Collège de France 1991, 111 - 121.

28. – *Cohomologie Galoisienne: Progrès et Problèmes.* Séminaire Bourbaki. 46ième année, 1993 – 94, n^0 783.

29. Shatz, S. S.: "Profinite groups, arithmetic, and geometry". Princeton: Princeton University Press 1972.

30. Springer, T. A.: "Oktaven, Jordan-Algebren und Ausnahmegruppen". Universität Göttingen: Lecture Notes 1963.

31. Waterhouse, W. C.: "Introduction to affine group schemes". GTM 66, New York Heidelberg Berlin: Springer 1979.