Title
Invariants of simple algebras

Journal
manuscripta mathematica, 129(4)

ISSN
1432-1785

Authors
Baek, Sanghoon
Merkurjev, Alexander S.

Publication Date
2009-08-01

DOI
10.1007/s00229-009-0265-4

Peer reviewed

manuscripta math. 129, 409–421 (2009)

Sanghoon Baek · Alexander S. Merkurjev

Invariants of simple algebras

Received: 10 January 2009 / Revised: 12 February 2009
Published online: 3 April 2009

Abstract. We determine the group of invariants with values in Galois cohomology with coefficients $\mathbb{Z}/2\mathbb{Z}$ of central simple algebras of degree at most 8 and exponent dividing 2.

0. Introduction

Let F be a field and let A be an "algebraic structure" over field extensions of F. More precisely, A is a functor from the category Fields/F of field extensions over F to the category Sets of sets. For example, the values of A can be the sets of isomorphism classes of central simple algebras of given degree n, quadratic forms of dimension n, étale algebras of rank n, etc. As defined in [7], an *invariant* of a functor A with values in a cohomology theory H (also viewed as a functor from Fields/F to Sets) is a morphism of functors $A \to H$. All the invariants of A with values in H form a group $\operatorname{Inv}(A, H)$.

An interesting functor Tors_G can be associated to an algebraic group G defined over F as follows. For a field extension L/F, $\mathit{Tors}_G(L)$ is the set of isomorphism classes of G-torsors over $\operatorname{Spec} L$. All examples of the functors A listed above are isomorphic to the functors Tors_G for certain groups G (cf. [7, §3]). For example, $\mathit{Tors}_G(L)$ for the projective linear group $G = \mathbf{PGL}_n$ is naturally bijective to the set of isomorphism classes of central simple L-algebras of degree n.

The structure of the group $\operatorname{Inv}(A, H)$ was determined for various functors A in [7]. The case $A = \mathit{Tors}_G$ for $G = \mathbf{PGL}_n$, i.e., the problem of classification of invariants of central simple algebras of degree n, is still wide open. In the present paper we determine the group of invariants with values in Galois cohomology with coefficients $\mathbb{Z}/2\mathbb{Z}$ of central simple algebras of degree at most 8 and exponent dividing 2, i.e., determine invariants of Tors_G for $G = \mathbf{GL}_n/\boldsymbol{\mu}_2$ with n dividing 8.

In the present paper, the word "variety" over a field F means a separated integral scheme of finite type over F.

The work of A. S. Merkurjev has been supported by the NSF grant DMS #0652316.

S. Baek · A. S. Merkurjev (✉): Department of Mathematics, University of California, Los Angeles, CA 90095-1555, USA. e-mail: shbaek@math.ucla.edu; merkurev@math.ucla.edu

Mathematics Subject Classification (2000): Primary 16K20; Secondary 12G05

DOI: 10.1007/s00229-009-0265-4

1. Invariants

1.1. Cohomology theories, residues and values

Let F be a field and let C be a Galois module for F such that $nC = 0$ for some n not divisible by char F. We define a graded *cohomology theory H over F* as follows. For any field extension L/F, we write

$$H(L) := \coprod_{r \geq 0} H^r\left(L, C(r)\right),$$

where $C(r)$ is the Tate twist of C [7, 7.8]. Note that $H(L)$ is a (left) module over the cohomology ring

$$\coprod_{r \geq 0} H^r\left(L, (\mathbb{Z}/n\mathbb{Z})(r)\right)$$

with respect to the cup-product. We shall write (x) for the element of

$$H^1\left(L, (\mathbb{Z}/n\mathbb{Z})(1)\right) = H^1(L, \mu_n) \simeq L^\times / L^{\times n}$$

corresponding to the coset $xL^{\times n}$.

Let L be a field extension of F with a discrete valuation v trivial on F and residue field $F(v)$. There is the *residue map* of degree -1 [7, §7.13]:

$$\partial_v : H^r(L) \to H^{r-1}\left(F(v)\right).$$

An element $h \in H^r(L)$ is called *unramified at v* if $\partial_v(h) = 0$.

Let $\pi \in L$ be a prime element. The graded map

$$s_\pi : H^r(L) \to H^r\left(F(v)\right), \quad s_\pi(h) = \partial_v\left((-\pi) \cup h\right)$$

is called a *specialization map* [15, §1]. If $h \in H^r(L)$ is unramified at v, then the element $s_\pi(h)$ does not depend on the choice of π and is called the *value of h at v*, denoted $h(v)$.

1.2. The group $A^0(X, H^r)$

Let X be a variety over F and let H be a cohomology theory over F. Recall that for any point $x \in X$ of codimension 1 we have the *residue map*

$$\partial_x : H^r\left(F(X)\right) \to H^{r-1}\left(F(x)\right)$$

defined as follows [15, §2]:

$$\partial_x = \sum \operatorname{cor}_{F(v)/F(x)} \circ \partial_v,$$

where the sum is taken over all (finitely many) discrete valuations of $F(X)$ over F dominating x, and $\partial_v : H^r\left(F(X)\right) \to H^{r-1}\left(F(v)\right)$ is the residue map for the discrete valuation v. We write

$$A^0(X, H^r) := \bigcap \operatorname{Ker}(\partial_x) \subset H^r\left(F(X)\right),$$

where the intersection is taken over all points $x \in X$ of codimension 1.

Let K/F be a field extension, $p \in X(K)$ a point and $\alpha \in A^0(X, H^r)$ an arbitrary element. We say that p is *nonsingular* if the image of $p : \operatorname{Spec} K \to X$ is a nonsingular point of X. If p is nonsingular, the *value* $\alpha(p)$ *of* α *at* p is the image of α under the pull-back map [15, §12]:

$$A^0(X, H^r) \to A^0(\operatorname{Spec} K, H^r) = H^r(K).$$

1.3. Values of invariants

We view the homogeneous components H^r of the cohomology theory H as functors from the category Fields/F of field extensions over F and field homomorphisms over F to the category Sets of sets. Let $S : \mathit{Fields}/F \to \mathit{Sets}$ be another functor. An H*-invariant of* S *of degree* r is a morphism of functors $q : S \to H^r$ [7, Def. 1.1]. We write $\operatorname{Inv}(S, H^r)$ for the group of H-invariant of S of degree r and $\operatorname{Inv}(S, H)$ for the graded group $\coprod_{r\geq 0} \operatorname{Inv}(S, H^r)$.

Let G be an algebraic group defined over a field F. Let $\operatorname{Tors}_G : \mathit{Fields}/F \to \mathit{Sets}$ be the functor taking a field extension K/F to the set of isomorphism classes of G-torsors over $\operatorname{Spec} K$. We have $\operatorname{Tors}_G(K) \simeq H^1(K, G)$ [11, Ch. VII]. We simply write $\operatorname{Inv}(G, H^r)$ for the group $\operatorname{Inv}(\operatorname{Tors}_G, H^r)$.

Example 1.1. Let $n > 0$ be an integer and $k > 0$ a divisor of n. We view the group $\boldsymbol{\mu}_k$ of kth roots of unity as a subgroup of $\mathbf{GL}_n$ via the embeddings $\boldsymbol{\mu}_k \subset \mathbf{G}_{\mathrm{m}} \subset \mathbf{GL}_n$ and set $G = \mathbf{GL}_n / \boldsymbol{\mu}_k$. By [11, Cor. 28.6], the exact sequence

$$1 \to \mathbf{G}_{\mathrm{m}} \xrightarrow{\alpha} G \xrightarrow{\beta} \mathbf{PGL}_n \to 1,$$

where α is the composition

$$\mathbf{G}_{\mathrm{m}} \xrightarrow{\sim} \mathbf{G}_{\mathrm{m}} / \boldsymbol{\mu}_k \to \mathbf{GL}_n / \boldsymbol{\mu}_k = G$$

and β is the natural epimorphism, and Hilbert Theorem 90 yield a bijection between $H^1(F, G)$ and the kernel of the connecting map

$$\delta : H^1(F, \mathbf{PGL}_n) \to H^2(F, \mathbf{G}_{\mathrm{m}}) = \operatorname{Br}(F).$$

The set $H^1(F, \mathbf{PGL}_n)$ is bijective to the set of isomorphism classes of central simple F-algebras A of degree n and the map δ takes the class of A to $k[A]$. Therefore, there is a natural bijection between $\operatorname{Tors}_G(F) = H^1(F, G)$ and the set of isomorphism classes of central simple F-algebras of degree n and exponent dividing k.

We shall need the following statement:

Proposition 1.2. [7, Th. 11.7] *Let G be an algebraic group over F and $q \in \operatorname{Inv}(G, H^r)$. Let R be a discrete valuation ring containing F with quotient field L and residue field K. Then for any G-torsor E over* $\operatorname{Spec} R$*, we have*:

(1) *The residue of $q(E_L)$ at v is zero, i.e., $q(E_L)$ is unramified at v.*
(2) *The value $q(E_L)(v)$ of $q(E_L)$ at v is $q(E_K)$.*

Let X be a variety over F and $E \to X$ a G-torsor. For a field extension K/F and a point $p \in X(K)$, we write $E_p \to \operatorname{Spec} K$ for the pull-back of the torsor E with respect to $p : \operatorname{Spec} K \to X$. Thus, we have a morphism of functors $X \to \operatorname{Tors}_G$

taking a point p to E_p. We also write E_{gen} for the generic fiber of $E \to X$. It is a G-torsor over Spec $F(X)$.

Theorem 1.3. *Let G be an algebraic group over F, X a variety over F. Let $E \to X$ be a G-torsor and $q \in \mathrm{Inv}(G, H^r)$. Then*

(1) $q(E_{\mathrm{gen}}) \in A^0(X, H^r)$.
(2) *Let K/F be a field extension and let $p \in X(K)$ be a nonsingular point. Then $q(E_p)$ is equal to the value of $q(E_{\mathrm{gen}})$ at p.*
(3) *Let X be smooth and let $f : Y \to X$ be a morphism of varieties over F. Then*
$$f^*\left(q(E_{\mathrm{gen}})\right) = q(f^*(E)_{\mathrm{gen}})$$
in $A^0(Y, H^r)$, where $f^* : A^0(X, H^r) \to A^0(Y, H^r)$ is the pull-back homomorphism.

Proof. (1) and (2) follow from Proposition 1.2 and [15, Cor. 12.4].

(3): By (2), the pull-back homomorphism for the composition Spec $F(Y) \to Y \to X$ is equal to $q(f^*(E)_{\mathrm{gen}})$. The pull-back homomorphism for the first morphism Spec $F(Y) \to Y$ is the inclusion of $A^0(Y, H^r)$ into $H^r(F(Y))$. □

It follows from Theorem 1.3(1) that a G-torsor $E \to X$ gives rise to a group homomorphism
$$\varphi_E : \mathrm{Inv}(G, H^r) \to A^0(X, H^r), \quad q \mapsto q(E_{\mathrm{gen}}).$$

1.4. Classifying torsors

A G-torsor $E \to X$ over F is called *classifying* if X is smooth and the corresponding morphism of functors $X \to \mathrm{Tors}_G$ is surjective, i.e., for any field extension K/F and any G-torsor $E' \to$ Spec K, there is a point $p \in X(K)$ such that $E' \simeq E_p$.

Remark 1.4. We do not require the density condition as in [7, Def. 5.1].

Theorem 1.5. *Let $E \to X$ be a classifying G-torsor over F. Then the map $\varphi_E : \mathrm{Inv}(G, H^r) \to A^0(X, H^r)$ is injective.*

Proof. Let $q \in \mathrm{Ker}(\varphi_E)$, i.e., $q(E_{\mathrm{gen}}) = 0$. Let K/F be a field extension and let $E' \to$ Spec K be a G-torsor. Choose a point $p \in X(K)$ such that $E' \simeq E_p$. By Theorem 1.3(2), $q(E_p)$ is the value of $q(E_{\mathrm{gen}})$ at p. Hence $q(E') = 0$. □

2. Invariants of algebras of degree 8

In this section we assume that $\mathrm{char}(F) \neq 2$.

2.1. The functors Alg_n and Dec_n

For a commutative F-algebra R and $a, b \in R^\times$ we write $(a, b) = (a, b)_R$ for the quaternion algebra $R \oplus Ri \oplus Rj \oplus Rk$ with the multiplication table $i^2 = a$, $j^2 = b, k = ij = -ji$. The class of $(a, b)_R$ in the Brauer group $Br(R)$ will be denoted by $[a, b] = [a, b]_R$. We write $\mathit{Quat}(R)$ for the set of isomorphism classes of quaternion algebras over R.

Let $a \in R^\times$ and $S = R[\sqrt{a}] := R[t]/(t^2 - a)$ the quadratic extension of R. We write $N_R(a)$ for the subgroup of $R^\times$ of all element of the form $x^2 - ay^2$ with $x, y \in R$, i.e., $N_R(a)$ is the image of the norm homomorphism $N_{S/R} : S^\times \to R^\times$. If $b \in N_R(a)$, then the quaternion algebra $(a, b)_R$ is isomorphic to the matrix algebra $M_2(R)$ by [10, Th. 6].

For every $n \geq 1$, $\mathit{Alg}_n(F)$ denotes the set of isomorphism classes of central simple F-algebras of degree 2^n and exponent dividing 2. We can identify $\mathit{Alg}_n(F)$ with the subset of $\mathrm{Br}(F)$ of classes of algebras of degree dividing 2^n. In particular, we have that

$$\mathit{Alg}_1(F) \subset \mathit{Alg}_2(F) \subset \mathit{Alg}_3(F) \subset \cdots \subset \mathrm{Br}_2(F).$$

The isomorphism class of an algebra A in $\mathit{Alg}_n(F)$ is called *decomposable* if A is isomorphic to the tensor product of n quaternion algebras over F. The subset of all decomposable classes in $\mathit{Alg}_n(F)$ is denoted by $\mathit{Dec}_n(F)$. The union of all $\mathit{Dec}_n(F)$ coincides with $\mathrm{Br}_2(F)$.

We view Alg_n and Dec_n as functors $\mathit{Fields}/F \to \mathit{Sets}$. By Example 1.1, the functor Alg_n is isomorphic to the functor Tors_G for $G = \mathbf{GL}_{2^n}/\boldsymbol{\mu}_2$.

Obviously, $\mathit{Alg}_1(F) = \mathit{Dec}_1(F) = \mathit{Quat}(F)$. By Albert's theorem [12, Prop. 5.2], $\mathit{Alg}_2(F) = \mathit{Dec}_2(F)$.

The case $n = 3$ is more complicated. It is shown in [1] that $\mathit{Alg}_3(F) \neq \mathit{Dec}_3(F)$ in general. On the other hand, Tignol proved in [18] that $\mathit{Alg}_3(F) \subset \mathit{Dec}_4(F)$ as the subsets of $\mathrm{Br}_2(F)$.

2.2. *Tignol's construction*

We recall Tignol's argument given in [18]. Let A be a central simple F-algebra in $\mathit{Alg}_3(F)$. By [16], there is a triquadratic splitting extension $F(\sqrt{a}, \sqrt{b}, \sqrt{c})/F$ of A with $a, b, c \in F^\times$. Let $L = F(\sqrt{a})$. By Albert's Theorem, we have

$$[A]_L = [b, s] + [c, t] \tag{1}$$

in $\mathrm{Br}(L)$ for some $s, t \in L^\times$.

Taking the corestriction for the extension L/F in (1), we get

$$0 = 2\,[A] = \left[b, N_{L/F}(s)\right] + \left[c, N_{L/F}(t)\right]$$

in $\mathrm{Br}(F)$, hence $\left[b, N_{L/F}(s)\right] = \left[c, N_{L/F}(t)\right]$. By the Common Slot Lemma [2, Lemma 1.7], we have

$$\left[b, N_{L/F}(s)\right] = \left[d, N_{L/F}(s)\right] = \left[d, N_{L/F}(t)\right] = \left[c, N_{L/F}(t)\right]$$

in $\mathrm{Br}(F)$ for some $d \in F^\times$. It follows that the classes $\left[bd, N_{L/F}(s)\right]$, $\left[cd, N_{L/F}(t)\right]$ and $\left[d, N_{L/F}(st)\right]$ are trivial. By [4, Lemma 2.3] (see also Lemma 2.2 below),

$$\begin{aligned} [bd, s] &= [bd, k]\,, \\ [cd, t] &= [cd, l]\,, \\ [d, st] &= [d, m]\,. \end{aligned}$$

in $\mathrm{Br}(L)$ for some $k, l, m \in F^\times$. It follows from (1) that

$$[A]_L = [bd, k]_L + [cd, l]_L + [d, m]_L$$

in $\mathrm{Br}(L)$. Hence

$$[A] = [a, e]+[bd, k]+[cd, l]+[d, m] = [a, e]+[b, k]+[c, l]+[d, klm] \qquad (2)$$

in $\mathrm{Br}(F)$ for some $e \in F^\times$. We shall also need the following well known statements:

Lemma 2.1. *Let K be a field and let A be a central simple K-algebra such that $[A] \in \mathrm{Br}_2(K)$ and let L/K be a quadratic field extension such that $[A]_L = [b, s] + [c, t]$ for some $b, c \in K^\times$ and $s, t \in L^\times$. Suppose that one of the classes $\big[b, N_{L/K}(s)\big]$ and $\big[c, N_{L/K}(t)\big]$ is zero in $\mathrm{Br}(K)$. Then $A \in \mathit{Dec}_3(K)$.*

Proof. Suppose that $\big[b, N_{L/K}(s)\big] = 0$. Taking the corestriction we get

$$0 = 2[A] = \big[b, N_{L/K}(s)\big] + \big[c, N_{L/K}(t)\big] = \big[c, N_{L/K}(t)\big].$$

By [4, Lemma 2.3], there are $u, v \in K^\times$ such that $[b, s] = [b, u]_L$ and $[c, t] = [c, v]_L$. It follows that the class $[A] - [b, u] - [c, v]$ is split by L, hence is the class of a quaternion algebra. Thus, $A \in \mathit{Dec}_3(K)$. □

Lemma 2.2. *Let R be a commutative F-algebra, $a, b \in R^\times$, $T = R[\sqrt{a}]$ and $x + y\sqrt{a} \in T^\times$ such that $x^2 - ay^2 = u^2 - bv^2$ for some $u, v \in R$. If $x + u \in R^\times$, then $2(x + u)(x + y\sqrt{a}) \in N_T(b)$. In particular,*

$$\big[b, x + y\sqrt{a}\big]_T = [b, 2(x + u)]_T\,.$$

Proof. We have the equality

$$\begin{aligned}(x + y\sqrt{a} + u)^2 - bv^2 &= (x + y\sqrt{a})(x + y\sqrt{a} + 2u) + (u^2 - bv^2)\\ &= (x + y\sqrt{a})(x + y\sqrt{a} + 2u) + (x + y\sqrt{a})(x - y\sqrt{a})\\ &= (x + y\sqrt{a})(2x + 2u).\end{aligned}$$

□

2.3. The Azumaya algebra $\mathcal{A}$

Consider the affine space $\mathbf{A}^8_F$ with coordinates $\mathbf{a}, \mathbf{e}, \mathbf{u}, \mathbf{v}, \mathbf{w}, \mathbf{x}, \mathbf{y}, \mathbf{z}$ and define the rational functions:

$$\begin{aligned}\mathbf{f} &= \mathbf{xy} + \mathbf{az},\\ \mathbf{g} &= \mathbf{y} + \mathbf{xz},\\ \mathbf{d} &= \mathbf{w}^2 - \mathbf{f}^2 + \mathbf{ag}^2,\\ \mathbf{b} &= (\mathbf{u}^2 - \mathbf{x}^2 + \mathbf{a})\mathbf{d}^{-1},\\ \mathbf{c} &= (\mathbf{v}^2 - \mathbf{y}^2 + \mathbf{az}^2)\mathbf{d}^{-1},\\ \mathbf{p} &= (\mathbf{u} + \mathbf{x})(\mathbf{v} + \mathbf{y})(\mathbf{w} + \mathbf{f}).\end{aligned}$$

Let X be the open subscheme of $\mathbf{A}_F^8$ given by

$$\mathbf{q} := \mathbf{adep}(\mathbf{u}^2 - \mathbf{x}^2 + \mathbf{a})(\mathbf{v}^2 - \mathbf{y}^2 + \mathbf{az}^2)(\mathbf{x}^2 - \mathbf{a})(\mathbf{y}^2 - \mathbf{az}^2)(\mathbf{f}^2 - \mathbf{ag}^2) \neq 0,$$

i.e., $X = \mathrm{Spec}(R)$ with $R = F[\mathbf{a}, \mathbf{e}, \mathbf{u}, \mathbf{v}, \mathbf{w}, \mathbf{x}, \mathbf{y}, \mathbf{z}, \mathbf{q}^{-1}]$. Let $S = R[\sqrt{\mathbf{a}}, \sqrt{\mathbf{b}}, \sqrt{\mathbf{c}}]$. Consider the Azumaya R-algebra

$$\mathcal{A}' = (\mathbf{a}, \mathbf{e})_R \otimes (\mathbf{b}, 2(\mathbf{u} + \mathbf{x}))_R \otimes (\mathbf{c}, 2(\mathbf{v} + \mathbf{y}))_R \otimes (\mathbf{d}, 2\mathbf{p})_R\,. \tag{3}$$

We view S as a subring of $\mathcal{A}'$. Moreover, $(\mathbf{d}, 2\mathbf{p})_S := (\mathbf{d}, 2\mathbf{p}) \otimes_R S \subset \mathcal{A}'$.

Let $T = R[\sqrt{\mathbf{a}}]$. It follows from Lemma 2.2 that

$$\begin{aligned}
2(\mathbf{u} + \mathbf{x})(\mathbf{x} + \sqrt{\mathbf{a}}) &\in N_T(\mathbf{bd}) \subset N_S(\mathbf{d}),\\
2(\mathbf{v} + \mathbf{y})(\mathbf{y} + \mathbf{z}\sqrt{\mathbf{a}}) &\in N_T(\mathbf{cd}) \subset N_S(\mathbf{d}),\\
2(\mathbf{w} + \mathbf{f})(\mathbf{x} + \sqrt{\mathbf{a}})(\mathbf{y} + \mathbf{z}\sqrt{\mathbf{a}}) &\in N_T(\mathbf{d}) \subset N_S(\mathbf{d}).
\end{aligned}$$

It follows from (3) that

$$\left[\mathcal{A}'\right]_T = \left[\mathbf{b}, \mathbf{x} + \sqrt{\mathbf{a}}\right] + \left[\mathbf{c}, \mathbf{y} + \mathbf{z}\sqrt{\mathbf{a}}\right] \tag{4}$$

in $\mathrm{Br}(T)$.

Moreover, we have $2\mathbf{p} = 2(\mathbf{u} + \mathbf{x})(\mathbf{v} + \mathbf{y})(\mathbf{w} + \mathbf{f}) \in N_S(\mathbf{d})$, therefore, $(\mathbf{d}, 2\mathbf{p})_S$ is isomorphic to the matrix algebra $M_2(S)$. In particular,

$$M_2(R) \subset M_2(S) \simeq (\mathbf{d}, 2\mathbf{p})_S \subset \mathcal{A}'$$

and hence $\mathcal{A}' \simeq M_2(\mathcal{A})$ for the centralizer $\mathcal{A}$ of $M_2(R)$ in $\mathcal{A}'$ by the proof of [8, Th. 4.4.2]. Then $\mathcal{A}$ is an Azumaya R-algebra of degree 8 that is Brauer equivalent to $\mathcal{A}'$ by [17, Th. 3.10].

Proposition 2.3. *The Azumaya algebra $\mathcal{A}$ is classifying for Alg_3, i.e, the corresponding $\mathbf{GL}_8/\boldsymbol{\mu}_2$-torsor over X is classifying.*

Proof. Let $A \in \mathsf{Alg}_3(K)$, where K is a field extension of F. We shall find a point $p \in X(K)$ such that $A \simeq \mathcal{A}(p)$.

We follow Tignol's construction. There is a triquadratic splitting extension $K(\sqrt{a}, \sqrt{b}, \sqrt{c})/K$ of A with $a, b, c \in K^\times$. Let $L = K(\sqrt{a})$, so

$$[A]_L = [b, s] + [c, t]$$

in $\mathrm{Br}(L)$ for some $s = x + x'\sqrt{a}$, and $t = y + z\sqrt{a} \in L^\times$. Modifying s by a norm for the extension $L(\sqrt{b})/L$, we may assume that $x' \neq 0$. Similarly, we may assume that $z \neq 0$. Moreover, replacing a by ax'^2, we may assume that $x' = 1$.

We have

$$\left[b, x^2 - a\right] = \left[d, x^2 - a\right] = \left[d, y^2 - az^2\right] = \left[c, y^2 - az^2\right]$$

in $\mathrm{Br}(K)$ for some $d \in K^\times$, so the classes $\left[bd, x^2 - a\right]$, $\left[cd, y^2 - az^2\right]$ and $\left[d, (x^2 - a)(y^2 - az^2)\right]$ are trivial. Hence

$$\begin{aligned} bd &= u^2 - (x^2 - a)u'^2, \\ cd &= v^2 - (y^2 - az^2)v'^2, \\ d &= w^2 - (x^2 - a)(y^2 - az^2)w'^2 \end{aligned}$$

for some u, u', v, v', w, w' in K. Moreover, we may assume that $u' \neq 0$. Replacing b and u by bu'^2 and uu' respectively, we may assume that $u' = 1$. Similarly, we may assume $v' = w' = 1$.

Replacing u by $-u$ if necessary, we may assume that $u + x \neq 0$ and similarly $v + y \neq 0$ and $w + s \neq 0$, where $s = xy + az$. It follows from Lemma 2.2 that

$$\begin{aligned} \left[b, x + \sqrt{a}\right] &= [b, 2(u + x)]_L\,, \\ \left[c, y + z\sqrt{a}\right] &= [c, 2(v + y)]_L\,, \\ \left[d, (x + \sqrt{a})(y + z\sqrt{a})\right] &= [d, 2(w + s)]_L \end{aligned}$$

in $\mathrm{Br}(L)$. Hence

$$[A] = [a, e] + [b, 2(u + x)] + [c, 2(v + y)] + [d, 2(u + x)(v + y)(w + s)]$$

in $\mathrm{Br}(K)$ for some $e \in K^\times$.

Let p be the point (a, e, u, v, w, x, y, z) in $X(K)$. We have $[\mathcal{A}(p)] = [A]$ and hence $\mathcal{A}(p) \simeq A$ as $\mathcal{A}(p)$ and A have the same dimension. □

Proposition 2.4. *Let K be the quotient field of the ring $R = F[X]$. Let $\widehat{K}$ be the completion of K with respect to the discrete valuation associated with one of the irreducible polynomials* $\mathbf{a}, \mathbf{u}^2 - \mathbf{x}^2 + \mathbf{a}, \mathbf{v}^2 - \mathbf{y}^2 + \mathbf{a}\mathbf{z}^2, \mathbf{d}, \mathbf{x}^2 - \mathbf{a}, \mathbf{y}^2 - \mathbf{a}\mathbf{z}^2, \mathbf{f}^2 - \mathbf{a}\mathbf{g}^2, \mathbf{u} + \mathbf{x}, \mathbf{v} + \mathbf{y}$ *and* $\mathbf{w} + \mathbf{f}$. *Then $\mathcal{A}_{\widehat{K}} \in Dec_3(\widehat{K})$.*

Proof. First assume that the valuation $v = v_{\mathbf{a}}$ is associated with $\mathbf{a}$. By Hensel's Lemma, $\mathbf{x}^2 - \mathbf{a} \in \widehat{K}^{\times 2}$. It follows that $\left[\mathbf{b}, \mathbf{x}^2 - \mathbf{a}\right]_{\widehat{K}} = 0$. By Lemma 2.1, applied to (4), $\mathcal{A}_{\widehat{K}} \in Dec_3(\widehat{K})$.

Let $v = v_{\mathbf{u}^2 - \mathbf{x}^2 + \mathbf{a}}$. In the residue field, $\bar{\mathbf{u}}^2 - \bar{\mathbf{x}}^2 + \bar{\mathbf{a}} = \bar{0}$, hence $\bar{\mathbf{x}}^2 - \bar{\mathbf{a}}$ is a square. By Hensel's Lemma, $\mathbf{x}^2 - \mathbf{a} \in \widehat{K}^{\times 2}$. Therefore, $\mathcal{A}_{\widehat{K}} \in Dec_3(\widehat{K})$ as in the previous case.

The case $v = v_{\mathbf{v}^2 - \mathbf{y}^2 + \mathbf{a}\mathbf{z}^2}$ is similar.

Let $v = v_{\mathbf{d}}$. In the residue field, $\bar{\mathbf{w}}^2 - \bar{\mathbf{f}}^2 + \bar{\mathbf{a}}\bar{\mathbf{g}}^2 = \bar{0}$, hence $\bar{\mathbf{f}}^2 - \bar{\mathbf{a}}\bar{\mathbf{g}}^2$ is a square. By Hensel's Lemma, $\mathbf{f}^2 - \mathbf{a}\mathbf{g}^2 \in \widehat{K}^{\times 2}$, hence $\left[\mathbf{b}, \mathbf{f}^2 - \mathbf{a}\mathbf{g}^2\right]_{\widehat{K}} = 0$. It follows from (4) that

$$[\mathcal{A}]_T = \left[\mathbf{b}, \mathbf{x} + \sqrt{\mathbf{a}}\right] + \left[\mathbf{c}, \mathbf{y} + \mathbf{z}\sqrt{\mathbf{a}}\right] = \left[\mathbf{b}, \mathbf{f} + \mathbf{g}\sqrt{\mathbf{a}}\right] + \left[\mathbf{bc}, \mathbf{y} + \mathbf{z}\sqrt{\mathbf{a}}\right].$$

By Lemma 2.1, $\mathcal{A}_{\widehat{K}} \in Dec_3(\widehat{K})$.

Let $v = v_{\mathbf{x}^2 - \mathbf{a}}$. In the residue field, $\bar{\mathbf{b}}\bar{\mathbf{d}} = \bar{\mathbf{u}}^2$ is a square. By Hensel's Lemma, $\mathbf{bd} \in \widehat{K}^{\times 2}$. It follows from (3) that $\mathcal{A}_{\widehat{K}} \in Dec_3(\widehat{K})$.

The cases $v = v_{\mathbf{y}^2 - \mathbf{a}\mathbf{z}^2}$ and $v = v_{\mathbf{f}^2 - \mathbf{a}\mathbf{g}^2}$ are similar.

Let $v = v_{\mathbf{u}+\mathbf{x}}$. In the residue field, $\bar{\mathbf{b}}\bar{\mathbf{d}} = \bar{\mathbf{a}}$. By Hensel's Lemma, $\mathbf{abd} \in \widehat{K}^{\times 2}$. It follows again from (3) that $\mathcal{A}_{\widehat{K}} \in \mathit{Dec}_3(\widehat{K})$.

The cases $v = v_{\mathbf{v}+\mathbf{y}}$ and $v = v_{\mathbf{w}+\mathbf{f}}$ are similar. □

From now on we consider the cohomology theory with values in the Galois module $\mathbb{Z}/2\mathbb{Z}$, i.e., $H(L) = H(L, \mathbb{Z}/2\mathbb{Z})$ for any field extension of F. Note that $H(L)$ has structure of a commutative ring.

Proposition 2.5. *The restriction homomorphism*

$$\mathrm{Inv}(\mathit{Alg}_3, H^r) \to \mathrm{Inv}(\mathit{Dec}_3, H^r)$$

is injective.

Proof. Let q be an invariant of Alg_3 of degree r and let K be the quotient field of the ring R, i.e., $K = F(X)$. By Theorem 1.3, we have $q(\mathcal{A}_K) \in A^0(X, H^r)$. Let X' be the open subscheme of $\mathbf{A}^8_F$ given by $\mathbf{e} \neq 0$, so $X \subset X' \subset \mathbf{A}^8_F$ and $X' \simeq \mathbf{A}^7_F \times \mathbf{G}_{\mathrm{m}}$. Note that

$$A^0(X', H^r) = A^0(\mathbf{G}_{\mathrm{m}}, H^r) = H^r(F) \oplus (\mathbf{e}) \cup H^{r-1}(F)$$

by [15, Prop. 2.2 and Prop. 8.6].

Suppose that the restriction of q on Dec_3 is zero. By Proposition 2.4, $\mathcal{A}_{\widehat{K}} \in \mathit{Dec}_3(\widehat{K})$, where $\widehat{K}$ is the completion of K with respect to every divisor x of X' in $X' \backslash X$. Hence $q(\mathcal{A}_{\widehat{K}}) = 0$ for all such $\widehat{K}$. The residue homomorphism $\partial_x : H^r(K) \to H^{r-1}(F(x))$ factors through the group $H^r(\widehat{K})$. It follows that $\partial_x(q(\mathcal{A}_K)) = 0$ and therefore,

$$q(\mathcal{A}_K) \in A^0(X', H^r) = H^r(F) \oplus (\mathbf{e}) \cup H^{r-1}(F),$$

i.e., $q(\mathcal{A}_K) = h_K + (\mathbf{e}) \cup h'_K$ for some $h \in H^r(F)$ and $h' \in H^{r-1}(F)$. Consider a point $p \in X(E)$ with $E = F(\mathbf{e})$ such that $\mathbf{e}(p) = \mathbf{e}$ and $\mathbf{b}(p) = 1$. It follows from (3) that $\mathcal{A}(p) \in \mathit{Dec}_3(E)$. Hence by Theorem 1.3(2),

$$0 = q(\mathcal{A}(p)) = h_E + (\mathbf{e}) \cup h'_E,$$

therefore, $h = h' = 0$ and $q(\mathcal{A}_K) = 0$. By Proposition 2.3 and Theorem 1.5, $q = 0$. □

2.4. *Invariants of Dec_n*

From now on we assume that $-1 \in F^{\times 2}$.

Let $K_*(F)$ denote the Milnor ring of a field F and set $k_*(F) = K_*(F)/2K_*(F)$. For every $n \geq 0$, let γ_n denote the *divided power* operation [9,19]:

$$k_2(F) \to k_{2m}(F)$$

defined by

$$\gamma_n\left(\sum_{i=1}^{r} \alpha_i\right) = \sum_{1 \leq i_1 \leq \cdots \leq i_m \leq n} \alpha_{i_1} \cdot \cdots \cdot \alpha_{i_m},$$

where the α_i are symbols. In particular, $\gamma_0 = 1 \in k_0(F) = \mathbb{Z}/2\mathbb{Z}$ and γ_1 is the identity.

We identify $k_2(F)$ with $\mathrm{Br}_2(F)$ via the norm residue isomorphism. Restricting γ_m to Dec_n and composing with the norm residue homomorphism $k_{2m}(F) \to H^{2m}(F)$, we can view the divided power operations (still denoted by γ_m) as invariants of Dec_n with values in H, so $\gamma_m \in \mathrm{Inv}(\mathit{Dec}_n, H^{2m})$ for all n. Clearly, $\gamma_m = 0$ if $m > n$.

Theorem 2.6. *The $H(F)$-module $\mathrm{Inv}(\mathit{Dec}_n, H)$ is free with basis $\{1 = \gamma_0, \gamma_1, \dots, \gamma_n\}$.*

Proof. The case $n = 1$, when $\mathit{Dec}_1 = \mathit{Quat}$ is proven in [7, Th. 18.1]. By [7, Ex. 16.5], the natural map

$$\mathrm{Inv}(\mathit{Quat}, H)^{\otimes n} \to \mathrm{Inv}(\mathit{Quat}^{\times n}, H)$$

is an isomorphism. It follows that $\mathrm{Inv}(\mathit{Quat}^{\times n}, H)$ is a free $H(F)$-module with basis of all monomials $\delta_1^{\varepsilon_1}\delta_2^{\varepsilon_2}\dots\delta_n^{\varepsilon_n}$, where $\varepsilon_1 = 0$ or 1 and the invariant δ_i is defined by $\delta_i(\alpha_1, \dots, \alpha_n) = \alpha_i$.

The natural morphism of functors

$$\mathit{Quat}^{\times n} \to \mathit{Dec}_n \tag{5}$$

given by the tensor product is surjective. It follows that the map

$$\mathrm{Inv}(\mathit{Dec}_n, H) \to \mathrm{Inv}(\mathit{Quat}^{\times n}, H)$$

is injective. The image of this map is element-wise invariant under the natural action of the symmetric group S_n and hence is contained in the free $H(F)$-submodule generated by the standard symmetric functions γ_m on the $\delta_1, \dots, \delta_n$ that are precisely the divided powers. □

Remark 2.7. Vial has computed all invariants of k_n in [19].

Restricting the divided powers on the subfunctors $\mathit{Alg}_n \subset \mathrm{Br}_2$ we view the γ_m as invariants on Alg_n.

Theorem 2.8. *If $n \le 3$, then the $H(F)$-module $\mathrm{Inv}(\mathit{Alg}_n, H)$ is free with basis $\{1 = \gamma_0, \gamma_1, \dots, \gamma_n\}$.*

Proof. If $n \le 2$, then $\mathit{Alg}_n = \mathit{Dec}_n$ and the statement follows from Theorem 2.6. The case $n = 3$ is implied by Proposition 2.5 and Theorem 2.6. □

2.5. Reduced trace form

Let A be a central simple algebra over a field F. Denote by q_A the quadratic form on A defined by $q_A(a) = \mathrm{Trd}_A(a^2)$ for $a \in A$, where Trd_A is the reduced trace form for A. If A and A' are two central simple algebras over F, then

$$q_{A\otimes A'} \simeq q_A \otimes q_{A'}.$$

Example 2.9. Let A be a quaternion algebra over a field F. Then q_A is the 2-fold Pfister form $\langle\langle a, b\rangle\rangle$, where $a, b \in F^\times$ such that $[A] = [a, b]$ in $\mathrm{Br}(F)$.

It follows from Example 2.9 that for any $A \in \mathit{Dec}_n(F)$ the form q_A is a $2n$-fold Pfister form. Moreover, the invariant $e_{2n}(q_A)$ in $H^{2n}(F)$ (cf. [6, §16]) coincides with the divided power $\gamma_n(A)$.

Theorem 2.10. *If $n \le 3$, then for any $A \in \mathit{Alg}_n(F)$, the form q_A is a $2n$-fold Pfister form such that $e_{2n}(q_A) = \gamma_n(A)$.*

Proof. If $n \le 2$, then $\mathit{Alg}_n = \mathit{Dec}_n$ and the statement follows.

Consider the case $n = 3$. Let $A \in \mathit{Alg}_3(F)$. Choose a splitting field $F(\sqrt{a}, \sqrt{b}, \sqrt{c})$ and set $L = F(\sqrt{a})$. We write $a \mapsto \bar{a}$ for the nontrivial automorphism of L over F. Let B be the centralizer of L in A. By Skolem–Noether Theorem [11, Th. 1.4], there is an $s \in A$ such that $sxs^{-1} = \bar{x}$ for all x in L. Note that s^2 commutes with all elements in L, hence $s^2 \in B$.

Let $\psi : B \to B$ be an automorphism defined by $y \mapsto sys^{-1}$. Then $A = B \oplus Bs$ with $sy = \psi(y)s$ for all $y \in B$. Since $\mathrm{Trd}_A(yzs) = \mathrm{Trd}_A(\sqrt{a}yzs(\sqrt{a})^{-1}) = -\mathrm{Trd}_A(yzs)$, we have $\mathrm{Trd}_A(yzs) = 0$ for any y and z in B. Moreover, $\mathrm{Trd}_A(y) = \mathrm{Tr}_{L/F}(\mathrm{Trd}_B(y))$ for any $y \in B$ by [5, §22, Cor. 5]. Therefore, for the trace forms we have

$$q_A = \mathrm{Tr}_{L/F}(q_B) \perp \mathrm{Tr}_{L/F}(q'_B),$$

where $q'_B(x) = \mathrm{Trd}_B\left((xs)^2\right)$.

Let $t \in F^\times$ and A_t the F-algebra with presentation $A_t = B \oplus By$ and $yby^{-1} = sbs^{-1}$ for all $b \in B$ and $y^2 = ts^2$. By Proposition [11, Th. 13.41],

$$[A_t] = [a, t] + [A].$$

Moreover,

$$q_{A_t} = \mathrm{Tr}_{L/F}(q_B) \perp t\,\mathrm{Tr}_{L/F}(q'_B),$$

hence, by Lemma 2.11 below, in the Witt ring of F, we have

$$q_A - tq_{A_t} = \langle\langle t\rangle\rangle \cdot \mathrm{Tr}_{L/F}(q_B) \in I^6(F).$$

By (2), we can choose t such that A_t is decomposable, hence $q_{A_t} \in I^6(F)$ and therefore, $q_A \in I^6(F)$. As $\dim(q_A) = 64$, the form q_A is a 6-fold Pfister form.

It follows that $e_6(q_A)$ is a well-defined invariant of Alg_3 that agrees with γ_3 on Dec_3. By Proposition 2.5, $e_6(q_A) = \gamma_3$ on Alg_3. □

Lemma 2.11. *In the notation above,* $\mathrm{Tr}_{L/F}(q_B) \in I^5(F)$.

Proof. In Tignol's construction (see (1) and (2)),

$$[A]_L = [b, s] + [c, t] = [a, e] + [b, k] + [c, l] + [d, klm]$$

in $\mathrm{Br}(L)$. Let

$$p := \langle\langle a, e\rangle\rangle + \langle\langle b, k\rangle\rangle + \langle\langle c, l\rangle\rangle + \langle\langle d, klm\rangle\rangle \in I^2(F). \tag{6}$$

It follows that

$$p_L \equiv \langle\langle b, s\rangle\rangle + \langle\langle c, t\rangle\rangle \mod I^3(L),$$

so $B \simeq (b, s) \otimes_L (c, t)$. We have in $W(L)$:

$$q_B = \langle\langle b, s\rangle\rangle \cdot \langle\langle c, t\rangle\rangle \equiv \langle\langle b, s\rangle\rangle \cdot p_L - \langle\langle b, s\rangle\rangle = \langle\langle b, s\rangle\rangle \cdot p_L \mod I^5(L)$$

since $\langle\langle b, b\rangle\rangle = 0$. By the projection formula and [6, Cor. 34.19],

$$\mathrm{Tr}_{L/F}(q_B) \equiv \mathrm{Tr}_{L/F}\left(\langle\langle b, s\rangle\rangle\right) \cdot p \equiv \langle\langle b, N_{L/F}(s)\rangle\rangle \cdot p \mod I^5(F). \quad (7)$$

We have $\langle\langle b, N_{L/F}(s)\rangle\rangle \simeq \langle\langle c, N_{L/F}(t)\rangle\rangle \simeq \langle\langle d, N_{L/F}(t)\rangle\rangle$. It follows that $\langle\langle b, N_{L/F}(s)\rangle\rangle$ annihilates all four summands in the right hand side of (6), hence $\langle\langle b, N_{L/F}(s)\rangle\rangle \cdot p = 0$. By (7), $\mathrm{Tr}_{L/F}(q_B) \in I^5(F)$. □

2.6. Essential dimension of Dec_n and Alg_3

Let $S : \mathit{Fields}/F \to \mathit{Sets}$ be a functor, $E \in \mathit{Fields}/F$ and $K \subset E$ a subfield over F. An element $\alpha \in S(E)$ is said to be *defined over* K (and K is called a *field of definition of* α) if there exists an element $\beta \in S(K)$ such that α is the image of β under the map $S(K) \to S(E)$. The *essential dimension of* α, denoted $\mathrm{ed}(\alpha)$, is the least transcendence degree $\mathrm{tr.deg}_F(K)$ over all fields of definition K of α. The *essential dimension of the functor* S is

$$\mathrm{ed}(S) = \sup\{\mathrm{ed}(\alpha)\},$$

where the supremum is taken over fields $E \in \mathit{Fields}/F$ and all $\alpha \in S(E)$ (cf. [3, Def. 1.2]).

The highest invariant γ_n of Alg_n and Dec_n of degree $2n$ is nontrivial, hence $\mathrm{ed}\left(\mathit{Alg}_n\right) \geq 2n$ and $\mathrm{ed}\left(\mathit{Dec}_n\right) \geq 2n$ by [3, Cor. 3.6]. On the other hand, using the surjection (5), we get

$$\mathrm{ed}\left(\mathit{Dec}_n\right) \leq \mathrm{ed}\left(\mathit{Quat}^{\times n}\right) \leq n \cdot \mathrm{ed}\left(\mathit{Quat}\right) = 2n.$$

Thus, $\mathrm{ed}\left(\mathit{Dec}_n\right) = 2n$.

It is proved in [13, Cor. 3.10] and [14, Th. 8.6] that $\mathrm{ed}\left(\mathit{Alg}_3\right) \leq 17$.

Theorem 2.12. $6 \leq \mathrm{ed}\left(\mathit{Alg}_3\right) \leq 8$.

Proof. By Proposition 2.3, there is a surjective morphism of functors $X \to \mathit{Alg}_3$, where X is a variety defined in Sect. 2. By [3, Cor. 1.19], $\mathrm{ed}\left(\mathit{Alg}_3\right) \leq \dim(X) = 8$. □

References

[1] Amitsur, S.A., Rowen, L.H., Tignol, J.-P.: Division algebras of degree 4 and 8 with involution. Israel J. Math. **33**(2), 133–148 (1979)
[2] Arason, J.Kr.: Cohomologische invarianten quadratischer formen. J. Algebra **36**(3), 448–491 (1975)
[3] Berhuy, G., Favi, G. : Essential dimension: a functorial point of view (after A Merkurjev). Doc. Math. **8**, 279–330 (electronic) (2003)
[4] Dherte, H.: Quadratic descent of involutions in degree 2 and 4. Proc. Am. Math. Soc. **123**(7), 1963–1969 (1995)
[5] Draxl, P.K.: Skew Fields, London Mathematical Society Lecture Note Series, vol. 81. Cambridge University Press, Cambridge (1983)
[6] Elman, R., Karpenko, N., Merkurjev, A.: The Algebraic and Geometric Theory of Quadratic Forms. American Mathematical Society Colloquium Publications, vol. 56, American Mathematical Society, Providence (2008)
[7] Garibaldi, R., Merkurjev, A., Serre, J.-P.: Cohomological Invariants in Galois Cohomology. American Mathematical Society, Providence (2003)
[8] Herstein, I.N.: Noncommutative Rings. Carus Mathematical Monographs, vol. 15. Mathematical Association of America, Washington, DC (1994) (Reprint of the 1968 original, With an afterword by L.W. Small)
[9] Kahn, B.: Comparison of some field invariants. J. Algebra **232**(2), 485–492 (2000)
[10] Kanzaki, T.: Note on quaternion algebras over a commutative ring. Osaka J. Math. **13**(3), 503–512 (1976)
[11] Knus, M.-A., Merkurjev, A., Rost, M., Tignol, J.-P.: The Book of Involutions. American Mathematical Society, Providence (1998) (with a preface in French by J. Tits)
[12] Lam, T.Y., Leep, D.B., Tignol, J.-P.: Biquaternion algebras and quartic extensions. Inst. Hautes Études Sci. Publ. Math. **77**, 63–102 (1993)
[13] Lorenz, M., Reichstein, Z., Rowen, L.H., Saltman, D.J.: Fields of definition for division algebras. J. Lond. Math. Soc. (2) **68**(3), 651–670 (2003)
[14] Reichstein, Z., Youssin, B. : Essential dimensions of algebraic groups and a resolution theorem for G-varieties. Can. J. Math. **52**(5), 1018–1056 (with an appendix by J. Kollár and E. Szabó) (2000)
[15] Rost, M.: Chow groups with coefficients. Doc. Math. **1**(16), 319–393 (electronic) (1996)
[16] Rowen, L.: Central simple algebras. Israel J. Math. **29**(2–3), 285–301 (1978)
[17] Saltman, D.J.: Lectures on Division Algebras, CBMS Regional Conference Series in Mathematics, vol. 94. American Mathematical Society, Providence (1999)
[18] Tignol, J.-P.: Sur les classes de similitude de corps à involution de degré 8. C. R. Acad. Sci. Paris Sér. A-B **286**(20), A875–A876 (1978)
[19] Vial, C.: Operations in milnor k-theory. http://www.math.uiuc.edu/K-theory/0881/ (2008)