manuscripta math. 106, 1 – 12 (2001)

Grégory Berhuy · Christoph Frings

On the second trace form of central simple algebras in characteristic two

Received: 14 September 2000 / Revised version: 18 January 2001

Abstract. Let K be a field and let A be a central simple algebra over K. Let $\mathcal{T}_A$ and $\mathcal{T}_{2,A}$ be respectively the trace form and the second trace form of A. If K has characteristic not two, it is shown in [U] that $\mathcal{T}_{2,A}$ does not give much more information than the usual trace form. If K has characteristic two, the quadratic form $\mathcal{T}_A$ has rank zero. In this article, we show that the second trace form of a central simple algebra A of even degree over a field of characteristic two is non-degenerate and we compute its classical invariants.

Introduction

Let K be a field and let A be a central simple algebra over K. The quadratic forms $\mathcal{T}_A : x \in A \mapsto \mathrm{Trd}_A(x^2)$ and $\mathcal{T}_{2,A} : x \in A \mapsto \mathrm{Srd}_A(x)$ are called respectively *the trace form* and *the second trace form* of A. If K has characteristic not two, the trace form has been studied by many authors (see [B1,B2,L,LM,Se,Ti] for example). In particular, its classical invariants are well-known (see [L,LM,Se] and [Ti]). The second trace form has also been studied in [U] when K has characteristic not two, but it is shown that this form does not give much more information than the usual trace form. When K has characteristic two, the trace form has rank zero. In this article, we show that the second trace form of a central simple algebra A of even degree over a field of characteristic two is non-degenerate and we compute its classical invariants. In the first part, we compute the second trace form of a split algebra. In the second one, we consider the case of cyclic algebras. Finally, we compute the Arf invariant and the Clifford invariant of the second trace form in the general case. The reader will also find in Appendix the proof of an unpublished result of Saltman which is the main ingredient of our work.

Preliminaries

Let A be a central simple algebra over a field K of arbitrary characteristic. If $a \in A$, *the reduced characteristic polynomial of* a, denoted by $\mathrm{Prd}_A(a)$, is defined as follows: let L be a splitting field of A and $\varphi : A \otimes L \to M_n(L)$ a K-isomorphism. Then $\mathrm{Prd}_A(a) := \det(XI_n - \varphi(a \otimes 1))$ is an element of $K[X]$ and is independent

G. Berhuy, C. Frings: UMR 6623 du CNRS, Laboratoire de Mathématiques, Bureau 401B, 16 route de Gray, 25030 Besançon Cedex, France. e-mail: berhuy@math.univ-fcomte.fr; frings@math.univ-fcomte.fr

of the choice of L and φ (cf. [Sc, Chapter 8, §5] for example). Write $\mathrm{Prd}_A(a) = X^n - s_1X^{n-1} + s_2X^{n-2} + \dots$, then $\mathrm{Trd}_A(a) := s_1$ and $\mathrm{Srd}_A(a) := s_2$ are called respectively *the reduced trace* and *the reduced second trace of a*. If $x_1, \cdots, x_n$ are the roots of $\mathrm{Prd}_A(a)$ in an algebraic closure, we have $\mathrm{Trd}_A(a) = x_1 + \cdots + x_n$ and $\mathrm{Srd}_A(a) = \sum\limits_{i<j} x_ix_j$. This easily implies the following equality for the bilinear form $b_{2,A}$ associated to the second trace form when the ground field has characteristic two:

$$b_{2,A}(x, y) := \mathrm{Srd}_A(x + y) + \mathrm{Srd}_A(x) + \mathrm{Srd}_A(y) = \mathrm{Trd}_A(x)\,\mathrm{Trd}_A(y) + \mathrm{Trd}_A(xy)$$

Finally, if A has degree n over K and if L is a maximal commutative subfield of A of degree n (if there is any), then it is well-known that A can be endowed with a structure of right L-vector space and that the map $A \otimes L \to \mathrm{End}_L(A)$, $a \otimes \lambda \mapsto (z \mapsto az\lambda)$ is an isomorphism. In particular, $\mathrm{Prd}_A(a)$ is the characteristic polynomial of the left multiplication by a in the right L-vector space A.

Assume that $\mathrm{char}\, K = 2$. We denote by $\wp(K)$ the set $\{x^2 + x, x \in K\}$. If $\alpha \in K^*$ and $\beta \in K$, we denote by $(\alpha, \beta]$ the class of the corresponding quaternion algebra in the Brauer group. This algebra has a K-basis $1, e, f, ef$ satisfying the relations $e^2 = \alpha$, $f^2 + f = \beta$ and $ef + fe = e$. Moreover, the map $(\alpha, \beta) \in K^*/K^{*2} \times K/\wp(K) \mapsto (\alpha, \beta] \in \mathrm{Br}(K)$ is well defined and bilinear. If $a, b \in K$, we denote by $\mathbb{P}_{a,b}$ the quadratic form $(x, y) \in K^2 \mapsto ax^2 + xy + by^2$. The class of the Clifford algebra of $\mathbb{P}_{a,b}$ in $\mathrm{Br}(K)$ is denoted by $((a, b))$. It is easy to see that $((a, b)) = 0$ if $a = 0$ and $((a, b)) = (a, ab]$ if $a \neq 0$. A non-degenerate quadratic form over K has even rank and is isomorphic to an orthogonal sum of some $\mathbb{P}_{a,b}$. If $q \simeq \mathbb{P}_{a_1,b_1} \perp \cdots \perp \mathbb{P}_{a_r,b_r}$, then *the Arf invariant of q* is the element of $K/\wp(K)$ defined by $\mathrm{Arf}(q) := a_1b_1 + \cdots + a_rb_r$. We also define *the Clifford invariant of q*, denoted by $c(q)$, to be the class of the Clifford algebra of q in the Brauer group. It is easy to see that

$$c(q) = ((a_1, b_1)) + \cdots + ((a_r, b_r)) \in \mathrm{Br}(K)$$

if $q \simeq \mathbb{P}_{a_1,b_1} \perp \cdots \perp \mathbb{P}_{a_r,b_r}$. If L/K is any field extension, $\mathrm{Res}_{L/K}$ denotes the homomorphism $[A] \in \mathrm{Br}(K) \mapsto [A \otimes L] \in \mathrm{Br}(L)$. Then $c(q_L) = \mathrm{Res}_{L/K}(c(q))$.

1. Motivations

Let K be a field of any characteristic. There are two interesting K-algebra structures, namely étale algebras and central simple algebras. In order to classify these algebras up to isomorphism, we need invariants. Since it is quite simple to deal with quadratic forms, one often searches for GrW-invariants.

Definition 1. *Let K be a field. A* GrW-**invariant of étale algebras of rank** n **over** K **(resp. of central simple algebras of degree** n **over** K**)** *is a map $E \mapsto q_E$ (resp. $A \mapsto q_A$), which sends every étale F-algebra of rank n (resp. every central simple F-algebra of degree n) to an element of $GrW(F)$ (the Grothendieck–Witt group of F) for every field extension F/K, and which commutes with scalar extensions.*

For example, $E \mapsto \mathcal{T}_E$, $E \mapsto \mathcal{T}_{2,E}$, $A \mapsto \mathcal{T}_A$ and $A \mapsto \mathcal{T}_{2,A}$ induce GrW-invariants as soon as these forms are non-degenerate.

If $\operatorname{char} K \neq 2$, the trace form invariants have been studied extensively, and the second trace form of central simple algebras has been studied by T. Unger in [U]. The second trace form of étale algebras has not been studied in characteristic not two, but it is easy to show as in [U] that

$$\mathcal{T}_{2,E} \simeq \mathcal{T}_{2,F} \iff \mathcal{T}_E \simeq \mathcal{T}_F$$

Moreover, we have the following result, proved by J.-P. Serre (unpublished):

Theorem 1 (Serre, unpublished). *Let K be a field of characteristic not two and let $E \mapsto q_E$ be a* GrW*-invariant of étale algebras of rank n over K. Then*

$$q_E \simeq \sum_{i=0}^{m} \lambda_i \Lambda^i \mathcal{T}_E$$

where $m = \left[\frac{n}{2}\right]$ denotes the integral part of $\frac{n}{2}$ and λ_i is an element of $\mathrm{GrW}(K)$.

In other words, the trace form is essentially the only GrW-invariant of étale algebras in characteristic not two.

If $\operatorname{char} K = 2$, $\mathcal{T}_E$ and $\mathcal{T}_A$ have rank zero. In the case of étale algebras, the second trace form is non-degenerate if and only if n is even (see [BM, Proposition 2.1 (ii)]). Then Bergé and Martinet proved the following result (see [BM, Theorem 5.1]):

Theorem 2 (Bergé-Martinet, [BM]). *Let K be a field of characteristic 2, and let E be an étale algebra of rank $2m$ over K. Then*

$$\mathcal{T}_{2,E} \simeq \mathbb{P}_{1,\mathrm{Arf}(E/K)} \perp (m-1) \times \mathbb{P}_{0,0}$$

where $\mathrm{Arf}(E/K)$ *is the* Arf *invariant of the second trace form of E/K.*

For two reasons, this theorem says that the second trace form is a very poor substitute for the trace form in characteristic two. The first reason is that this result implies in particular that $c(\mathcal{T}_{2,E}) = 0$ for any étale algebra of even rank. This is no longer true if $\operatorname{char} K \neq 2$. For example, an easy computation shows that $c(\mathcal{T}_{2,E})$ is the class of the quaternion algebra (a, b) if E is the biquadratic extension $k(\sqrt{a}, \sqrt{b})$.

The second, obvious, reason is that the second trace form is uniquely determined by its Arf-invariant (up to isomorphism), contrary to what happens in characteristic $\neq 2$.

Remark 1. In [Be] Berlekamp defined an invariant for finite separable extensions of fields of characteristic 2 – similar to the usual discriminant in characteristic $\neq 2$ – in the following way: let L/K be a separable field extension of finite degree n and η_0 a primitive element of L over K (such that $L = K(\eta_0)$). Consider the conjugates η_i, $0 \leq i \leq n-1$ of η_0 and define the *Berlekamp-invariant of L/K* (or *additive discriminant* as we will call it according to [BM]) $d^+_{L/K}$ by

$$d^+_{L/K} = \sum_{i<j} \frac{\eta_i \eta_j}{(\eta_i + \eta_j)^2} \in K/\wp(K).$$

This discriminant can be extended to étale algebras in an obvious way and is related to the Arf-invariant of the second trace form by the following formula:

$$d^{+}_{E/K} = \mathrm{Arf}(E'/K) + \varepsilon_n$$

where $E' = E$ (resp. $E \times K$) if n is even (resp. n is odd), and ε_n is the element in $\{0, 1\}$ representing the congruence class of $[\frac{n}{4}]$ modulo 2 (resp. $[\frac{n+1}{4}]$) if n is even (resp. if n is odd). See [BM,W] or [Wa] for more details.

Thus the additive discriminant $d^{+}_{E/K}$ determines uniquely the isomorphism class of the second trace form of E/K.

Now consider the GrW-invariants of central simple algebras.

Let $A \mapsto q_A$ be a GrW-invariant. If n is an odd integer, we have $q_A \simeq q_{M_n(K)}$ for any central simple algebra of degree n. Indeed, in this case A has a splitting field L/K of odd degree, so we have

$$q_A \otimes L \simeq q_{A\otimes L} \simeq q_{M_n(L)} \simeq q_{M_n(K)} \otimes L$$

and we conclude by Springer's theorem (which also holds in characteristic two, see [Re, lemma p. 231], for example).

Now assume that n is even. In [Ti,LM,U] and [Se], it is shown that

$$c(q_A) = c(q_{M_n(K)}) + \frac{n}{2}[A]$$

when $q_A = \mathcal{T}_A$ or $\mathcal{T}_{2,A}$ and char $K \neq 2$. In Sect. 4, we show that this formula holds for the second trace form in characteristic two. This means that the second trace form is an equivalent substitute to the trace form in characteristic two, in opposition to the case of étale algebras. It can be explained by the fact that the crucial point in the proof of the result of Bergé-Martinet is that an étale algebra is commutative.

2. The split case

Since we are in the split case, the reduced characteristic polynomial of a matrix M coincides with its usual characteristic polynomial, and will be denoted by $\chi(M)$.

Proposition 1. *Let K be a field of characteristic two, $n = 2m \geq 2$ an even integer and $A = M_n(K)$. Then*

$$\mathcal{T}_{2,A} \simeq \left[\frac{m}{2}\right] \times \mathbb{P}_{1,1} \perp (2m^2 - \left[\frac{m}{2}\right]) \times \mathbb{P}_{0,0}.$$

Proof. Let $(E_{i,j})$ be the standard basis of A. We will write E_i instead of $E_{i,i}$. For $1 \leq k \leq m$, let

$$F_{2k-1} := E_1 + \cdots + E_{2k-2} + E_{2k-1} \text{ and } F_{2k} := E_1 + \cdots + E_{2k-2} + E_{2k}.$$

Using the fact that the bilinear form $b_{2,A}$ associated to the second trace form satisfies $b_{2,A}(x, y) = \mathrm{Trd}_A(x)\,\mathrm{Trd}_A(y) + \mathrm{Trd}_A(xy)$, it is easy to see that putting together the

symplectic pairs $(E_{i,j}, E_{j,i}), i < j, (F_{2k-1}, F_{2k}), 1 \leq k \leq m$ gives a symplectic basis for $\mathcal{T}_{2,A}$.
Moreover, we have $\chi(E_{i,j}) = X^n$, so $\mathrm{Srd}_A(E_{i,j}) = 0$. We also get
$\chi(F_{2k}) = \chi(F_{2k-1}) = (X+1)^{2k-1}X^{n-2k+1}$, so we have

$$\mathcal{T}_{2,A}(F_{2k-1}) = \mathcal{T}_{2,A}(F_{2k}) = \binom{2k-1}{2k-3} = \binom{2k-1}{2} = (2k-1)(k-1) = k-1.$$

This finishes the proof. □

Corollary 1. *Let K be a field of characteristic two, $n \geq 2$ an even integer and A a central simple algebra of degree n. Then $\mathcal{T}_{2,A}$ is a non-degenerate quadratic form over K.*

Proof. Let L be any splitting field of A. We have

$$\mathcal{T}_{2,A} \otimes L \simeq \mathcal{T}_{2,A\otimes L} \simeq \mathcal{T}_{2,M_n(L)}$$

By Proposition 1, the latter form is non-degenerate, so is $\mathcal{T}_{2,A}$.

3. The cyclic case

We recall first the definition of a cyclic algebra. Let E/K be a cyclic extension of degree n, σ a generator of the Galois group and $a \in K^*$. The K-vector space

$$(a, E/K, \sigma) := \bigoplus_{i=0}^{n-1} Ee^i$$

with the multiplication law $e^n = a$ and $e\lambda = \lambda^\sigma e, \lambda \in E$ is a central simple algebra of degree n over K, called a *cyclic algebra*, which contains E as a maximal commutative subfield. The cyclic algebra $(1, E/K, \sigma)$ is split (see [Sc], Chapter 8, §12 for example).

Proposition 2. *Let K be a field of characteristic two, $n = 2m \geq 2$ and $A = (a, E/K, \sigma)$ a cyclic algebra of degree n. Then we have*

$$\mathcal{T}_{2,A} \simeq \left[\frac{m}{2}\right] \times \mathbb{P}_{a^{-1},a} \perp \mathbb{P}_{1,\mathrm{Arf}(E/K)} \perp \mathbb{P}_{a^{-1},a\,\mathrm{Arf}(E/K)} \perp \left(2m^2 - 2 - \left[\frac{m}{2}\right]\right) \times \mathbb{P}_{0,0}$$

where $\mathrm{Arf}(E/K)$ *is the Arf invariant of the second trace form of the field extension E/K.*

Proof. • If $x = \lambda_0 + \lambda_1 e + \cdots + \lambda_{n-1}e^{n-1}$, then $\mathrm{Trd}_A(x) = \mathrm{Tr}_{E/K}(\lambda_0)$. Indeed, we have seen that $\mathrm{Trd}_A(x)$ is the trace of left mutiplication by x in A, considered as a right E-vector space. Since we have $xe^j = \lambda_0 e^j + \cdots = e^j\lambda_0^{\sigma^{n-j}} + \cdots$, we get

$$\mathrm{Trd}_A(x) = \sum_{j=0}^{n-1} \lambda_0^{\sigma^{n-j}} = \mathrm{Tr}_{E/K}(\lambda_0).$$

It follows easily that we have the following orthogonal decomposition of the K-vector space A with respect to $\mathcal{T}_{2,A}$: $A = E \oplus Ee^m \oplus M$,
where $M = \langle \lambda e^k, \lambda \in E, k \neq 0, m \rangle$, using the formula

$$b_{2,A}(x, y) = \mathrm{Trd}_A(x)\,\mathrm{Trd}_A(y) + \mathrm{Trd}_A(xy).$$

- Now we study the restriction of the second trace form to the three spaces E, Ee^m and M. For this, we first compute the matrix $S = (s_{ij})_{0 \leq i, j \leq n-1}$ of left multiplication by $\lambda e^k, 0 \leq k \leq m, \lambda \in E$. If $k = 0$, then we have $S = \mathrm{diag}\langle \lambda, \lambda^{\sigma^{n-1}}, \ldots, \lambda^{\sigma} \rangle$. Thus we get $\mathrm{Srd}_A(\lambda) = \mathrm{Srd}_E(\lambda)$, i.e. $\mathcal{T}_{2,A}|_E \simeq \mathcal{T}_{2,E}$. Assume now that $1 \leq k \leq m$. We have $\lambda e^k e^j = e^{k+j} \lambda^{\sigma^{-k-j}}$, thus

$$\begin{cases} s_{k+j,j} = \lambda^{\sigma^{-k-j}} & \text{if } 0 \leq j \leq n-k-1, \\ s_{k+j-n,j} = a\lambda^{\sigma^{-k-j}} & \text{if } n-k \leq j \leq n-1, \\ s_{i,j} = 0 & \text{otherwise.} \end{cases}$$

For any matrix $C = (c_{i,j})_{0 \leq i, j \leq n-1}$, we know that

$$\det C = \sum_{\tau \in S_n} \varepsilon(\tau) c_{0,\tau(0)} \cdots c_{n-1,\tau(n-1)}$$

where $\varepsilon(\tau)$ denotes the signature of τ. Since we want to compute the coefficient corresponding to X^{n-2} in the expansion of $\det(XI_n - S)$, we have to sum over the elements of S_n which have exactly $n-2$ fixed points, namely the transpositions. So we get

$$\mathrm{Srd}_A(\lambda e^k) = \sum_{i>j} s_{i,j} s_{j,i} = \sum_{j=0}^{n-k-1} s_{k+j,j} s_{j,j+k}.$$

If $i < j$, we have $s_{i,j} \neq 0$ if and only if $i = k + j - n$. In particular, $s_{j,j+k} \neq 0$ if and only if $j = 2k + j - n$, *i.e.* $k = m$. Thus $\mathrm{Srd}_A(\lambda e^k) = 0$ for $1 \leq k \leq m-1$. Since we have $b_{2,A}(\lambda e^i, \mu e^j) = 0$ for $\lambda, \mu \in E$ and $1 \leq i, j \leq m-1$, we finally get that the restriction of the second trace form to the subspace $H := \langle \lambda e^k, \lambda \in E, k = 1, \ldots, m-1 \rangle$ is zero. So M is metabolic because H is a subspace of M satisfying $\dim_K H = \frac{1}{2} \dim_K M$. In particular, $\mathcal{T}_{2,A}|_M$ is hyperbolic. Moreover we have $\mathrm{Srd}_A(\lambda e^m) = a \sum_{j=0}^{m-1} \lambda^{\sigma^{-j}} \lambda^{\sigma^{-m-j}}$.

Finally we have obtained

$$\mathcal{T}_{2,A} \simeq \mathcal{T}_{2,E} \perp aq \perp h,$$

where q is the quadratic form $\lambda \in E \mapsto \sum_{j=0}^{m-1} \lambda^{\sigma^{-j}} \lambda^{\sigma^{-m-j}}$ and h is hyperbolic.

- If $a = 1$, the algebra A is split, so we get $\mathcal{T}_{2,E} \perp q \sim \left[\frac{m}{2}\right] \times \mathbb{P}_{1,1}$ by Proposition 1 and the previous point, where $\sim$ denotes the Witt-equivalence of quadratic forms. By Theorem 2, we have $\mathcal{T}_{2,E} \sim \mathbb{P}_{1,\mathrm{Arf}(E/K)}$, so

$$q \sim \mathbb{P}_{1,\mathrm{Arf}(E/K)} \perp \left[\frac{m}{2}\right] \times \mathbb{P}_{1,1}.$$

Using the fact that $a\mathbb{P}_{u,v} \simeq \mathbb{P}_{\frac{u}{a},av}$ if $a \in K^*$ and $u, v, \in K$, we get the result.

4. The general case

Theorem 3. *Let K be a field of characteristic two, $n \geq 2$ an even integer and A a central simple algebra of degree n over K. Then we have:*

(1) $\mathrm{Arf}(\mathcal{T}_{2,A}) = \left[\frac{n}{4}\right]$
(2) $c(\mathcal{T}_{2,A}) = \frac{n}{2}[A]$

Before proving the theorem, we want to recall further results. Let K be a field and A a central simple algebra of degree n over K. Fix a K-basis $e_1, \dots, e_{n^2}$ of A and let $n_A(X_1, \dots, X_{n^2}) := \mathrm{Nrd}_A(X_1e_1 + \cdots + X_{n^2}e_{n^2})$. This polynomial is absolutely irreducible, so $R_A := K[X_1, \dots, X_{n^2}]/(n_A)$ is a domain.

Proposition 3. *The quotient field $K(A)$ of R_A has the following properties:*

(a) *$K(A)$ splits A,*
(b) *K is algebraically closed in $K(A)$,*
(c) $\mathrm{Ker}\,\mathrm{Res}_{K(A)/K} = \langle [A] \rangle$.

The proof of (a) can be found in [S1], and (b) is proved in [L, p. 369]. Moreover, it is shown in [S1] that $K(A)$ is a rational extension of the field $K(\nu_A)$ of rational functions of the Severi-Brauer variety of A, so $\mathrm{Res}_{K(A)/K(\nu_A)}$ is an injection (see [J, Theorem 3.8.6] for example).
Since $\mathrm{Ker}\,\mathrm{Res}_{K(\nu_A)/K} = \langle [A] \rangle$ (see [Am, Theorem 9.3 and Theorem 12.1]) and $\mathrm{Res}_{K(A)/K} = \mathrm{Res}_{K(A)/K(\nu_A)} \circ \mathrm{Res}_{K(\nu_A)/K}$, we get assertion (c).
The following theorem is due to Saltman, and will be proved in Appendix:

Theorem 4 (Saltman, unpublished). *Let K be a field, A a central simple algebra of degree n over K and G a finite group of order n. Then there exists a field extension L_G/K such that:*

(1) *$A \otimes L_G$ is isomorphic to a G-crossed product,*
(2) $\mathrm{Res}_{L_G/K}$ *is an injection.*

Proof of Theorem 3. • Let us prove assertion (1). If L/K is a field extension, the inclusion $K \subseteq L$ induces a map $\iota_{L/K} : K/\wp(K) \to L/\wp(L)$. Then we have

$$\mathrm{Arf}(q_L) = \iota_{L/K}(\mathrm{Arf}(q))$$

for any quadratic form over K. Moreover $\iota_{K(A)/K}$ is an injection. Indeed, if $x \in K(A)$ satisfies $x = \lambda + \lambda^2$ for some $\lambda \in K(A)$, then λ is an element of $K(A)$ which is algebraic over K, so $\lambda \in K$ by Proposition 3 (b), i.e. $x \in \wp(K)$.

Since we have

$$\begin{aligned}\iota_{K(A)/K}(\mathrm{Arf}(\mathcal{T}_{2,A})) &= \mathrm{Arf}(\mathcal{T}_{2,A} \otimes K(A)) = \mathrm{Arf}(\mathcal{T}_{2,A\otimes K(A)})\\ &= \mathrm{Arf}(\mathcal{T}_{2,M_n(K(A))}) \text{ (by Proposition 3 (a))}\\ &= \mathrm{Arf}(\mathcal{T}_{2,M_n(K)\otimes K(A)}) = \mathrm{Arf}(\mathcal{T}_{2,M_n(K)} \otimes K(A))\\ &= \iota_{K(A)/K}(\mathrm{Arf}(\mathcal{T}_{2,M_n(K)})),\end{aligned}$$

we get the result using Proposition 1 and the injectivity of $\iota_{K(A)/K}$.

• Now we prove (2) for cyclic algebras. Using Proposition 2, we get

$$\begin{aligned}c(\mathcal{T}_{2,A}) &= (1, \mathrm{Arf}(E/K)] + \left[\frac{n}{4}\right](a^{-1}, 1] + (a^{-1}, \mathrm{Arf}(E/K)]\\ &= (a, \left[\frac{n}{4}\right] + \mathrm{Arf}(E/K)].\end{aligned}$$

Since n is even, we have $\left[\frac{n}{4}\right] = \varepsilon_n + 2l$, for a suitable integer l, so

$$\begin{aligned}c(\mathcal{T}_{2,A}) &= (a, d_E^+ + 2l]\\ &= (a, d_E^+] + 2(a, l]\\ &= (a, d_E^+],\end{aligned}$$

since a quaternion algebra has order at most 2 in $\mathrm{Br}(K)$. By [J], Corollary 2.13.20, we have $\frac{n}{2}[A] = (a, F/K, \sigma|_F)$, where F is the unique quadratic subfield of E.

We now recall how to associate a separable field extension of degree at most 2 to an étale algebra over a field K of any characteristic: if E is an étale algebra over K of rank n, let H be the set of the n K-homomorphisms from E to K_s. Then $\mathrm{Gal}(K_s/K)$ acts on H by left multiplication. Now define $\tilde{E}$ to be the subfield of K_s fixed by the elements $s \in \mathrm{Gal}(K_s/K)$ inducing an even permutation on H. Then $\tilde{E}/K$ is a separable field extension of degree at most 2. If char $K = 2$, it is shown in [BM, Theorem 2.6.], that this extension is defined by d_E^+, i.e. $\tilde{E}$ is generated by an element $x \in K_s$ satisfying $x^2 + x + d_E^+ = 0$ (if char $K \neq 2$, one can show that $\tilde{E} = K(\sqrt{d_E})$, where $d_E := \det \mathcal{T}_E$ is the classical discriminant).

We now prove that in our case, we have $\tilde{E} = F$. Here E/K is a Galois field extension, so $h(E) \subseteq E$ for every $h \in H$ and we have in fact $H = \mathrm{Gal}(E/K)$. In particular, $sh = h$ for $s \in \mathrm{Gal}(K_s/E)$ and $h \in H$, so every element of $\mathrm{Gal}(K_s/E)$ induced the trivial permutation on H, which is even. This implies that any element of $\tilde{E}$ is fixed by $\mathrm{Gal}(K_s/E)$, so $\tilde{E}$ is a subfield of E. Since E/K is cyclic, the generator σ of $\mathrm{Gal}(E/K)$ permutes cyclically the elements of $\mathrm{Gal}(E/K)$, and this permutation is odd (since it is a n-cycle with n even). In particular, the subgroup of $\mathrm{Gal}(K_s/K)$ which is used to define $\tilde{E}$ is not the full absolute Galois group (since it

does not contain any extension of σ to K_s), so $[\tilde{E} : K] = 2$. Hence $\tilde{E}$ is a quadratic subfield of E. Since E/K is cyclic of even degree, E contains a unique quadratic subfield, so $\tilde{E} = F$.
We finally obtain $\frac{n}{2}[A] = (a, \tilde{E}/K, \sigma|_{\tilde{E}})$. It is immediate to check that this algebra is $(a, d_E^+]$.

Now let A be any central simple algebra of degree n over K. Using Theorem 2 with G cyclic, we get a field extension L_G/K such that $A \otimes L_G$ is a cyclic algebra and $\mathrm{Res}_{L_G/K}$ is an injection. Since we have

$$\begin{aligned}\mathrm{Res}_{L_G/K}(c(\mathcal{T}_{2,A})) &= c(\mathcal{T}_{2,A} \otimes L_G) = c(\mathcal{T}_{2,A\otimes L_G})\\ &= \frac{n}{2}[A \otimes L_G] = \mathrm{Res}_{L_G/K}\left(\frac{n}{2}[A]\right),\end{aligned}$$

we get the result. □

Remark 2. As in [U,LM,Ti] and [Se], we obtain

$$c(\mathcal{T}_{2,A}) = c(\mathcal{T}_{2,M_n(K)}) + r_n[A]$$

for any central simple algebra of even degree n, where r_n is an integer which only depends on n. This is not very surprising, and can be explained as follows: let $A \mapsto q_A$ be a GrW-invariant of central simple K-algebras, where K is a field of any characteristic. Assume that q_A is a quadratic form for every central simple algebra A of degree n. We easily get that $c(q_A) - c(q_{M_n(K)}) \in \mathrm{Ker}\,\mathrm{Res}_{K(A)/K}$, so $c(q_A) = c(q_{M_n(K)}) + r(A)[A]$. Replacing A by the generic division algebra $UD := UD(K, n, r)$ of degree n over K (see for example [S2, Sect. 14]) and K by its center, we get $c(q_{UD}) = c(q_{M_n(K)}) + r(UD)[UD]$. By [Ro, Theorem 1], we have $\exp(UD) = n$. So $r(UD)$ is a multiple of $\frac{n}{2}$ and we have $r(UD)[UD] = r_n[UD]$, with $r_n = 0$ or $\frac{n}{2}$, since $[UD]$ is killed by n. Thus $c(q_A) = c(q_{M_n(k)}) + r_n[UD]$. Since any central simple algebra can be obtained by specialization of UD (see [S2, Sect. 14]), we get $c(q_A) = c(q_{M_n}(K)) + r_n[A]$ for any central simple algebra of degree n over K, where $r_n = 0$ or $\frac{n}{2}$. It is also easy to show that $\det q_A = \det q_{M_n(k)}$ (or $\mathrm{Arf}(q_A) = \mathrm{Arf}(q_{M_n(K)})$ if char $K = 2$). This method has first been applied by Saltman to compute the Clifford invariant of the trace form of a central simple algebra when char $K \neq 2$ (unpublished).

Appendix: Proof of Theorem 4

In this appendix, we want to give a proof of Theorem 4, since Saltman never published his result, which is nevertheless of independent interest.

We first recall the notion of *generic G-crossed product*, defined by Saltman in [S2, Sect. 12, p. 84].

Let K be any field and G a finite group of order n. Consider the following short exact sequence

$$0 \to M \to \bigoplus_{g\in G} \mathbb{Z}[G]d_g \xrightarrow{f} \mathbb{Z}[G]$$

where f is $\mathbb{Z}[G]$-linear and maps d_g to $g-1$. Then M is a finitely generated $\mathbb{Z}[G]$-module, which is free as a $\mathbb{Z}$-module. We will write it multiplicatively. Now let $c(g,h) := gd_h + d_g - d_{gh} \in M$ for $g,h \in G$. We extend the action of G on the group algebra $K[M]$ by K-linearity. This action extends naturally on the quotient field $K(M)$ of $K[M]$. Then $M \subseteq K(M)^*$ and c is a 2-cocycle of G with values in $K(M)^*$. If $K' := K(M)^G$, the crossed product $E_G := (K(M)/K', G, c)$ is called *the generic G-crossed product over K*. Before proving Theorem 4, we need the following proposition:

Proposition 4. *The generic G-crossed product has exponent n, i.e. $[E_G]$ has order n in* $\mathrm{Br}(K')$.

Proof. This is equivalent to show that $[c]$ has order n in $H^2(G, K(M)^*)$.

- We first prove that the map $H^2(G,M) \to H^2(G, K(M)^*)$ is injective. Since $M \simeq \mathbb{Z}^r$ as an abelian group, we have

$$K[M] = K[m_1, m_1^{-1}, \cdots, m_r, m_r^{-1}]$$

where (m_i) is a basis of M. In particular, $K[M]$ is a unique factorization domain. So the primes of $K[M]$ form a basis of $K(M)^*/K[M]^*$. Moreover, it is easy to see that G preserves the set of primes up to units. So G permutes the elements of the basis of $K(M)^*/K[M]^*$. For each orbit ω of $K(M)^*/K[M]^*$ under this action, choose a representative p_ω and let H_ω be the stabilizer of p_ω. Then we have

$$K(M)^*/K[M]^* \simeq \bigoplus_{\omega} \mathbb{Z}[G/H_\omega]$$

as G-modules.

By Shapiro's lemma, we have $H^1(G, \mathbb{Z}[G/H_\omega]) = H^1(H_\omega, \mathbb{Z})$. Here G acts trivially on $\mathbb{Z}$, so $H^1(\mathbb{Z}[G/\mathrm{H}_\omega]) = \mathrm{Hom}(H_\omega, \mathbb{Z}) = 0$ since H_ω is finite. Finally we get

$$H^1(G, K(M)^*/K[M]^*) = 0.$$

Using the long exact sequence of group cohomology induced by the short exact sequence

$$0 \to K[M]^* \to K(M)^* \to K(M)^*/K[M]^* \to 0$$

we get that the map $H^2(G, K[M]^*) \to H^2(G, K(M)^*)$ is injective. Moreover $K[M]^*$ is the set of monomials with leading coefficient in K^*. Then it is easy to see that $K[M]^* = K^* \oplus M$ as G-modules. So we have

$$H^2(G, K[M]^*) = H^2(G, K^*) \oplus H^2(G, M)$$

and the map $H^2(G,M) \to H^2(G, K[M]^*)$ is injective. We get the desired conclusion by composition with the previous injective map. Notice that the injectivity of the map $H^2(G, K[M]^*) \to H^2(G, K(M)^*)$ can also be obtained as a particular case of [S2], Theorem 12.4 (a) (untwisted case).

• By the previous point, it suffices to show that $[c]$ has order n in $H^2(G, M)$. Let $t : \mathbb{Z}[G] \to \mathbb{Z}$ be the $\mathbb{Z}$-linear map which sends g to 1. Then $(g-1)_{g\in G}$ is a basis of $\operatorname{Ker} t$ and we have the following exact sequence

$$0 \to M \to \bigoplus_{g\in G} \mathbb{Z}[G]d_g \xrightarrow{f} \operatorname{Ker} t \to 0.$$

Since every free $\mathbb{Z}[G]$-module is cohomologically trivial (apply Shapiro's lemma to the trivial subgroup), the long exact sequence of cohomology gives that the connecting map

$$\partial : H^1(G, \operatorname{Ker} t) \to H^2(G, M)$$

is an isomorphism. If α is the 1-cocycle $g \mapsto g-1$, then $\partial([\alpha]) = [c]$, so it remains to show that $[\alpha]$ has order n in $H^1(G, \operatorname{Ker} t)$.

• Taking the long exact sequence of cohomology associated to

$$0 \to \operatorname{Ker} t \to \mathbb{Z}[G] \to \mathbb{Z} \to 0$$

we get

$$H^0(G, \mathbb{Z}[G]) \xrightarrow{t^*} H^0(G, \mathbb{Z}) \xrightarrow{\partial} H^1(G, \operatorname{Ker} t) \to 0.$$

It is easy to see that $H^0(G, \mathbb{Z}[G]) = \mathbb{Z} \sum_{g\in G} g$, so $\operatorname{Im} t^* = n\mathbb{Z}$ and we finally get $H^1(G, \operatorname{Ker} t) \simeq \mathbb{Z}/n\mathbb{Z}$. But $[\alpha]$ corresponds precisely to the image of 1 in $\mathbb{Z}/n\mathbb{Z}$, which has order n. This finishes the proof. □

Now we are ready to prove Theorem 4. Let $L_G = K'((A \otimes_K K') \otimes_{K'} E_G^{op})$. By Proposition 3 (a), we have $A \otimes_K L_G \simeq E_G \otimes_{K'} L_G$. By [J], Theorem 2.13.16 for example, we know that $E_G \otimes_{K'} L_G$ is Brauer-equivalent to a G'-crossed product over L_G, where $G' = \operatorname{Gal}(L_G K(M)/L_G)$. Since K' is algebraically closed in L_G, we have $L_G \bigcap K(M) = K'$, since an element of L_G which belongs to this intersection is algebraic over K'. Since $K(M)/K'$ is a Galois extension, this implies that L_G and $K(M)$ are linearly disjoint over K'. In particular, $[L_G K(M) : L_G] = n$ and $\operatorname{Gal}(L_G K(M)/L_G) \simeq G$.
Finally, $A \otimes_K L_G$ is Brauer-equivalent to a G-crossed product. Since the degrees are equal, we get the desired isomorphism.

We know prove that $\operatorname{Res}_{L_G/K}$ is an injection. We have

$$\operatorname{Res}_{K(M)/K} = \operatorname{Res}_{K(M)/K'} \circ \operatorname{Res}_{K'/K}.$$

Notice that $K(M)/K$ is rational. Indeed, since $M \simeq \mathbb{Z}^l$ as a $\mathbb{Z}$-module, we have $K[M] \simeq K[X_1, X_1^{-1}, \cdots, X_l, X_l^{-1}]$, so $K(M) \simeq K(X_1, \cdots, X_l)$. Consequently $\operatorname{Res}_{K(M)/K}$ is an injection, so $\operatorname{Res}_{K'/K}$ is an injection.
Since $\operatorname{Res}_{L_G/K} = \operatorname{Res}_{L_G/K'} \circ \operatorname{Res}_{K'/K}$, we get

$$\operatorname{Ker} \operatorname{Res}_{L_G/K} = \operatorname{Br}(K) \cap \langle [(A \otimes_K K') \otimes_{K'} E_G^{op}] \rangle$$

by Proposition 3 (c). Let $[B] = r[A \otimes_K K') \otimes_{K'} E_G^{op}]$ be an element of this kernel. Let $\tilde{K} = K'\overline{K} = \overline{K}(M)^G$, where $\overline{K}$ is an algebraic closure of K. Since $[B] \in \operatorname{Br}(K)$ and $\tilde{K}$ contains $\overline{K}$, we have $[B \otimes_K \tilde{K}] = 0$. On the other hand, we have $[B \otimes_K \tilde{K}] = r[E_G^{op} \otimes_{K'} \tilde{K}] = -r[E_G \otimes_{K'} \tilde{K}]$, since $\tilde{K}$ splits $A \in \mathrm{Br}(K)$. So we have $r[E_G \otimes_{K'} \tilde{K}] = 0$. Since $E_G \otimes_{K'} \tilde{K}$ is the generic G-crossed product over $\overline{K}$, which has order n in $\mathrm{Br}(\tilde{K})$, we get $n|r$. Now $A \otimes_K K'$ and E_G^{op} have degree n over K', so $[B] = 0$.

Acknowledgements. This work is supported by the TMR research network (ERB FMRX CT-97-0107) on “K-theory and algebraic groups”.

The authors are very grateful to Pr. Saltman for patiently answering their numerous questions on his unpublished result and several other topics.

References

[Am] Amitsur, S.A.: Generic splitting fields of central simple algebras. Ann. Math. **62**, 8–43 (1955)

[B1] Berhuy, G.: Autour des formes trace des algèbres cycliques. to appear in Pub. Math. de Besançon, Théorie des nombres

[B2] Berhuy, G.: Trace forms of central simple algebras over a local field or a global field. Preprint

[Be] Berlekamp, E.: An Analogue to the Discriminant over Fields of Characteristic Two, J. Algebra **38**, 315–317 (1976)

[BM] Bergé, A.-M., Martinet, J.: Formes quadratiques et extensions en caractéristique 2. Ann. Inst. Fourier Grenoble **35**, 57–77 (1985)

[J] Jacobson, A.: *Finite-Dimensional Algebras over Fields.* Berlin–Heidelberg–New York: Springer-Verlag 1996

[L] Lewis, D.W.: Trace forms of central simple algebras. Math.Z. **215**, 367–375 (1994)

[LM] Lewis, D.W., Morales, J.: The Hasse invariant of the trace form of a central simple algebra. Pub. Math. de Besançon, Théorie des nombres, 1–6 (1993/94)

[Re] Revoy, Ph.: Remarques sur la forme trace. Linear Mult. Algebra **10**, 223–233 (1981)

[Ro] Rowen, L.H: Universal PI-algebras and algebras of generic matrices, Israel J. Math. **(18)**, 65–74 (1974)

[S1] Saltman, D.: Norm polynomials and algebras. J. of Algebra **62**, 333–345 (1980)

[S2] Saltman, D.: *Lectures on division algebras.* Conference board of the mathematical science: regional conference series in maths. Providence, RI: AMS, 1999

[Sc] Scharlau, W.: *Quadratic and hermitian forms.* Grundlehren Math. Wiss. **270**. Berlin–Heidelberg–New York: Springer-Verlag, 1985

[Se] Serre, J.-P.: *Cohomologie galoisienne.* Cinquième édition, Lecture Notes in Mathematics **5**. Berlin–Heidelberg–New York: Springer-Verlag, 1994

[Ti] Tignol, J.-P.: La norme des espaces quadratiques et la forme trace des algèbres simples centrales. Pub.Math.Besançon, Théorie des nombres (92/93–93/94)

[U] Unger, T.: A note on surrogate forms of central simple algebras. Mathematical Proceedings of the Royal Irish Academy (to appear)

[W] Wadsworth, A.: Discriminants in characteristic 2. Linear. Mult. Algebra **17**, 235–263 (1985)

[Wa] Waterhouse, W.C.: Discriminants of étale algebras and related structures. J. reine angew. Math. **379**, 209–220 (1987)