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

Grégory Berhuy, Christoph Frings

U.M.R.6623 du C.N.R.S., Laboratoire de Mathématiques, Bureau 401B, 16 route de Gray, F-25030 Besançon cedex, France

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 $\mathcal{T}_{2,A} : x \in A \mapsto \mathrm{T}_{2,A}(x)$ 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 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 The reader will also find in Appendix the proof of an unpublished result of Saltman which is the main ingredient of our work.

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

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 of the choice of L and φ (cf.[Sc], chapter 8, §5 for example). If $\mathrm{Prd}_A(a) = X^n - s_1X^{n-1} + s_2X^{n-2} + \dots$, then $\mathrm{Trd}_A(a) := s_1$ and $\mathrm{T}_{2,A}(a) := s_2$ 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 $\mathrm{T}_{2,A}(a) = \sum\limits_{i<j} x_i x_j$. 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:

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

Finally, if L is a maximal commutative subfield of A (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 $A \otimes L \longrightarrow \mathrm{End}_L(A), a \otimes \lambda \mapsto (z \mapsto az\lambda)$ 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 $ef + fe = f$. 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

For any real number x, denote by $[x]$ its integral part.

Let K be a field of any characteristic. There are two interesting structures of K-algebras, namely étale algebras and central simple algebras. In order to classify these algebras up to isomorphism, we need invariants. Since it is relatively simple to deal with quadratic forms, one even search quadratic invariants. Let us recall their definition.

Definition: Let K be a field. *A quadratic invariant of étale algebras of rank n over K (resp. of central simple algebras of degree n over K)* is a function $E \mapsto q_E$ (resp. $A \mapsto q_A$), which maps every étale F-algebra of rank n (resp. every central simple F-algebra of degree n) to a non-degenerate quadratic form over 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 $A \mapsto \mathcal{T}_{2,A}$ are quadratic 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 does not have 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: Let K be a field of characteristic not two and let $E \mapsto q_E$ be a quadratic 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 $m = \left[\dfrac{n}{2}\right]$ and λ_i is a quadratic form over K.

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

If $\operatorname{char} K = 2$, $\mathcal{T}_{2,E}$ 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: Let K be a field of characteristic 2, and let E be an étale algebra of rank $2m$ over K. Then

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

where $\operatorname{Arf}(E/K)$ 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 bad 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 $\mathrm{char}\, K \neq 2$. For example, easy computation shows that $c(\mathcal{T}_{2,E})$ is the class of the quaternion algebra (a, b) if E is the biquadratic extension $k(\sqrt{a}, \sqrt{b})$.
Moreover, we can associate to E its *additive discriminant* as follows, when K has characteristic 2: let $E' := E$ if n is even and $E' := E \times K$ if n is odd. Then $Q' := \mathcal{T}_{2,E'}$ is non-degenerate. Define ε_n to be the unique element of $\{0, 1\}$ which represents the class of $\left[\dfrac{m}{2}\right]$ mod 2, if $n = 2m$ or $2m-1$ (one can show easily that this definition of ε_n coincides with the definition of [BM], (2.1)). Then the element

$$d_E^+ := \mathrm{Arf}(Q') + \varepsilon_n \in K/\wp(K)$$

is called *the additive discriminant of E.*
So theorem 2 says that the trace form is uniquely determined by the additive discriminant, which is not the case in characteristic not two. It seems that we get nowhere, because the additive discriminant is defined using $\mathrm{Arf}(E/K)$ (when n is even), but it is not the case, since as for the classical discriminant, one can compute d_E^+ using conjugates of a suitable element. Indeed, d_E^+ is additive with respect to the direct product of étale algebras (see [BM], remark 2.4). Moreover, if E/K is a field generated by a primitive element γ, and if $\gamma_1, \cdots, \gamma_n$ are the conjugates of γ, then

$$d_E^+ = \sum_{i<j} \frac{\gamma_i \gamma_j}{(\gamma_i + \gamma_j)^2}$$

(see [BM], proof of theorem 2.6).

Now consider the quadratic invariants of central simple algebras.

Let $A \mapsto q_A$ a quadratic invariant. If n is odd, 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] 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 section 4, we show that this formula holds for the second trace form in characteristic two. This is not very surprising, as it will be explained later. 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 the 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 $\mathcal{T}_{2,A} \simeq \left[\dfrac{m}{2}\right] \times \mathbb{P}_{1,1} \perp (2m^2 - \left[\dfrac{m}{2}\right]) \times \mathbb{P}_{0,0}$.

Proof: Let (E_{ij}) be the standard basis of A. We will write E_i instead of E_{ii}. 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 $(E_{ij}, E_{ji}), i < j$, $(F_{2k-1}, F_{2k}), 1 \leq k \leq m$ is a symplectic basis for $\mathcal{T}_{2,A}$.
Moreover, we have $\chi(E_{ij}) = X^n$, so $\mathrm{T}_{2,A}(E_{ij}) = 0$. We also get
$\chi(F_{2k}) = \chi(F_{2k-1}) = (X+1)^{2k-1}X^{n-2k+1}$, so we have

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

This finishes the proof.

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

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

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

Proof:

• If $x = \sum_{i=0}^{n-1} \lambda_i e^i$, 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 previous spaces. 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 $S = diag\langle \lambda, \lambda^{\sigma^{n-1}}, \cdots, \lambda^\sigma\rangle$. Thus we get $\mathrm{T}_{2,A}(\lambda) = \mathrm{T}_{2,E}(\lambda)$, *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 $C = (c_{i,j})_{0 \le i,j \le n-1}$, we know that

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

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

$$\mathrm{T}_{2,A}(\lambda e^k) = \sum_{i>j} s_{i,j} s_{j,i} = \sum_{j=0}^{n-k-1} s_{k+j,j} s_{j,j+k}.$$

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 $\mathrm{T}_{2,A}(\lambda e^k) = 0$ for $1 \le k \le m-1$. Since we have $b_{2,A}(\lambda e^i, \mu e^j) = 0$ for $\lambda, \mu \in E$ and $1 \le i, j \le m-1$, we finally get that the restriction of the second trace form to the subspace $H := \langle \lambda e^k, \lambda \in E, k = 1, \cdots, m-1 \rangle$ 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 $\mathrm{T}_{2,A}(\lambda e^m) = a \sum_{j=0}^{m-1} \lambda^{\sigma^{-j}} \lambda^{\sigma^{-m-j}}$.
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 $q \sim \mathbb{P}_{1,\mathrm{Arf}(E/K)} \perp [\frac{m}{2}] \times \mathbb{P}_{1,1}$. 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 $e_1, \cdots, e_{n^2}$ of A and let $n_A(X_1, \cdots, X_{n^2}) := \mathrm{Nrd}_A(X_1 e_1 + \cdots + X_{n^2} e_{n^2})$. This polynomial is absolutely irreducible, so $R_A := K[X_1, \cdots, X_{n^2}]/(n_A)$ 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 integrally 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 $\mathrm{Res}_{K(\nu_A)/K} = \langle [A] \rangle$ (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 the 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/K such that:

(1) $A \otimes L$ is isomorphic to a G-crossed product,

(2) $\mathrm{Res}_{L/K}$ 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), that is $x \in \wp(K)$.
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

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

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 $Gal(K_s/K)$ acts on H by left multiplication. Now define $\tilde{E}$ to be the subfield of K_s fixed by the elements $s \in Gal(K_s/K)$ inducing an even permutation on H. Then $\tilde{E}/K$ is a separable field extension of degree at most 2. If $\mathrm{char}\, K = 2$, 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 $\mathrm{char}\, K \neq 2$, 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 $\tilde{E} = F$. Let $s \in \mathrm{Gal}(K_s/K)$. Here E/K is a Galois field extension, so every element of H is a K-automorphism of E and $t := s|_E$ permutes the elements of $G := \mathrm{Gal}(E/K)$. It is easy to see that this permutation is a product of $\dfrac{n}{o(t)}$ disjoint $o(t)$-cycles (they are obtained by restriction of the permutation to each class of $G/\langle t \rangle$). So the signature of this permutation is $(-1)^{n - \frac{n}{o(t)}}$, which is equal to 1 if and only if $\dfrac{n}{o(t)}$ is even (because n is even). Since G is cyclic, we have $\langle t \rangle = \langle \sigma^{\frac{n}{o(t)}} \rangle \subseteq \langle \sigma^2 \rangle$. Now if $u \in F \subseteq E$, we have $s(u) = t(u) = u$, because $F = E^{\langle \sigma^2 \rangle}$. So we have obtained $F \subseteq \tilde{E}$. Since $[F : K] = 2 \leq [\tilde{E} : K] \leq 2$, we get $F = \tilde{E}$.
We finally obtain $\dfrac{n}{2}[A] = (a, \tilde{E}/K, \sigma|_{\tilde{E}})$. 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/K such that $A \otimes L$ is a cyclic algebra and $\mathrm{Res}_{L/K}$ is an injection.

Since we have

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

we get the result.

Remark: As in [U], [LM], [Ti] and [Se], we obtain
$c(\mathcal{T}_{2,A}) = c(\mathcal{T}_{2,M_n(K)}) + \dfrac{n}{2}[A]$ for any central simple algebra of even degree n. This is not very surprising, and can be explained as follows: Let $A \mapsto q_A$ be a quadratic invariant of central simple K-algebras, where K is a field of any characteristic . We easily get that $c(q_A) - c(q_{M_n(K)}) \in Ker\mathrm{Res}_{K(A)/K}$, so $c(q_A) = c(q_{Mn(K)}) + r(A)[A]$. Applying this equality to the generic division algebra of degree n, one can show that $r(A)$ only depends on n, so $c(q_A) = c(q_{M_n(K)}) + r_n[A]$. 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 $\mathrm{char}\, K = 2$). This method has been first applied by Saltman to compute the Clifford invariant of the trace form of a central simple algebra when $\mathrm{char}\, K \neq 2$ (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], section 12.

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 $c(g,h) := (gd_h)d_g(d_{gh})^{-1} \in M$ for $g,h \in G$. Let $K(M)$ be the quotient field of the group algebra $K[M]$. 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 $E := (K(M)/K', G, c)$ is called *the generic G-crossed product over K*. It follows immediately from [S2], Theorem 12.4, that $[E]$ has order n in $\mathrm{Br}(K')$.

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

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

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

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 $\mathrm{Res}_{K(M)/K}$ is an injection, so $\mathrm{Res}_{K'/K}$ is an injection.
Since $\mathrm{Res}_{L/K} = \mathrm{Res}_{L/K'} \circ \mathrm{Res}_{K'/K}$, we get

$$\mathrm{Ker}\,\mathrm{Res}_{L/K} = \mathrm{Br}(K) \cap \langle [(A \otimes_K K') \otimes_{K'} E^{op}] \rangle$$

by Proposition 3 (c). Let $[B] = r[A \otimes_K K') \otimes_{K'} E^{op}]$ 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 $[B] \in \mathrm{Br}(K)$ and $\tilde{K}$ contains $\overline{K}$, we have $[B \otimes_K \tilde{K}] = 0$. On the other hand, we have $[B \otimes_K \tilde{K}] = r[E^{op} \otimes_{K'} \tilde{K}] = -r[E \otimes_{K'} \tilde{K}]$, since $\tilde{K}$ splits $A \in \mathrm{Br}(K)$. So we have $r[E \otimes_{K'} \tilde{K}] = 0$. Since $E \otimes_{K'} \tilde{K}$ 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^{op} have degree n over K', so $[B] = 0$.

Acknowledgments: The first author would thank David Saltman for fruitful conversations.

References

[B1] Berhuy G. *Autour des formes trace des algèbres cycliques.* Preprint

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

[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.* Springer (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)

[S1] Saltman D. *Generic splitting fields of central simple algebras.* Ann. of Math. **62**, 8-43 (1955)

[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**, Springer, Berlin (1985)

[Se] Serre J.-P. *Cohomologie galoisienne.* Cinquième édition, Lecture Notes in Mathematics **5**, 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.* Preprint

Equipe de Mathématiques de Besançon
U.F.R. Sciences et Techniques
16, route de Gray
25030 Besançon cedex
France

berhuy@math.univ-fcomte.fr
frings@math.univ-fcomte.fr