La forme seconde trace d'une algèbre simple centrale de degré 4 de caractéristique 2

Jean-Pierre Tignol [a,1]

[a] *Département de mathématique, Université catholique de Louvain, B-1348 Louvain-la-Neuve, Belgique*

Reçu le *****; accepté le +++++

Présenté par Jean-Pierre Serre

Résumé

Soit A une algèbre simple centrale de degré 4 sur un corps k de caractéristique 2. La forme quadratique q_A donnée par le deuxième coefficient du polynome caractéristique réduit s'écrit de façon unique comme une somme (au sens de Witt) $[1,1]+q_2+q_4$, où $[1,1]$ est la forme x^2+xy+y^2 et q_2 (resp. q_4) est une 2-forme de Pfister (resp. une 4-forme de Pfister). On a $q_4=0$ si et seulement si A est cyclique, et $q_2=0$ si et seulement si $2.[A]=0$ dans $\mathrm{Br}(k)$. *Pour citer cet article : J-P. Tignol, C. R. Acad. Sci. Paris, Ser. I 340 (2005).*

Abstract

The second trace form of a central simple algebra of degree 4 of characteristic 2. Let A be a central simple algebra of degree 4 over a field k of characteristic 2 and let q_A be the quadratic form on A given by the second coefficient of the reduced characteristic polynomial. We show that A uniquely determines a 2-fold Pfister form q_2 and a 4-fold Pfister form q_4 such that $q_A=[1,1]+q_2+q_4$ in the Witt group of k, where $[1,1]$ is the form x^2+xy+y^2. The form q_2 is the norm form of the quaternion algebra Brauer-equivalent to $A\otimes_k A$, and q_4 is hyperbolic if and only if A is cyclic. *To cite this article: J-P. Tignol, C. R. Acad. Sci. Paris, Ser. I 340 (2005).*

1. Énoncé des résultats

L'objectif de cette note est de montrer comment les résultats de [7] peuvent être adaptés au cas de la caractéristique 2.

Soit k un corps de caractéristique 2. Pour a, $b\in k$, la forme quadratique $ax_1^2+x_1x_2+bx_2^2$ est notée $[a,b]$. Pour $a_1,\ldots,a_n\in k^\times$, la forme bilinéaire $a_1x_1y_1+\cdots+a_nx_ny_n$ est notée $\langle a_1,\ldots,a_n\rangle$. Les formes

Email address: tignol@math.ucl.ac.be (Jean-Pierre Tignol).

[1] L'auteur est subventionné en partie par le FNRS et participe au réseau européen HPRN-CT-2002-00287, KTAGS.

quadratiques $\langle 1, a_1\rangle \otimes \cdots \otimes \langle 1, a_n\rangle \otimes [1, b]$ sont appelées $(n+1)$-*formes de Pfister*. En particulier, la forme norme d'une algèbre de quaternions est une 2-forme de Pfister.

Soit A une algèbre simple centrale de degré 4 sur k. On note $q_A \colon A \to k$ la forme quadratique donnée par le deuxième coefficient du polynome caractéristique réduit,

$$\mathrm{Pcrd}_x(t) = t^4 - \mathrm{Trd}_A(x)t^3 + q_A(x)t^2 - \cdots .$$

D'après [4, Corollary 1], la forme q_A est non singulière. Les §§2 et 3 donnent les démonstrations des théorèmes suivants :

Théorème 1 *Il existe une 2-forme de Pfister q_2 et une 4-forme de Pfister q_4 sur k telles que l'on ait $q_A = [1,1] + q_2 + q_4$ dans le groupe de Witt $W_q(k)$. Ces conditions déterminent q_2 et q_4 de manière unique. De plus,*

(1) q_2 est la forme norme de l'algèbre de quaternions équivalente au sens de Brauer à $A \otimes_k A$.

(2) q_4 est un multiple de q_2, c'est-à-dire qu'il existe r_1, $r_2 \in k^\times$ tels que $q_4 = \langle 1, r_1\rangle \otimes \langle 1, r_2\rangle \otimes q_2$.

Théorème 2 *La forme q_4 est hyperbolique (i.e. on a $q_4 = 0$ dans $W_q(k)$) si et seulement si l'algèbre A est cyclique, c'est-à-dire si elle contient une k-algèbre étale $\mathbb{Z}/4\mathbb{Z}$-galoisienne.*

Il résulte de ces théorèmes que A est cyclique si elle est d'exposant 2. C'est un cas particulier d'une propriété générale, voir [1, Lemma 13, p. 109].

2. Démonstration du Théorème 1

Supposons d'abord que A contienne une k-algèbre étale $\mathbb{Z}/4\mathbb{Z}$-galoisienne E. Soit σ un automorphisme de E qui résulte de l'action d'un générateur de $\mathbb{Z}/4\mathbb{Z}$. On peut alors trouver $z \in A^\times$ tel que

$$A = E \oplus Ez \oplus Ez^2 \oplus Ez^3 \qquad \text{et} \qquad zx = \sigma(x)z \quad \text{pour tout } x \in E.$$

Soit $z^4 = a \in k^\times$ et soit $e \in k$ l'invariant d'Arf de la restriction de q_A à E. D'après [4, Proposition 2],

$$q_A = [a^{-1}, a] + [1, e] + [a^{-1}, ae] \qquad \text{dans } W_q(k).$$

Dans $W_q(k)$, on a $[1, u] + [1, v] = [1, u + v]$ pour u, $v \in k$ et $[a^{-1}, au] = \langle a\rangle \otimes [1, u]$. Dès lors, on peut mettre le résultat précédent sous la forme suivante :

$$q_A = \langle a\rangle[1,1] + \langle 1, a\rangle[1, e] = [1,1] + \langle 1, a\rangle[1, 1+e] \qquad \text{dans } W_q(k).$$

On obtient donc une décomposition de la forme souhaitée avec $q_2 = \langle 1, a\rangle[1, 1+e]$ et $q_4 = 0$.

Considérons pour suivre le cas où A n'est pas cyclique. Alors A est un corps, et d'après un théorème d'Albert [1, Theorem 11.9], l'algèbre A contient un sous-corps commutatif maximal K qui est une extension galoisienne de degré 4 de k, de groupe de Galois abélien élémentaire. Soient σ_1, σ_2 et σ_3 les éléments non triviaux du groupe de Galois de K/k. On pose pour $j = 1, 2, 3$,

$$K_j = \{x \in A \mid xy = \sigma_j(y)x \text{ pour tout } y \in K\}.$$

Alors $A = K \oplus K_1 \oplus K_2 \oplus K_3$, et cette décomposition est orthogonale pour la forme q_A. On désigne par φ_0, φ_1, φ_2, φ_3 les restrictions de q_A à K, K_1, K_2, K_3 respectivement, de sorte que $q_A = \varphi_0 \oplus \varphi_1 \oplus \varphi_2 \oplus \varphi_3$. D'après [3, Théorème 3.5], on a $\varphi_0 = [1,1]$ dans $W_q(k)$, donc

$$q_A = [1,1] + \varphi_1 + \varphi_2 + \varphi_3 \qquad \text{dans } W_q(k). \tag{1}$$

Lemme 3 *Pour $x \in K_1$ et $y \in K_2$, on a $xy + yx \in K_3$ et $\varphi_3(xy + yx) = \varphi_1(x)\varphi_2(y)$.*

Preuve : Il suffit de vérifier ces relations après extension des scalaires à une clôture séparable k_s de k. On peut trouver un isomorphisme θ: $A \otimes_k k_s \to M_4(k_s)$ tel que $\theta(K \otimes k_s)$ soit l'ensemble des matrices diagonales et

$$\theta(K_1 \otimes k_s) = \left(\begin{array}{cc|cc} & * & & \\ * & & & \\ \hline & & & * \\ & & * & \end{array}\right), \qquad \theta(K_2 \otimes k_s) = \left(\begin{array}{cc|cc} & & * & \\ & & & * \\ \hline * & & & \\ & * & & \end{array}\right), \qquad \theta(K_3 \otimes k_s) = \left(\begin{array}{cc|cc} & & & * \\ & & * & \\ \hline & * & & \\ * & & & \end{array}\right).$$

Un calcul matriciel établit le lemme. $\square$

Ce lemme montre que les formes φ_1, φ_2, φ_3 de rang 4 «permettent la composition». D'après [5, Theorem 2.10], il existe une 2-forme de Pfister φ et des éléments $r_1, r_2 \in k^\times$ tels que

$$\varphi_1 = \langle r_1 \rangle \otimes \varphi, \qquad \varphi_2 = \langle r_2 \rangle \otimes \varphi, \qquad \varphi_3 = \langle r_1 r_2 \rangle \otimes \varphi.$$

L'équation (1) prend alors la forme

$$q_A = [1,1] + \langle r_1, r_2, r_1 r_2 \rangle \varphi = [1,1] + \varphi + \langle 1, r_1 \rangle \langle 1, r_2 \rangle \varphi \qquad \text{dans } W_q(k).$$

On obtient donc la décomposition souhaitée avec $q_2 = \varphi$ et $q_4 = \langle 1, r_1 \rangle \otimes \langle 1, r_2 \rangle \otimes \varphi$.

Pour établir l'unicité de q_2 et q_4, considérons une décomposition arbitraire $q_A = [1,1] + q_2 + q_4$ dans $W_q(k)$, où q_2 est la forme norme d'une algèbre de quaternions Q et q_4 est une 4-forme de Pfister. D'après [6, Proposition 5, p. 116], l'algèbre de Clifford de q_A est équivalente au sens de Brauer à celle de q_2, donc aussi à Q. Cela prouve l'unicité de la forme q_2, donc aussi de q_4. Par ailleurs, Berhuy et Frings ont montré [4, Theorem 3] que l'algèbre de Clifford de q_A est équivalente au sens de Brauer à $A \otimes_k A$, donc $[Q] = 2[A]$ dans $\mathrm{Br}(k)$.

3. Démonstration du Théorème 2

Si A est cyclique, le début de la preuve du Théorème 1 montre que q_4 est hyperbolique. Il suffit donc de prouver la réciproque. L'algèbre A est cyclique si elle n'est pas un corps ; on peut donc supposer que A est un corps et utiliser les notations de la preuve du Théorème 1. Si q_4 est hyperbolique, alors toute sous-forme de dimension 9 est isotrope, donc la forme $\varphi_1 \oplus \varphi_2$ représente 1. Soit $x \in K_1 \oplus K_2$ tel que $q_A(x) = 1$ et soit $y \in K$ tel que $\sigma_1(y) = \sigma_2(y) = y + 1$, ce qui entraîne $y^2 - y \in k$. On a $xyx^{-1} = y + 1$ et $x^2yx^{-2} = y$, donc $x \notin k(x^2)$. Comme $q_A(x) = 1$, le polynome minimal de x sur k est de la forme $t^4 + t^2 + a$ pour un certain $a \in k^\times$. Pour $z = x^3 + x + y$, on a $z^2 - z = a(x^2 + 1) + y^2 - y \in k(x^2)$. On peut dès lors définir un k-automorphisme τ d'ordre 4 de $k(x^2, z)$ en posant $\tau(x^2) = x^2 + 1$ et $\tau(z) = z + x^2$, ce qui prouve que le sous-corps $k(x^2, z)$ de A est une extension cyclique de degré 4 de k.

4. Exemple

Une algèbre A pour laquelle $q_4 \neq 0$ est nécessairement non cyclique et d'exposant 4. L'exemple ci-dessous est un cas particulier de ceux construits par Amitsur et Saltman [2]. Soit A_0 un corps de degré et d'exposant 4 sur un corps k_0 de caractéristique 2 et soit K_0 un sous-corps maximal de A_0 qui est une extension galoisienne de k_0 de groupe de Galois abélien élémentaire. Soient σ_1 et σ_2 des automorphismes de K_0/k_0 qui engendrent le groupe de Galois. On peut alors choisir dans $A_0^\times$ des éléments z_1, z_2 tels que $z_i\ell = \sigma_i(\ell)z_i$ pour tout $\ell \in K_0$ et pour $i = 1, 2$. Alors il y a dans $K_0^\times$ des éléments u, b_1, b_2 tels que

$$z_2z_1 = uz_1z_2, \qquad z_1^2 = b_1, \qquad z_2^2 = b_2, \qquad \text{ce qui entraîne } \sigma_i(b_i) = b_i \text{ pour } i = 1, 2.$$

Soient t_1, t_2 deux indéterminées sur k_0. On pose $k = k_0(t_1, t_2)$ et $K = K_0(t_1, t_2)$, et on étend σ_1 et σ_2 à K en fixant t_1 et t_2. Considérons l'algèbre A_1 engendrée sur k par K et par deux éléments y_1, y_2 soumis aux relations suivantes pour $i = 1, 2$:

$$y_i\ell = \sigma_i(\ell)y_i \quad \text{pour tout } \ell \in K, \qquad y_i^2 = t_i, \qquad y_2y_1 = y_1y_2.$$

L'algèbre A_1 est un produit de deux algèbres de quaternions qui, comme $A_0 \otimes_{k_0} k$, contient K comme sous-corps commutatif maximal. Par conséquent, $A_0 \otimes_{k_0} A_1$ est équivalente au sens de Brauer à une k-algèbre simple centrale A de degré 4, contenant aussi K comme sous-corps commutatif maximal. D'après [8, p. 422], l'algèbre A est engendrée sur K par deux éléments x_1, x_2 soumis aux relations suivantes pour $i = 1, 2$:

$$x_i\ell = \sigma_i(\ell)x_i \quad \text{pour tout } \ell \in K, \qquad x_i^2 = b_it_i, \qquad x_2x_1 = ux_1x_2.$$

Comme $A_1 \otimes_k A_1$ est déployée, on a $2[A] = 2[A_0 \otimes_{k_0} k]$ dans $\mathrm{Br}(k)$, donc l'algèbre A est d'exposant 4 et la forme q_2 de A est une forme anisotrope définie sur k_0. Avec les notations de la preuve du Théorème 1, on a $K_1 = Kx_1$, $K_2 = Kx_2$, $K_3 = K(x_1x_2 + x_2x_1)$. En posant $c_1 = b_1 + \sigma_2(b_1) \in k_0$ et $c_2 = b_2 + \sigma_1(b_2) \in k_0$, on a $q_A(x_1) = c_1t_1$ et $q_A(x_2) = c_2t_2$. D'après la preuve du Théorème 1, on a

$$q_4 = \langle 1, c_1t_1\rangle \otimes \langle 1, c_2t_2\rangle \otimes q_2.$$

La forme q_4 n'est pas hyperbolique puisque q_2 est une forme anisotrope définie sur k_0 et que t_1 et t_2 sont des indéterminées sur k_0.

Références

[1] A. A. Albert, *Structure of algebras*, Amer. Math. Soc., Providence, R.I., 1961. MR0123587 (23 #A912) Zbl 0023.19901

[2] S. A. Amitsur and D. Saltman, Generic Abelian crossed products and p-algebras, J. Algebra **51** (1978), 76–87. MR0491789 (58 #10988) Zbl 0391.13001

[3] A.-M. Bergé et J. Martinet, Formes quadratiques et extensions en caractéristique 2, Ann. Inst. Fourier (Grenoble) **35** (1985), 57–77. MR0786534 (87a :11036) Zbl 0539.10018

[4] G. Berhuy and C. Frings, On the second trace form of central simple algebras in characteristic two, Manuscripta Math. **106** (2001), 1–12. MR1860978 (2002i :16024) Zbl 1003.11015

[5] M. Kneser et al., Composition of quaternary quadratic forms, Compositio Math. **60** (1986), 133–150. MR0868134 (88a :11037) Zbl 0612.10015

[6] P. Mammone, J.-P. Tignol and A. Wadsworth, Fields of characteristic 2 with prescribed u-invariants, Math. Ann. **290** (1991), 109–128. MR1107665 (92g :11035) Zbl 0713.12002

[7] M. Rost, J-P. Serre et J-P. Tignol, La forme trace d'une algèbre simple centrale de degré 4, à paraître.

[8] J.-P. Tignol, Produits croisés abéliens, J. Algebra **70** (1981), 420–436. MR0623817 (84f :16026) Zbl 0473.16004