Multiples of trace forms and algebras with involution

Eva Bayer–Fluckiger

Introduction

Let k be a field of characteristic $\neq 2$, and let L be a Galois extension of k with group G. Let

$$q_L : L \times L \to k$$

$$q_L(x, y) = \mathrm{Tr}_{L/k}(xy)$$

be the trace form. It is well–known that L has a normal basis over k, in other words there exists $x \in L$ such that $\{gx\}_{g \in G}$ is a basis of L as a k-vector space. Such a basis is called a *self–dual normal basis* if $q_L(gx, hx) = \delta_{g,h}$ for all $g, h \in G$.

The following question was studied in [1], [2], [3], [5], [7] :

Question. *Which Galois extensions have a self–dual normal basis ?*

This question is settled in some cases, for instance when G has odd order [3], when the 2–Sylow subgroups of G are elementary abelian [7], but it is open in general.

Note that the existence of a normal basis is equivalent with the fact that L is a free $k[G]$–module of rank one. A similar reformulation can be given for the self–dual normal basis question. Indeed, remark that the quadratic form q_L is invariant by G, that is $q_L(gx, gy) = q_L(x, y)$ for all $x, y \in L$ and for all $g \in G$. In other words, q_L is a G–quadratic form (cf. 1.3). Let us define the *unit G–quadratic form* as being $q_0 : k[G] \times k[G] \to k$ characterized by $q_0(g, h) = \delta_{g,h}$. Then the existence of a self–dual normal basis is equivalent with the isomorphism of q_L and q_0 as G–quadratic forms.

It is more natural to work in the category of *G–Galois algebras* instead of Galois extensions with group G. Let us denote by L_0 the split G–Galois algebra; then $q_{L_0} \simeq_G q_0$. This leads us to the following question :

Question. *Let L and L' be two G–Galois algebras. When are the G–forms q_L and $q_{L'}$ isomorphic ?*

The results of [3] and [7] apply to this more general situation. However, a complete answer to the question seems out of reach at this point. For this reason, a weaker question was raised in [1]. Indeed, if ϕ is a non–degenerate quadratic form and q is a G–quadratic form, then the tensor product $\phi \otimes q$ is a G–quadratic form. One can ask the following

Question. *Let L and L' be two G–Galois algebras, and let ϕ be a non–degenerate quadratic form. When are the G–forms $\phi \otimes q_L$ and $\phi \otimes q_{L'}$ isomorphic ?*

If ϕ is an odd dimensional form, then this question is equivalent with the previous one. Let $W(k)$ be the Witt ring of k, and let I be the ideal of $W(k)$ consisting of the Witt classes of the even dimensional forms. Let k_s be a separable closure of k, and set $\Gamma_k = \mathrm{Gal}(k_s/k)$. For every positive integer n, let us denote by $e_n : I^n/I^{n+1} \to H^1(\Gamma_k, \mathbf{Z}/2\mathbf{Z})$ the Milnor–Voevodsky isomorphism (see 1.2). Let $\mathrm{cd}_2(\Gamma_k)$ be the 2–cohomological dimension of Γ_k (cf. 1.1), and let $d \geq 0$ be an integer. The following two statements are easy consequences of the above isomorphisms (cf. 1.2.2, 1.2.5) :

I. *Suppose that* $\mathrm{cd}_2(\Gamma_k) \leq d$. *Let* q *and* q' *be two quadratic forms with* $\dim(q) = \dim(q')$, *and let* $\phi \in I^d$. *Then*

$$\phi \otimes q \simeq \phi \otimes q'.$$

II. *Suppose that* $\mathrm{cd}_2(\Gamma_k) \leq d$. *Let* q *and* q' *be two quadratic forms with* $\dim(q) = \dim(q')$, *and let* $\phi \in I^{d-1}$. *Then*

$$\phi \otimes q \simeq \phi \otimes q' \text{ if and only if } e_{d-1}(\phi) \cup (\mathrm{disc}(q)) = e_{d-1}(\phi) \cup (\mathrm{disc}(q')) \text{ in } H^d(k).$$

It is natural to look for similar statements concerning trace forms of G–Galois algebras, as proposed in [1]. As an analog of I, we have the following :

Theorem. (Chabloz, [9]) *Suppose that* $\mathrm{cd}_2(\Gamma_k) \leq d$. *Let* L *and* L' *be two* G*–Galois algebras, and let* $\phi \in I^d$. *Then* $\phi \otimes q_L \simeq_G \phi \otimes q_{L'}$.

In order to go further, we need some invariants defined in [7]. Let $f_L : \Gamma_k \to G$ be a continuous homomorphism corresponding to the G–Galois algebra L. The homomorphism f_L induces $f_L^* : H^1(G, \mathbf{Z}/2\mathbf{Z}) \to H^1(\Gamma_k, \mathbf{Z}/2\mathbf{Z})$. For all $x \in H^1(G, \mathbf{Z}/2\mathbf{Z})$, set $x_L = f_L^*(x)$. Then x_L is an invariant of the G–quadratic form q_L (cf. [7], 2.2.3).

The following statement is inspired by II, and is proved in §3 :

Theorem. *Suppose that* $\mathrm{cd}_2(\Gamma_k) \leq d$. *Let* L *and* L' *be two* G*–Galois algebras, and let* $\phi \in I^{d-1}$. *Then the* G*–quadratic forms* $\phi \otimes q_L$ *and* $\phi \otimes q_{L'}$ *are isomorphic if and only if* $e_{d-1}(\phi) \cup x_L = e_{d-1}(\phi) \cup x_{L'}$ *for all* $x \in H^1(G, \mathbf{Z}/2\mathbf{Z})$.

This was conjectured in [1], and proved in special cases by Chabloz, Monsurro, Morales, Parimala and Schoof (see [4], [5], [6], [9] and [12]).

The proof uses results concerning hermitian forms over algebras with involution (see 1.5 and §2 for details). Let (D, σ) be a division algebra with involution over k, and let $W(D, \sigma)$ be the Witt group of hermitian forms over (D, σ). Then $W(D, \sigma)$ is a $W(k)$–module. Let us denote by J the $W(k)$–submodule of $W(D, \sigma)$ consisting of even dimensional hermitian forms over D.

Theorem. *Suppose that* $\mathrm{cd}_2(\Gamma_k) \leq d$. *Then*

(a) We have $I^d J = 0$.
(b) If σ is of the second kind, then $I^{d-1}J = 0$.
(c) If σ is of the first kind and of the symplectic type, then $I^{d-2}J = 0$.

Part (a) is due to Chabloz [9]. Parts (b) and (c) are proved in §2, and are used in the proof of the main result of this paper in §3. In order to deal with involutions of the first kind and of the orthogonal type, we need the following :

Theorem. *Suppose that* $\mathrm{cd}_2(\Gamma_k) \leq d$. *Let* (D, σ) *be a quaternion algebra with an orthogonal involution, and let* (V, h) *and* (V', h') *be two hermitian forms over* (D, σ) *with* $\dim_D(V) = \dim_D(V')$. *Let* $\phi \in I^{d-1}$. *Then* $\phi \otimes h \simeq \phi \otimes h'$ *if and only if*

$$e_{d-1}(\phi) \cup (\mathrm{disc}(h)) = e_{d-1}(\phi) \cup (\mathrm{disc}(h')).$$

This follows from results of Parimala, Sridharan and Suresh [14] and of Berhuy [8].

§1. Definitions, notation and basic facts

1.1. Galois cohomology

Let k_s be a separable closure of k, and set $\Gamma_k = \mathrm{Gal}(k_s/k)$. For any discrete Γ_k–module C, set $H^i(k, C) = H^i(\Gamma_k, C)$. We say that the *2–cohomological dimension* of Γ_k is at most d, denoted by $\mathrm{cd}_2(\Gamma_k) \leq d$, if $H^i(k, C) = 0$ for all $i > d$ and for every finite 2–primary Γ_k–module C.

Set $H^i(k) = H^i(k, \mathbf{Z}/2\mathbf{Z})$, and recall that $H^1(k) \simeq k^*/k^{*2}$. For all $a \in k^*$, let us denote by $(a) \in H^1(k)$ the corresponding cohomology class. We use the additive notation for $H^1(k)$. If $a_1, \ldots, a_n \in k^*$, we denote by $(a_1) \cup \ldots \cup (a_n) \in H^n(k)$ their cup product.

If U is a linear algebraic group defined over k, let $H^1(k, U)$ be the pointed set $H^1(\Gamma_k, U(k_s))$ (cf. [16], [17] Chap. 10).

1.2. Quadratic forms

All quadratic forms are supposed to be non–degenerate. We denote by $W(k)$ the Witt ring of k, and by $I = I(k)$ the fundamental ideal of $W(k)$. For all $a_1, \ldots, a_n \in k^*$, let us denote by $<< a_1, \ldots, a_n >>=< 1, -a_1 > \otimes \ldots \otimes < 1, -a_n >$ the associated n–fold Pfister form. It is well–known that I^n is generated by the n-fold Pfister forms. The following has been conjectured by Milnor, and proved by Voevodsky (see also Orlov–Vishik–Voevodsky [13], [18], [19], and the survey paper [10]) :

Theorem 1.2.1. (Voevodsky) : *For every positive integer n, there exists an isomorphism*

$$e_n : I^n/I^{n+1} \to H^n(k)$$

such that

$$e_n(<< a_1, \ldots, a_n >>) = (a_1) \cup \ldots \cup (a_n)$$

for all $a_1, \ldots, a_n \in k^*$.

It is easy to see that the above theorem has the following consequences :

Corollary 1.2.2. *Suppose that* $\mathrm{cd}_2(\Gamma_k) \leq d$. *Let* q *and* q' *be two quadratic forms with* $\dim(q) = \dim(q')$, *and let* $\phi \in I^d$. *Then*

$$\phi \otimes q \simeq \phi \otimes q'.$$

Proof. Note that by 1.2.1, $\mathrm{cd}_2(\Gamma_k) \leq d$ implies that $I^{d+1} = 0$. As $\dim(q) = \dim(q')$, we have $q \oplus (-q') \in I$. Therefore $\phi \otimes (q \oplus (-q')) \in I^{d+1} = 0$. This implies that $\phi \otimes q \simeq \phi \otimes q'$.

For every quadratic form q, let us denote by $\mathrm{disc}(q) \in H^1(k)$ its discriminant. Recall that if $n = \dim(q)$, then $\mathrm{disc}(q) = (-1)^{\frac{n(n-1)}{2}} \det(q)$. We need the following proposition :

Proposition 1.2.3. *Let* q *and* q' *be two quadratic forms with* $\dim(q) = \dim(q')$, *and let* $\phi \in I^{d-1}$. *Then*

$$e_d(\phi \otimes (q \oplus (-q')) = e_{d-1}(\phi) \cup (\mathrm{disc}(q)) + e_{d-1}(\phi) \cup (\mathrm{disc}(q')).$$

Proof. Set $Q = q \oplus (-q')$, and let $m = \dim(q) = \dim(q')$, $n = 2m = \dim(Q)$. Note that $(-1)^{\frac{n(n-1)}{2}} = (-1)^m$, hence $(\mathrm{disc}(Q)) = (\mathrm{disc}(q)) + (\mathrm{disc}(q'))$. We have $Q \in I$, and $e_1(Q) = (\mathrm{disc}(Q)) = (\mathrm{disc}(q)) + (\mathrm{disc}(q'))$. Therefore

$$e_d(\phi \otimes Q) = e_{d-1}(\phi) \cup e_1(Q) = e_{d-1}(\phi) \cup (\mathrm{disc}(q)) + e_{d-1}(\phi) \cup (\mathrm{disc}(q')),$$

hence the proposition is proved.

Corollary 1.2.4. *Let* q *and* q' *be two quadratic forms with* $\dim(q) = \dim(q')$, *and let* $\phi \in I^{d-1}$. *If* $\phi \otimes q \simeq \phi \otimes q'$, *then* $e_{d-1}(\phi) \cup (\mathrm{disc}(q)) = e_{d-1}(\phi) \cup (\mathrm{disc}(q')) \in H^d(k)$.

Proof. As $\phi \otimes q \simeq \phi \otimes q'$, the quadratic form $\phi(\otimes(q \oplus (-q'))$ is hyperbolic. Hence $e_d(\phi \otimes (q \oplus (-q')) = 0$. By prop. 1.2.3, we have

$$e_d(\phi \otimes (q \oplus (-q')) = e_{d-1}(\phi) \cup (\mathrm{disc}(q)) + e_{d-1}(\phi) \cup (\mathrm{disc}(q')),$$

therefore $e_{d-1}(\phi) \cup (\mathrm{disc}(q)) = e_{d-1}(\phi) \cup (\mathrm{disc}(q'))$, as claimed.

Corollary 1.2.5. *Suppose that* $\mathrm{cd}_2(\Gamma_k) \leq d$. *Let* q *and* q' *be two quadratic forms with* $\dim(q) = \dim(q')$, *and let* $\phi \in I^{d-1}$. *Then*

$$\phi \otimes q \simeq \phi \otimes q' \text{ if and only if } e_{d-1}(\phi) \cup (\mathrm{disc}(q)) = e_{d-1}(\phi) \cup (\mathrm{disc}(q')) \in H^d(k).$$

Proof. Set $Q = q \oplus (-q')$. By prop. 1.2.3, we have

$$e_d(\phi \otimes Q) = e_{d-1}(\phi) \cup (\mathrm{disc}(q)) + e_{d-1}(\phi) \cup (\mathrm{disc}(q')).$$

Hence $e_d(\phi \otimes Q) = 0$ is equivalent with $e_{d-1}(\phi) \cup (\mathrm{disc}(q)) = e_{d-1}(\phi) \cup (\mathrm{disc}(q'))$. But by 1.2.1, $e_d(\phi \otimes Q) = 0$ is equivalent with $\phi \otimes Q$ hyperbolic, hence with $\phi \otimes q \simeq \phi \otimes q'$.

1.3. G–quadratic forms

Let G be a finite group, and let us denote by $k[G]$ the associated group ring. A *G–quadratic form* is a pair (M, q), where M is a $k[G]$–module that is a finite dimensional k–vector space, and $q : M \times M \to k$ is a non–degenerate symmetric bilinear form such that

$$q(gx, gy) = q(x, y)$$

for all $x, y \in M$ and all $g \in G$. We say that two G–quadratic forms (M, q) and (M', q') are *isomorphic* if there exists an isomorphism of $k[G]$–modules $f : M \to M'$ such that $q(f(x), f(y)) = q'(x, y)$ for all $x, y \in M$. If this is the case, we write $(M, q) \simeq_G (M', q')$, or $q \simeq_G q'$.

If ϕ is a quadratic form over k, and q a G–quadratic form, then the tensor product $\phi \otimes q$ is a G–quadratic form.

1.4. Trace forms

Let L be a G–Galois algebra, and let

$$q_L : L \times L \to k, \quad q_L(x, y) = \mathrm{Tr}_{L/k}(xy),$$

be its trace form. Then q_L is a *G–quadratic form.*

Let $^{-} : k[G] \to k[G]$ be the canonical involution of the group ring $k[G]$, in other words the k–linear involution of $k[G]$ characterized by $\overline{g} = g^{-1}$ for all $g \in G$. Let U_G be the linear algebraic group defined over k such that for every commutative k–algebra A, we have $U_G(A) = \{x \in A[G] \mid x\overline{x} = 1\}$. Recall that we denote by $H^1(k, U_G)$ the pointed set $H^1(\Gamma_k, U(k_s))$.

Let $f_L : \Gamma_k \to G$ be a continuous homomorphism corresponding to L. The composition of f_L with the inclusion of G in $U_G(k_s)$ is a 1–cocycle $\Gamma_k \to U_G(k_s)$. Let us denote by $u(L)$ its class in the cohomology set $H^1(k, U_G)$. The following is proved in [7], prop. 1.5.1

Proposition 1.4.1 *Let L and L' be two G–Galois algebras. Then the G–quadratic forms q_L and $q_{L'}$ are isomorphic if and only if $u(L) = u(L') \in H^1(k, U_G)$.*

The trace form of a G–Galois algebra, considered as a G–form, determines the trace forms of all of its subalgebras of fixed points (se [7], 1.4). We have a similar result for *multiples* of trace forms, as follows :

Proposition 1.4.2 *Let L and L' be two G–Galois algebras. Let H be a subgroup of G, and set $E = L^H$, $E' = L'^H$. Let ϕ be a quadratic form over k. Suppose that $\phi \otimes q_L \simeq_G \phi \otimes q_{L'}$. Then we have*

(a) The quadratic forms $\phi \otimes q_E$ and $\phi \otimes q_{E'}$ are isomorphic.

(b) If moreover H is a normal subgroup of G, then the (G/H)–quadratic forms $\phi \otimes q_E$ and $\phi \otimes q_{E'}$ are isomorphic.

Proof. The proof of this statement is similar to the proof of [7], 1.5.1.

The homomorphism $f_L : \Gamma_k \to G$ induces $f_L^* : H^1(G, \mathbf{Z}/2\mathbf{Z}) \to H^1(k)$. For any $x \in H^1(G, \mathbf{Z}/2\mathbf{Z})$, set $x_L = f_L^*(x)$. Then the elements x_L are invariants of the G–quadratic form q_L (cf. [7], 2.2.3). Let $x \in H^1(G, \mathbf{Z}/2\mathbf{Z})$, and let $\chi : G \to \mathbf{Z}/2\mathbf{Z}$ the corresponding homomorphism. Let H be the kernel of χ, and let $E_\chi = L^H$ be the invariant subalgebra; it is a quadratic subalgebra of L. The discriminant of the quadratic algebra E_χ is equal to x_L.

The following is a generalization of [7], 2.2.3 :

Proposition 1.4.3 *Let L and L' be two G–Galois algebras. Let $\phi \in I^{d-1}$. Suppose that $\phi \otimes q_L \simeq_G \phi \otimes q_{L'}$. Then $e_{d-1}(\phi) \cup x_L = e_{d-1}(\phi) \cup x_{L'}$ for all $x \in H^1(G, \mathbf{Z}/2\mathbf{Z})$.*

Proof. Let $x \in H^1(G, \mathbf{Z}/2\mathbf{Z})$, and let $\chi : G \to \mathbf{Z}/2\mathbf{Z}$ the corresponding homomorphism. Let H be the kernel of χ, and set $E_\chi = L^H$, $E'_\chi = L'^H$. By prop. 1.4.2, the quadratic forms $\phi \otimes q_E$ and $\phi \otimes q_{E'}$ are isomorphic. Using 1.2.4, we have $e_{d-1}(\phi) \cup \mathrm{disc}(q_E) = e_{d-1}(\phi) \cup \mathrm{disc}(q_{E'})$. As the discriminant of a quadratic algebra is equal to the discriminant of its trace form, we obtain $e_{d-1}(\phi) \cup x_L = e_{d-1}(\phi) \cup x_{L'}$, so the proposition is proved.

1.5. Hermitian forms over division algebras with involution

Let D be a division algebra over k. An *involution* of D is a k–linear anti–automorphism $\sigma : D \to D$ of order 2. Let K be the center of D. We say that (D, σ) is a *division algebra with involution over k* if the fixed field of σ in K is equal to k. If $K = k$, then σ is said to be of the *first kind*. After extension to k_s, the involution σ is determined by a symmetric or a skew–symmetric form. In the first case, σ is said to be of the *orthogonal type*, in the second one, of the *symplectic type*. If $K \neq k$, then K is a quadratic extension of k and the restriction of σ to K is the non–trivial automorphism of K over k. In that case, the involution is said to be of the *second kind*, or a *unitary involution*, or a K/k–involution. See for instance [11] or [15], chap 7, for more details on algebras with involution.

Let (D, σ) be a division algebra with involution over k. A *hermitian form* over (D, σ) is by definition a pair (V, h), where V is a finite dimensional D–vector space, and $h : V \times V \to D$ is hermitian with respect to σ. We say that (V, h) is *hyperbolic* if there exists a sub D–vector space W of V with $\dim(V) = 2\dim(W)$ and such that $h(x, y) = 0$ for all $x, y \in W$. This leads to a notion of Witt group $W(D, \sigma)$ (cf. for instance [15], Chap 7. §2). Note that the tensor product of a quadratic form over k with a hermitian form over (D, σ) is a hermitian form over (D, σ), hence $W(D, \sigma)$ is a $W(k)$–module.

Let (V,h) be a hermitian form over (D,σ), as above. Let $n=\dim_D(V)$, and let H be the matrix of h with respect to some D–basis of V. Let us denote by $\mathrm{Nrd}: M_n(D)\to k$ the reduced norm. The *discriminant* of h is by definition $\mathrm{disc}(h)=(-1)^{\frac{n(n-1)}{2}}\mathrm{Nrd}(H)\in k^*/k^{*2}$.

§2. Multiples of hermitian forms

Let (D,σ) a division algebra with involution over k. Let us denote by J the sub $W(k)$–module of $W(D,\sigma)$ consisting of the hermitian forms (V,h) with $\dim_D(V)$ even. Suppose that $\mathrm{cd}_2(\Gamma_k)\leq d$.

Theorem 2.1.1. *(a) We have $I^dJ=0$.*
(b) If σ is of the second kind, then $I^{d-1}J=0$.
(c) If σ is of the first kind and of the symplectic type, then $I^{d-2}J=0$.

Part (a) was proved by Chabloz in [9]. We need the following lemma :

Lemma 2.1.2. *Let $a\in D^*$ such that $\sigma(a)=a$. We have :*
(a) If $\phi\in I^d$, then $\phi\otimes<1,a>$ is hyperbolic.
(b) If $\phi\in I^{d-1}$ and σ is of the second kind, then $\phi\otimes<1,a>$ is hyperbolic.
(c) If $\phi\in I^{d-2}$ and σ is of the first kind and of the symplectic type, then $\phi\otimes<1,a>$ is hyperbolic.

Proof.

(a) Let $F=k(a)$, and let $f:W(F)\to W(D,\sigma)$ be the base change homomorphism. We have $f(\phi\otimes<1,a>)=\phi\otimes<1,a>$, hence it suffices to check that $\phi\otimes<1,a>=0$ in $W(F)$. Note that $\phi\otimes<1,a>\in I^{d+1}(F)$. As $\mathrm{cd}_2(k)\leq d$, we have $\mathrm{cd}_2(F)\leq d$, therefore by Theorem 1.2.1, we have $I^{d+1}(F)=0$. Hence $\phi\otimes<1,a>$ is hyperbolic, and this concludes the proof of (a).

(b) Suppose that σ is a K/k–involution, and set $E=K(a)$, $F=k(a)$. Let us denote by $\tau:E\to E$ the restriction of $\sigma:D\to D$ to E. Then τ is an E/F–involution, an involution of the second kind. Let $f:W(E,\tau)\to W(D,\sigma)$ be the base change homomorphism. We have $f(\phi\otimes<1,a>)=\phi\otimes<1,a>$, hence it suffices to check that $\phi\otimes<1,a>=0$ in $W(E)$. Let $E=F(\sqrt{\delta})$, for some $\delta\in F$. Let $\mathrm{tr}_{E/F}:W(E,\tau)\to W(F)$ be the $W(F)$–homomorphism given by the trace of hermitian forms. It is well–known that $\mathrm{tr}_{E/F}$ is injective, and its image is equal to $<1,-\delta>W(F)$ (cf. for instance [15], Chap 10, §1). We have

$$\mathrm{tr}_{E/F}(<1,a>))=<1,-\delta>\otimes<1,a>,$$

hence $\mathrm{tr}_{E/F}(\phi\otimes<1,a>)=\phi\otimes<1,-\delta>\otimes<1,a>$. This implies that

$$\mathrm{tr}_{E/F}(\phi\otimes<1,a>)\in I^{d+1}(F).$$

As in (a), we see that $I^{d+1}(F) = 0$. Therefore $\phi\otimes < 1, a >= 0$ in $W(E, \tau)$, and (b) is proved.

(c) Suppose that σ is symplectic. Then the degree of D is even. Set $\deg(D) = 2m$, and let us prove the statement by induction on m. If $m = 1$, then D is a quaternion algebra and σ is the canonical involution of D. As $\sigma(a) = a$, we have $a \in k^*$. Let $\mathrm{trd} : W(D, \sigma) \to W(k)$ be the $W(k)$–homomorphism given by the reduced trace of hermitian forms. It is well–known that this homomorphism is injective, and its image is equal to $n_D W(k)$, where n_D is the norm form of the quaternion algebra D (cf. [15], chap. 10, §1). We have $\mathrm{trd}(< 1, a >) = n_D\otimes < 1, a >\in I^3$. Let $\phi \in I^{d-2}$. Then

$$\mathrm{trd}(\phi\otimes < 1, a >) = \phi \otimes n_D\otimes < 1, a >\in I^{d+1} = 0.$$

This implies that $\mathrm{trd}(\phi\otimes < 1, a >) = 0$ in $W(k)$, hence $\phi\otimes < 1, a >= 0$ in $W(D, \sigma)$.

Suppose that $m > 1$. If $a \notin k$, set $F = k(a)$. If $a \in k$, take any $b \in D^*$ such that $\sigma(b) = b$ and that $b \notin k$ (this is possible as $m > 1$) and set $F = k(b)$. Let $D' = Z_D(F)$ be the centralizer of F in D. Note that F is invariant by σ. By [11], 2.9. we know that $[F : k] \leq m$. The F–algebra D' is also invariant by σ. We have $[F : k] > 1$, hence $\deg D' < \deg(D)$. Let $\deg(D') = 2m'$. As $m' < m$, we can apply the induction hypothesis, hence $\phi\otimes < 1, a >= 0$ in $W(D', \sigma)$. Let $f : W(D', \sigma) \to W(D, \sigma)$ be the base change homomorphism. We have $f(\phi\otimes < 1, a >) = \phi\otimes < 1, a >$. Hence $\phi\otimes < 1, a >= 0$ in $W(D, \sigma)$, as claimed.

Proof of Theorem 2.1.1 Let $q \in J$. We have $q =< a_1, \ldots, a_n >$, with $a_i \in D^*$, $\sigma(a_i) = a_i$. Note that n is even, as $q \in J$. Set $m = \frac{n}{2}$. Let $H =< 1, -1 >$, and let us denote by $[m]H$ the orthogonal sum of m copies of H. Then in $W(D, \sigma)$, we have $q = q \oplus [m]H =< 1, a_1 > \oplus < -1, a_2 > \oplus \ldots \oplus < -1, a_n >$. By the lemma, $\phi\otimes < 1, a_i >$ and $\phi\otimes < -1, a_i >$ are hyperbolic for all i whenever $\phi \in I^d$, or $\phi \in I^{d-1}$ and σ is unitary, or $\phi \in I^{d-2}$ and σ is symplectic. Hence $\phi \otimes q$ is hyperbolic in these cases too, so the theorem is proved.

The following is a consequence of results of Parimala, Sridharan and Suresh [14] and of Berhuy [8].

Theorem 2.1.3 *Suppose that D is a quaternion algebra, and that σ is of the first kind and of the orthogonal type. Let $h \in J$, and let $\phi \in I^{d-1}$. Then $\phi \otimes h$ is hyperbolic if and only if $e_{d-1}(\phi) \cup (\mathrm{disc}(h)) = 0$.*

Proof. By Berhuy [8], Theorem 13, it suffices to show that $e_{d-1}(\phi) \cup (\mathrm{disc}(h)) = 0$ if and only if $e_{n,D}(\phi \otimes h) = 0$ for all $n \geq 0$ (cf. [8], 2.2 for the definition of the invariant $e_{n,D}$). As $\mathrm{cd}_2(\Gamma_k) \leq d$, we have $e_{n,D}(\phi \otimes h) = 0$ for $n > d$, so it suffices to check that $e_{d-1}(\phi) \cup (\mathrm{disc}(h)) = 0$ is equivalent with $e_{n,D}(\phi \otimes h) = 0$ for all $n = 0, \ldots, d$. Let $k(D)$ be the function field of the quadric associated to D. Then $D \otimes k(D) \simeq M_2(k(D))$, and $h_{k(D)}$ corresponds via Morita equivalence to a quadratic form q_h over $k(D)$. Note that

$\mathrm{disc}(q_h) = \mathrm{disc}(h)$. Similarly, the hermitian form $(\phi \otimes h)_{k(D)}$ corresponds to a quadratic form $q_{\phi h}$ over $k(D)$, and we have $q_{\phi h} \simeq \phi \otimes q_h$.

For all $n = 0, \ldots, d$, we have by construction that $e_{n,D}(\phi \otimes h) = 0$ if and only if $e_n(q_{\phi h}) = 0$ (cf. [8], 2.2). But $q_{\phi h} \simeq \phi \otimes q_h$, hence

$$e_n(q_{\phi h}) = e_n(\phi \otimes q_h) = e_{n-1}(\phi) \cup (\mathrm{disc}(q_h)) = e_{n-1}(\phi) \cup (\mathrm{disc}(h)).$$

If $n < d$, then $e_n(\phi) = 0$ as $\phi \in I^{d-1}$. We have $e_d(q_{\phi h}) = e_{d-1}(\phi) \cup (\mathrm{disc}(h))$. Hence $e_n(q_{\phi h}) = 0$ for all $n \geq 0$ if and only if $e_{d-1}(\phi) \cup (\mathrm{disc}(h)) = 0$. This concludes the proof.

Corollary 2.1.4 *Suppose that D is a quaternion algebra, and that σ is of the first kind and of the orthogonal type. Let h and h' be two hermitian forms over (D, σ), and let $\phi \in I^{d-1}$. Then $\phi \otimes h \simeq \phi \otimes h'$ if and only if $e_{d-1}(\phi) \cup (\mathrm{disc}(h)) = e_{d-1}(\phi) \cup (\mathrm{disc}(h'))$.*

Proof. The hermitian forms $\phi \otimes h$ and $\phi \otimes h'$ are isomorphic if and only if $\phi \otimes (h \oplus (-h'))$ is hyperbolic. By 2.1.3, this is equivalent with $e_{d-1}(\phi) \cup \mathrm{disc}(h \oplus (-h')) = 0$. Note that as $\dim_k(D)$ is even, $\mathrm{disc}(-h') = \mathrm{disc}(h')$. Therefore

$$e_{d-1}(\phi) \cup (\mathrm{disc}(h \oplus (-h'))) = e_{d-1}(\phi) \cup (\mathrm{disc}(h)) + e_{d-1}(\phi) \cup (\mathrm{disc}(h')),$$

hence the corollary is proved.

Let us denote by J_2 the sub $W(k)$–module of J consisting of the classes of the hermitian forms h such that $(\mathrm{disc}(h)) = 0$.

Corollary 2.1.5 *Suppose that D is a quaternion algebra, and that σ is of the first kind and of the orthogonal type. Then $I^{d-1} J_2 = 0$.*

Proof. This is an immediate consequence of 2.1.4.

§3. Multiples of trace forms

Let L and L' be two G–Galois algebras. The aim of this section is to prove a result concerning multiples of trace forms (see 3.1.2) that was conjectured in [1], and to derive some consequences for generalized self–dual normal bases. Suppose that $\mathrm{cd}_2(\Gamma_k) \leq d$.

Theorem 3.1.1. *Let $\phi \in I^{d-1}$. Then $\phi \otimes q_L \simeq_G \phi \otimes q_{L'}$ if and only if $e_{d-1}(\phi) \cup x_L = e_{d-1}(\phi) \cup x_{L'}$ for all $x \in H^1(G, \mathbf{Z}/2\mathbf{Z})$.*

Special cases of this have been proved in [1], [4], [5], [6], [9] and [12].

Proof. The condition is necessary by 1.4.3. Let us prove that it is also sufficient. By [3], 4.1 and [7], 2.3.1 we can assume that k is perfect. Set $A = k[G]$, and let us denote by $\sigma_A : A \to A$ the canonical involution. Let R_A be the radical of the algebra A, and set

$\overline{A} = A/R$. Then the projection $A \to \overline{A}$ induces a bijection of pointed sets $H^1(k, U_A) \to H^1(k, U_{\overline{A}})$. We have

$$\overline{A} \simeq A_1 \times \ldots \times A_s \times (A_{s+1} \times A'_{s+1}) \times \ldots \times (A_m \times A'_m),$$

where A_i is a simple algebra for all $i = 1, \ldots, m$, with $\sigma(A_i) = A_i$ for $i = 1, \ldots, s$ and $\sigma(A_i) = A'_i$ for $i = s+1, \ldots, m$. Let $\sigma_i : A_i \to A_i$ be the restriction of σ_A to A_i for $i = 1, \ldots, s$, and let us denote by $\sigma_i : A_i \times A'_i \to A_i \to A_i \times A'_i$ the restriction of σ_A to $A_i \times A'_i$ if $i = s+1, \ldots, m$. Let F_i be the maximal subfield of the center of A_i such that σ_i is F_i–linear if $i = 1, \ldots, s$, and let U_i be the norm–one–group of (A_i, σ_i). For $i = s+1, \ldots, m$, let F_i be the center of A_i, and let U_i be the norm–one–group of $((A_i \times A_i), \sigma_i)$. Then U_i is a linear algebraic group defined over F_i for all $i = 1, \ldots, m$. We have a bijection of pointed sets

$$H^1(k, U_A) \to \prod_{i=1,\ldots,m} H^1(F_i, U_i).$$

If $i = s+1, \ldots, m$, then U_i is a general linear group, hence $H^1(F_i, U_i) = 0$. Hence we have a bijection of pointed sets

$$H^1(k, U_A) \to \prod_{i=1,\ldots,s} H^1(F_i, U_i).$$

Let us denote by u_i, $u'_i \in H^1(F_i, U_i)$, $i = 1, \ldots, s$, the images of $u(L)$, $u(L') \in H^1(k, U_A)$.

For all $i = 1, \ldots, s$, the simple algebra A_i is a matrix algebra over a division algebra with involution D_i, and the classes u_i, u'_i correspond to isomorphism classes of hermitian forms h_i, h'_i over D_i.

Let $r = \dim(\phi)$, and set $B = M_r(A)$. Let us denote by $\sigma_B : B \to B$ the involution induced by σ_A and the transposition, i.e. $\sigma_B(a_{i,j}) = (\sigma_A(a_{j,i}))$ for all $a_{i,j} \in A$. Let R_B be the radical of B, and set $\overline{B} = B/R_B$.

We have

$$\overline{B} \simeq M_r(A_1) \times \ldots \times M_r(A_m).$$

As above, we get a bijection of pointed sets

$$H^1(k, U_B) \to \prod_{i=1,\ldots,s} H^1(F_i, U_{M_r(A_i)}).$$

Sending a G–quadratic form to its tensor product with the quadratic form ϕ gives us a map $f : H^1(k, U_A) \to H^1(k, U_B)$. The map f induces $\overline{f} : H^1(k, U_{\overline{A}}) \to H^1(k, U_{\overline{B}})$, and

$$f_i : H^1(F_i, U_i) \to H^1(k, U_{M_r(A_i)})$$

for all $i = 1, \ldots, s$. The image of the isomorphism class of the hermitian form h_i is the hermitian form $\phi \otimes h_i$.

Let us show that for all $i = 1, \ldots, s$, we have $\phi \otimes h_i \simeq \phi \otimes h'_i$. This is equivalent with proving that $\phi \otimes (h_i \oplus (-h'_i))$ is hyperbolic. If U_i is unitary or symplectic, then this follows from Theorem 2.1.1. (b) and (c). Suppose that U_i is orthogonal. Then $A_i = M_{n_i}(D_i)$, where $D_i = F_i$ or D_i is a quaternion field with center F_i (cf. [15], Chap. 8, 13.5. (ii)). We have $(U_i/U_i^0)(k_s) \simeq \mathbf{Z}/2\mathbf{Z}$. Let $\iota : \Gamma_{F_i} \to \Gamma_k$ be the inclusion, and let us consider

$$\delta_i : \Gamma_{F_i} \xrightarrow{\iota} \Gamma_k \xrightarrow{\phi_L} G \to U_G(k_s) \to U_i(k_s) \simeq \mathbf{Z}/2\mathbf{Z}$$

and

$$\delta'_i : \Gamma_i \xrightarrow{\iota} \Gamma_k \xrightarrow{\phi_{L'}} G \to U_G(k_s) \to U_i(k_s) \simeq \mathbf{Z}/2\mathbf{Z}.$$

Then δ_i, δ'_i are 1–cocycles that define elements (δ_i), $(\delta'_i) \in H^1(F_i, \mathbf{Z}/2\mathbf{Z})$ corresponding to the relative discriminants $\mathrm{disc}(h_i)$ and $\mathrm{disc}(h'_i)$ of the hermitian forms h_i and h'_i with respect to the unit hermitian form h_0.

Note that $\delta_i = \iota x_L$ and $\delta_i = \iota x_{L'}$ for all $x \in H^1(G, \mathbf{Z}/2\mathbf{Z})$. By hypothesis, we have $e_{d-1}(\phi) \cup x_L = e_{d-1}(\phi) \cup x_{L'}$ for all $x \in H^1(G, \mathbf{Z}/2\mathbf{Z})$. This implies that

$$e_{d-1}(\phi) \cup (\mathrm{disc}(h_i)) = e_{d-1}(\phi) \cup (\mathrm{disc}(h'_i))$$

for all $i = 1, \ldots, s$. By cor. 2.1.4, we conclude that the hermitian forms $\phi \otimes h_i$ and $\phi \otimes h'_i$ are isomorphic, and hence the theorem is proved.

Recall that for any G–quadratic form q, we denote by $[m]q$ the orthogonal sum of m copies of q, in other words the quadratic form $< 1, \ldots, 1 > \otimes q$. Let us denote by $\epsilon_{d-1} \in H^{d-1}(k)$ the cup product of $d-1$ copies of $(-1) \in H^1(k)$. The following is an immediate consequence of 3.1.1 :

Corollary 3.1.2 *Let L and L' be two G–Galois algebras. Then $[2^{d-1}]q_L \simeq_G [2^{d-1}]q_{L'}$ if and only if $\epsilon_{d-1} \cup x_L = \epsilon_{d-1} \cup x_{L'}$.*

Let L_0 be the split G–Galois algebra, and let $q_0 = q_{L_0}$ be its trace form. Recall that a G–Galois algebra is said to have a *self–dual normal basis* if $q_L \simeq_G q_0$.

For any positive integer m, we denote by $[m]L$ the product of m copies of the G–Galois algebra L. We say that $[m]L$ *has a self–dual normal basis* if $[m]q_L \simeq_G [m]q_0$. A subalgebra E of L is said to be a *subalgebra of invariants* if there exists a subgroup H of G such that $E = L^H$.

Corollary 3.1.3 *Let L be a G–Galois algebra. Then the algebra $[2^{d-1}]L$ has a self–dual normal basis if and only if the discriminant of every quadratic subalgebra of invariants is a sum of 2^{d-1} squares.*

Proof. Let us denote by q the 2^{d-1}–dimensional unit form, and let $D(q)$ be the set of non–zero elements of k represented by q. Then $a \in D(q)$ if and only if a is a sum of 2^{d-1}

squares in k. It is well–known that $a \in D(q)$ if and only if the quadratic form $q \oplus < -a >$ is isotropic. This is equivalent with the 2^d–fold Pfister form $q \otimes < 1, -a >$ being hyperbolic, hence by 1.2.1 with $\epsilon_{d-1} \cup (a) = 0$.

Let $x \in H^1(G, \mathbf{Z}/2\mathbf{Z})$. The argument above shows that x_L is a sum of 2^{d-1} squares if and only if $\epsilon_{d-1} \cup x_L = 0$. Let $\chi : G \to \mathbf{Z}/2\mathbf{Z}$ the corresponding homomorphism. Let H be the kernel of χ, and let $E_x = L^H$ be the invariant subalgebra. Then E_x is a quadratic subalgebra of L, and its discriminant is equal to x_L.

By 3.1.2, the algebra $[2^{d-1}]L$ has a self–dual normal basis if and only if $\epsilon_{d-1} \cup x_L = 0$ for all $x \in H^1(G, \mathbf{Z}/2\mathbf{Z})$. We have just seen that this is equivalent with the discriminant of the quadratic subalgebra E_x being a sum of 2^{d-1} squares for all $x \in H^1(G, \mathbf{Z}/2\mathbf{Z})$, hence the corollary is proved.

Bibliography

[1] E. Bayer–Fluckiger, Galois cohomology and the trace form, *Jahresber. DMV* **96** (1994), 35–55.

[2] E. Bayer–Fluckiger, Self–dual normal bases and related topics, Proceedings of the conference *Finite Fields and Applications* (Augsburg, 1999), *Springer Verlag* (2001), 25–36.

[3] E. Bayer–Fluckiger and H.W. Lenstra, Jr., Forms in odd degree extensions and self-dual normal bases, *Amer. J. Math.* **112** (1990), 359-373.

[4] E. Bayer–Fluckiger and M. Monsurro, Doubling trace forms, *St. Petersburg J. Math.* **11** (2000), 405–417.

[5] E. Bayer–Fluckiger, M. Monsurro, R. Parimala, R. Schoof, Trace forms of Galois algebras over fields of cohomological dimension ≤ 2, *Pacific J. Math*, **217** (2004), 29-43.

[6] E. Bayer–Fluckiger and J. Morales, Multiples of trace forms in number fields, *AMS Proc. Symposia Pure Math.*, **58.2** (1995), 73–81.

[7] E. Bayer–Fluckiger and J–P. Serre, Torsions quadratiques et bases normales autoduales, *Amer. J. Math.* **116** (1994) 1–64.

[8] G. Berhuy, Cohomological invariants of quaternionic skew–hermitian forms, *Archiv Math* (to appear).

[9] Ph. Chabloz, Anneau de Witt des G–formes et produit des G–formes trace par des formes quadratiques, *J. Algebra* **266** (2003), 338–361.

[10] B. Kahn, La conjecture de Milnor, d'après Voevodsky, *Séminaire Bourbaki* (1996/97), Exp. **834** (juin 1997), *Astérisque* **245** (1997), 379–418.

[11] M. Knus, A. Merkurjev, M. Rost, J–P. Tignol, *The Book of Involutions*, AMS Colloquium Publications, Vol 44 (1998).

[12] M. Monsurro, Pfister forms times trace forms, *Comm. Algebra* **30** (2002), 3391–3402.

[13] D. Orlov, A. Vishik, V. Voedovsky, An exact sequence for Milnor's K–theory with applications to quadratic forms, preprint (2001), arxiv.org/abs/math/0101023

[14] R. Parimala, R. Sridharan and V. Suresh, Hermitian analogue of a theorem of Springer, *J. Algebra* **243** (2001), 780–789.

[15] W. Scharlau, *Quadratic and Hermitian Forms*, Grundlehren der Math. Wiss, Springer–Verlag (1985).

[16] J-P. Serre, *Cohomologie galoisienne*, Lecture Notes in Mathematics, Springer–Verlag (1964 and 1994)

[17] J-P. Serre, *Corps locaux*, Hermann (1968).

[18] V. Voevodsky, Reduced power operations in motivic cohomology, *Publ. Math. IHES* **98** (2003), 1–57.

[19] V. Voevodsky, Motivic cohomology with $\mathbf{Z}/2\mathbf{Z}$–coefficients, *Publ. Math. IHES* **98** (2003), 59–104.

Address

E. Bayer–Fluckiger, Ecole Polytechnique Fédérale de Lausanne, Mathématiques, CSAG–IMB–FSB, Station 8, 1015 Lausanne, Switzerland, eva.bayer@epfl.ch