Cohomological Invariants for G-Galois Algebras and Self-Dual Normal Bases

E. Bayer-Fluckiger and R. Parimala

Received: August 26, 2016

Communicated by Nikita Karpenko

Abstract. We define degree two cohomological invariants for G-Galois algebras over fields of characteristic not 2, and use them to give necessary conditions for the existence of a self–dual normal basis. In some cases (for instance, when the field has cohomological dimension ≤ 2) we show that these conditions are also sufficient.

Introduction

Let k be a field of characteristic $\neq 2$, and let L be a finite degree Galois extension of k. Let $G = \mathrm{Gal}(L/k)$. The *trace form* of L/k is by definition the quadratic form $q_L : L \times L \to k$ defined by $q_L(x,y) = \mathrm{Tr}_{L/k}(xy)$. Note that q_L is a *G-quadratic form*, in other words we have $q_L(gx, gy) = q_L(x,y)$ for all $x, y \in L$. A normal basis $(gx)_{g \in G}$ of L over k is said to be *self-dual* if $q_L(gx, gx) = 1$ and $q_L(gx, hx) = 0$ if $g \neq h$. It is natural to ask which extensions have a self-dual normal basis. This question is investigated in several papers (see for instance [BL 90], [BSe 94], [BPS 13]). It is necessary to work in a more general context than the one of Galois extensions, namely that of *G-Galois algebras* (see for instance [BSe 94], §1); one advantage being that this category is stable by base change of the ground field; the notion of a self-dual normal basis is defined in the same way.

If k is a global field, then the *Hasse principle* holds : a G-Galois algebra has a self-dual normal basis over k if and only if such a basis exists everywhere locally (see [BPS 13]). The present paper completes this result by giving necessary and sufficient conditions for the existence of a self-dual normal basis when k is a local field (cf. §7). The conditions are given in terms of cohomological invariants defined over the ground field k constructed in §3 and §4.

For an arbitrary ground field k, we start with the H^1-invariants defined in [BSe 94], §2. Recall from [BSe 94] that the vanishing of these invariants is a necessary condition for the existence of a self-dual normal basis; it is also sufficient in the case of fields of cohomological dimension 1 (see [BSe 94], Corollary 2.2.2 and Proposition 2.2.4).

Let $k[G]$ be the group algebra of G over k, and let J be its radical; the quotient $k[G]^s = k[G]/J$ is a semisimple k-algebra. Let $\sigma : k[G] \to k[G]$ be the k-linear involution sending g to g^{-1}; it induces an involution $\sigma^s : k[G]^s \to k[G]^s$. The algebra $k[G]^s$ splits as a product of simple algebras. If A is a σ^s-stable simple algebra which is a factor of $k[G]^s$, we denote by σ_A the restriction of σ^s to A, and by E_A the subfield of the center of A fixed by σ_A. We say that A is *orthogonal* if σ_A is the identity on the center of A, and if over a separable closure of k it is induced by a symmetric form, and *unitary* if σ_A is not the identity on the center of A (see 1.3 for details).

Let L be a G-Galois algebra over k, and let us assume that its H^1-invariants are trivial. We then define, for every orthogonal or unitary A as above, cohomology classes in $H^2(k, Z/2Z)$, denoted by $c_A(L)$ in the orthogonal case and by $d_A(L)$ in the unitary case (see §3 and §4). They are invariants of the G-Galois algebra L. They also provide necessary conditions for the existence of a self-dual normal basis (this involves restriction to certain finite degree extensions of k, namely, the extensions E_A/k; see Propositions 3.5 and 4.7 for precise statements). If moreover k has cohomological dimension ≤ 2, then these conditions are also sufficient (Theorem 5.3.). Finally, if k is a local field, then the conditions can be expressed in terms of the invariants $c_A(L)$ and $d_A(L)$, without passing to finite degree extensions (Theorem 7.1). Section 8 applies the results of §7 and the Hasse principle of [BSP 13] to give necessary and sufficient conditions for the existence of a self-dual normal basis when k is a global field (Theorem 8.1).

Section 6 deals with the case of cyclic groups of order a power of 2 over arbitrary fields. We show that at most one of the unitary components A gives rise to a non-trivial invariant $d_A(L)$ (Proposition 6.4 (i)), and that this invariant provides a necessary and sufficient condition for the existence of a self-dual normal basis (Corollary 6.5).

Acknowledgment : The first named author is partially supported by grant 200021-163188 of the Swiss National Science Foundation, and the second named author is partially supported by National Science Foundation grant DMS-1401319.

§1. Definitions, notation and basic facts

1.1. Galois cohomology

We use standard notation in Galois cohomology. If K is a field, we denote by K_s a separable closure of K, and by Γ_K the Galois group $\mathrm{Gal}(K_s/K)$. For any discrete Γ_K-module C, set $H^i(K, C) = H^i(\Gamma_K, C)$. If Γ is a finite or profinite group, set $H^i(\Gamma) = H^i(\Gamma, Z/2Z)$. If U is a K-group scheme, we denote by $H^1(K, U)$ the pointed set $H^1(\Gamma_K, U(K_s))$.

1.2. Algebras with involution and unitary groups

Let K be a field of characteristic $\neq 2$, and let R be a finite dimensional algebra over K. An *involution* of R is a K-linear anti-automorphism $\sigma : R \to R$ such that σ^2 is the identity.

Let us denote by Comm_K the category of commutative K-algebras, and by Group the category of groups. If (R, σ) is an algebra with involution, the functor $\mathrm{Comm}_K \to \mathrm{Group}$ given by $S \mapsto \{x \in R \otimes_K S \mid x\sigma(x) = 1\}$ is the functor of points of a scheme over $\mathrm{Spec}(K)$; we denote it by $U_{R,K}$.

Let $h = \langle 1 \rangle$ be the rank one unit hermitian form over (R, σ), given by $h(x, y) = x\sigma(y)$ for all $x, y \in R$. Then $U_{R,K}$ is the scheme of automorphisms of the hermitian form h. This is a smooth, finitely presented affine group scheme over $\mathrm{Spec}(K)$ (see for instance [BF 15], Appendix A). Moreover, $H^1(K, U_{R,K})$ is in natural bijection with the set of isomorphism classes of rank one hermitian forms over (R, σ) that become isomorphic to h over K_s (see [Se 64], chap. III, §1).

If F is a subfield of K, then $U_{R,F} = \mathrm{R}_{K/F}(U_{R,K})$, where $\mathrm{R}_{K/F}$ denotes Weil restriction of scalars relative to the extension K/F.

Let Z be the center of R, and assume that R is a simple algebra. We say that (R, σ) is a *central simple algebra with involution over* K if the fixed field of σ in Z is equal to K. If (R, σ) is central simple algebra with involution over K, we set $U_R = U_{R,K}$.

1.3. Dévissage

Let G be a finite group and let $k[G]$ be its group algebra over k. The *canonical involution* of $k[G]$ is the k-linear involution $\sigma : k[G] \to k[G]$ such that $\sigma(g) = g^{-1}$ for all $g \in G$. Let J be the radical of $k[G]$, and set $k[G]^s = k[G]/J$; it is a semisimple k-algebra. Since J is stable by σ, we obtain an involution $\sigma^s : k[G]^s \to k[G]^s$. Set $U_G = U_{k[G],k}$ and $U_G^r = U_{k[G]^s,k}$. Let N be the kernel of the natural surjection $U_G \to U_G^r$. Let us define group schemes N_i by setting $N_i(S) = \{x \in N(S) \mid x \equiv 1 \bmod J^i \otimes_k S\}$. Then $1 = N_m \subset N_{m-1} \subset \cdots \subset N_1 = N$, where m is an integer such that $J^m = 0$. Note that J^i/J^{i+1} is a module over the semisimple algebra $k[G]^s$, hence N_i/N_{i-1} is isomorphic to a finite product of additive groups G_a; therefore N is a split unipotent group. This implies that $H^1(k, U_G) = H^1(k, U_G^r)$ (see for instance [Sa 81], Lemme 1.13).

The semisimple algebra $k[G]^s$ is known to be a direct product of simple algebras. Note that $k[G]$ comes by scalar extension from $k_0[G]$ for $k_0 = Q$ or F_p, hence the centers of the factors of $k[G]^s$ are abelian Galois extensions of k of finite degree; some are stable under σ^s (we call them A), and others come in pairs, interchanged by σ^s (we call them B).

If A is a σ^s-stable simple factor of $k[G]^s$, we denote by σ_A the restriction of σ^s to A, by F_A the center of A, and by E_A the subfield of σ_A-invariant elements of F_A. Note that U_A is a group scheme over $\mathrm{Spec}(E_A)$. Similarly, if B is the product of two simple algebras interchanged by σ^s, we denote by E_B the subfield of the center of B fixed by the involution; U_{B,E_B} is a group scheme over $\mathrm{Spec}(E_B)$.

We have $U_G^r \simeq \prod_A \mathrm{R}_{E_A/k}(U_A) \times \prod_B \mathrm{R}_{E_B/k}(U_{B,E_B})$, hence

$$H^1(k, U_G^r) = \prod_A H^1(k, \mathrm{R}_{E_A/k}(U_A)) \times \prod_B H^1(k, \mathrm{R}_{E_B/k}(U_{B,E_B})).$$

Note that $H^1(k, \mathrm{R}_{E_B/k}(U_{B,E_B})) = H^1(E_B, U_{B,E_B}) = 0$ (see for instance [KMRT 98], (29.2)), that $H^1(k, \mathrm{R}_{E_A/k}(U_A)) = H^1(E_A, U_A)$ (see for instance [O 84], 2.3), and that $H^1(k, U_G) = H^1(k, U_G^r)$ (see above). Therefore we have

$$H^1(k, U_G) = \prod_A H^1(E_A, U_A).$$

The algebras with involution (A, σ_A) appearing in this product are of three types :

(a) The involution $\sigma_A : A \to A$ is not the identity on the center F_A of A. Hence F_A/E_A is a quadratic extension. Such an algebra with involution is called *unitary*; the group scheme U_A is of Dynkin type A.

(b) The involution $\sigma_A : A \to A$ is the identity on F_A (which is then equal to E_A), and, over a separable closure of E_A, the involution is induced by a symmetric form. Such an algebra with involution is called *orthogonal*; the group scheme U_A is of Dynkin type B or D.

(c) The involution $\sigma_A : A \to A$ is the identity on F_A (which is then equal to E_A), and, over a separable closure of E_A, the involution is induced by a skew-symmetric form. Such an algebra with involution is called *symplectic*; the group scheme U_A is of Dynkin type C.

1.4. G-quadratic forms

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 $q \simeq_G q'$. It is well-known that G-quadratic forms correspond bijectively to non-degenerate hermitian forms over $(k[G], \sigma)$ (see for instance [BPS 13], 2.1, Example on page 441). The *unit G-form* is by definition the pair $(k[G], q_0)$, where q_0 is the G-form characterized by $q(g, g) = 1$ and $q(g, h) = 0$ if $g \neq h$, for $g, h \in G$.

1.5. Trace forms of G-Galois algebras

If L is an étale k-algebra, we denote by

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

its trace form. Then q_L is a non-degenerate quadratic form over k; if moreover L is a G-Galois algebra, then q_L is a G-quadratic form.

Let L be a G-Galois algebra; then L has a self-dual normal basis over k if and only if q_L is isomorphic to q_0 as a G-quadratic form. Let $\phi : \Gamma_k \to G$ be a continuous homomorphism corresponding to L (see for instance [BSe 94], 1.3). Recall that ϕ is unique up to conjugation. The composition

$$\Gamma_k \xrightarrow{\phi} G \to U_G(k) \to U_G(k_s)$$

is a 1-cocycle $\Gamma_k \to U_G(k_s)$. Let $u(L)$ be its class in the cohomology set $H^1(k, U_G)$; it does not depend on the choice of ϕ. The G-Galois algebra L has a self-dual normal basis over k if and only if $u(L) = 0$, cf. [BSe 94], Corollaire 1.5.2.

Recall from 1.3 that we have

$$H^1(k, U_G) = \prod_A H^1(E_A, U_A).$$

Let $u_A(L)$ be the image of $u(L)$ in $H^1(E_A, U_A)$; note that L has a self-dual normal basis if and only if $u_A(L) = 0$ for every A.

Let A be as above. Composing the injection $G \to U_G(k)$ with the natural map $U_G(k) \to U_G^r(k) \to \mathrm{R}_{E_A/k}(U_A)(k) = U_A(E_A)$, we obtain a homomorphism $G \to U_A(E_A)$, denoted by i_A.

Let $\phi_A : \Gamma_{E_A} \to \Gamma_k \to G$ be the composition of $\phi : \Gamma_k \to G$ with the inclusion of Γ_{E_A} in Γ_k. Composing ϕ_A with the map $i_A : G \to U_A(E_A)$ defined above we obtain a 1-cocycle $\Gamma_{E_A} \to U_A(k_s)$. The class of this 1-cocycle in $H^1(E_A, U_A)$ is equal to $u_A(L)$.

§2. The H^1-condition

Let L be a G-Galois algebra over k, and let $\phi : \Gamma_k \to G$ be a homomorphism corresponding to L. Let n be an integer ≥ 1. Then ϕ induces a homomorphism

$$\phi^* : H^n(G) \to H^n(k, Z/2Z).$$

Note that ϕ^* is independent of the choice of ϕ in its conjugacy class (see [Se 68], chap. VII, proposition 3). For all $x \in H^n(G)$, set $x_L = \phi^*(x)$.

Proposition 2.1. *If L has a self-dual normal basis over k, then for all $x \in H^1(G)$ we have $x_L = 0$.*

Proof. See [BSe 94], Corollaire 2.2.2.

If $\mathrm{cd}_2(\Gamma_k) \leq 1$, then L has a self-dual normal basis over k if and only if $x_L = 0$ for all $x \in H^1(G)$, see [BSe 94], Proposition 2.2.4.

We say that *the H^1-condition is satisfied* if $x_L = 0$ for all $x \in H^1(G)$. Let G^2 be the subgroup of G generated by the squares of elements of G. Note that G/G^2 is an elementary abelian 2-group, and that the H^1-condition means that the homomorphism $\Gamma_k \to G \to G/G^2$ induced by ϕ is trivial, i.e. $\phi(\Gamma_k) \subset G^2$.

§3. Orthogonal invariants

We keep the notation of the previous sections. In particular, G is a finite group, L is a G-Galois algebra, and $\phi : \Gamma_k \to G$ is a homomorphism corresponding to L. Let us suppose that the H^1-condition is satisfied.

Let A be an *orthogonal* σ^s-stable central simple factor of $k[G]^s$ (see 1.3), and recall that the center of A is denoted by E_A. Let us denote by $\langle A \rangle$ the subgroup of $\mathrm{Br}(E_A)$ generated by the class of the algebra A. Note that since $\sigma_A : A \to A$ is an orthogonal involution, this class has order at most 2, hence $\langle A \rangle$ is a subgroup of $\mathrm{Br}_2(E_A)$.

The aim of this section is to define two invariants : an invariant $c_A(L) \in H^2(k)$ of the G–Galois algebra L, and an invariant $\mathrm{clif}_A(q_L) \in \mathrm{Br}_2(E_A)/\langle A \rangle$ of the G-form q_L. We shall compare these two invariants (cf. Theorem 3.3), and give a necessary condition for the existence of self-dual normal bases (Corollary 3.5).

Let U_A^0 be the connected component of the identity in U_A. Let $i_A : G \to U_A(E_A)$ be the homomorphism defined in 1.5, and let $\pi : U_A(E_A) \to U_A(E_A)/U_A^0(E_A)$ be the projection. Since $U_A(E_A)/U_A^0(E_A)$ is of order ≤ 2, we have $\pi(i_A(G^2)) = 0$; i.e. $i_A(G^2) \subset U_A^0(E_A)$.

Let $\tilde{U}_A$ be the Spin group of (A, σ); note that if $\dim_k(A) \geq 3$, then $\tilde{U}_A$ is the universal cover of U_A^0. Let $s : \tilde{U}_A \to U_A^0$ be the covering map. We have an exact sequence of algebraic groups over E_A

$$1 \to Z/2Z \to \tilde{U}_A \xrightarrow{s} U_A^0 \to 1.$$

Let us consider the associated cohomology exact sequence

$$\tilde{U}_A(E_A) \xrightarrow{s} U_A^0(E_A) \xrightarrow{\delta} H^1(E_A).$$

Lemma 3.1. *We have $i_A(G^2) \subset s(\tilde{U}_A(E_A))$.*

Proof. In view of the above exact sequence, it suffices to prove that $\delta(i_A(G^2)) = 0$. In order to prove this, let us first assume that A is not split. Then we have $U_A(E_A) = U_A^0(E_A)$ (cf. [K 69], Lemma 1 b, see also [B 94], cor. 2). Since $H^1(E_A)$ is a 2-torsion group and since $i_A(G^2) \subset U_A^0(E_A)$, this implies that $\delta(i_A(G^2)) = 0$, as claimed. Assume now that A is split. Then U_A is the orthogonal group of a quadratic form q; let $\mathrm{sn} : U_A(E_A) \to H^1(E_A)$ be the associated spinor norm, and note that sn is a group homomorphism (see for instance [L 05], Chapter 5, Theorem 1.13). The homomorphism sn depends on the choice of the quadratic form q with orthogonal group U_A, but its restriction to U_A^0 does not depend on this choice. Note that $\delta : U_A^0(E_A) \to H^1(E_A)$ is the restriction of sn to $U_A^0(E_A)$. Therefore for all $g \in G$, we have $\delta(i_A(g^2)) = \mathrm{sn}(i_A(g))^2$, and since $H^1(E_A)$ is a 2-torsion group, this implies that $\delta(i_A(G^2)) = 0$. This completes the proof of the lemma.

Let H be a subgroup of G^2. By Lemma 3.1, we have $i_A(H) \subset s(\tilde{U}_A(E_A))$. Let

$$V_A^H = \tilde{U}_A(E_A) \times_{U_A^0(E_A)} H$$

be the fibered product of $s : \tilde{U}_A(E_A) \to U_A^0(E_A)$ and $i_A : H \to U_A^0(E_A)$. Therefore we have a central extension

$$1 \to Z/2Z \to V_A^H \xrightarrow{p} H \to 1,$$

where p is the projection to the factor H. Note that the surjectivity of p follows from the fact that by Lemma 3.1 every element of $i_A(H)$ has a preimage in $\tilde{U}_A(E_A)$.

Let us denote by

$$e_A^H \in H^2(H)$$

the cohomology class corresponding to the extension V_A^H. If $\phi(\Gamma_k) \subset H$, we denote by

$$\phi^* : H^2(H) \to H^2(k)$$

the homomorphism induced by $\phi : \Gamma_k \to H$.

Proposition 3.2. *Let $\psi : \Gamma_k \to G$ be another continuous homomorphism corresponding to the G–Galois algebra L. Set $H_\phi = \phi(\Gamma_k)$ and $H_\psi = \psi(\Gamma_k)$. Then we have*

$$\phi^*(e_A^{H_\phi}) = \psi^*(e_A^{H_\psi}) \quad in \quad H^2(k).$$

Proof. We have $\psi = \mathrm{Int}(g) \circ \phi$ for some $g \in G$. Note that $i_A(g) \in U_A(E_A)$, and that $\mathrm{Int}(i_A(g))$ is an automorphism of $U_A^0(E_A)$. Any automorphism of $U_A^0(E_A)$ can be lifted to an automorphism of $\tilde{U}_A(E_A)$; indeed, such a lift exists over a separable closure, and is unique, hence defined over the ground field. Let $f : \tilde{U}_A(E_A) \to \tilde{U}_A(E_A)$ be a lift of $\mathrm{Int}(i_A(g))$. Then f induces an isomorphism $V_A^{H_\phi} \to V_A^{H_\psi}$, which sends H_ϕ to H_ψ, and is the identity on $Z/2Z$. This implies that $\phi^*(e_A^{H_\phi}) = \psi^*(e_A^{H_\psi})$ in $H^2(k)$.

The invariant $c_A(L)$

Recall that we assume that the H^1-condition is satisfied. We now choose for H the image $\phi(\Gamma_k)$ of Γ_k in G, and set $V_A = V_A^H$, $e_A = e_A^H$. We denote by $c_A(L)$ the class of $\phi^*(e_A)$ in $H^2(k)$; Proposition 3.2 shows that this class does not depend on the choice of $\phi : \Gamma_k \to G$ defining the G–Galois algebra L. Since $H^2(k) \simeq \mathrm{Br}_2(k)$, we can also consider $c_A(L)$ as an element of $\mathrm{Br}_2(k)$.

Recall that the G-trace form q_L determines a rank one hermitian form over (A, σ_A). We want to relate $c_A(L)$ to the Clifford invariant of this hermitian form.

The invariant $\mathrm{clif}_A(q_L)$

The map $i_A : H \to U_A^0(E_A)$ induces a map of pointed sets

$$i_A : H^1(E_A, H) \to H^1(E_A, U_A^0).$$

Let $u_A^0(L)$ be the image of $[\phi_A] \in H^1(E_A, H)$ by this map. Then the element $u_A(L)$ defined in 1.5 is the image of $u_A^0(L)$ under the further composition with the map $H^1(E_A, U_A^0) \to H^1(E_A, U_A)$.

Let us consider the exact sequence $1 \to Z/2Z \to \tilde{U}_A \to U_A^0 \to 1$, and let δ be the connecting map $H^1(E_A, U_A^0) \to H^2(E_A) \simeq \mathrm{Br}_2(E_A)$ of the associated cohomology exact sequence. Recall that $\langle A \rangle$ is the subgroup of $\mathrm{Br}_2(E_A)$ generated by the class of the algebra A. The *Clifford invariant* of q_L at A is by definition the image of $\delta(u_A^0(L))$ in $\mathrm{Br}_2(E_A)/\langle A \rangle$. Let us denote it by $\mathrm{clif}_A(q_L)$.

Theorem 3.3. *The image of* $\mathrm{Res}_{E_A/k}(c_A(L))$ *in* $\mathrm{Br}_2(E_A)/\langle A \rangle$ *is equal to* $\mathrm{clif}_A(q_L)$.

We need the following lemma :

Lemma 3.4. *Let K be a field, let C be a finite group, and let $f : \Gamma_K \to C$ be a continuous homomorphism. Let us denote by $[f] \in H^1(K, C)$ the corresponding cohomology class. Let*

$$1 \to Z/2Z \to V \to C \to 1$$

be a central extension with trivial Γ_K-action. Let $[e] \in H^2(C)$ be the class of a 2-cocycle $e : C \times C \to Z/2Z$ representing this extension. Let $\partial : H^1(K, C) \to H^2(K)$ be the connecting map associated to the above exact sequence, and let $f^* : H^2(C) \to H^2(K)$ be the map induced by f. Then

$$f^*([e]) = \partial([f]).$$

Proof. This follows from a direct computation. For all $\sigma, \tau \in \Gamma_K$, we have $f^*(e)(\sigma, \tau) = e(f(\sigma), f(\tau)) = x_{f(\sigma)} x_{f(\tau)} x^{-1}_{f(\sigma\tau)}$, where $x : C \to V$ is a section. On the other hand, $(\partial f)(\sigma, \tau) = x_{f(\sigma)}{}^{f(\sigma)}(x_{f(\tau)}) x^{-1}_{f(\sigma\tau)}$, and this is equal to $x_{f(\sigma)} x_{f(\tau)} x^{-1}_{f(\sigma\tau)}$, since the action of Γ_k on V is trivial.

Proof of Theorem 3.3. Let $\partial : H^1(E_A, H) \to H^2(E_A)$ be the connecting map of the cohomology exact sequence associated to the exact sequence

$$1 \to Z/2Z \to V_A \to H \to 1$$

with all the groups having trivial Γ_{E_A}-action. Recall that $\phi_A : \Gamma_{E_A} \to \Gamma_k \to H$ is the composition of $\phi : \Gamma_k \to H$ with the inclusion of Γ_{E_A} into Γ_k. By Lemma 3.4 we have $\partial([\phi_A]) = \phi_A^*(e_A) = \mathrm{Res}_{E_A/k}(\phi^*(e_A)) = \mathrm{Res}_{E_A/k}(c_A(L))$. In view of the commutative diagram of Γ_{E_A}-groups

$$\begin{array}{ccccccccc} 1 & \to & Z/2Z & \to & \tilde{U}_A(k_s) & \to & U_A^0(k_s) & \to & 1 \\ & & \uparrow & & \uparrow & & \uparrow & & \\ 1 & \to & Z/2Z & \to & V_A & \to & H & \to & 1 \end{array}$$

we have $\delta(u_A^0(L)) = \partial([\phi_A])$. Therefore we obtain $\mathrm{Res}_{E_A/k}(c_A(L)) = \delta(u_A^0(L))$. Since the class of $\delta(u_A^0(L))$ in $\mathrm{Br}_2(E_A)/\langle A \rangle$ is equal to $\mathrm{clif}_A(q_L)$ by definition, this completes the proof of the theorem.

Proposition 3.5. *If L has a self-dual normal basis over k, then $\mathrm{Res}_{E_A/k}(c_A(L))$ is trivial in $\mathrm{Br}_2(E_A)/\langle A \rangle$.*

Proof. Since L has a self-dual normal basis over k, the class $u_A(L)$ corresponds to the class of the rank one unit hermitian form $\langle 1 \rangle$ in $H^1(E_A, U_A)$. As $\langle 1 \rangle$ corresponds to the trivial cocycle in $Z^1(E_A, U_A^0)$, its Clifford invariant is trivial, in other words, $\mathrm{clif}_A(q_L)$ is trivial. By Theorem 3.3 the image of $\mathrm{Res}_{E_A/k}(c_A(L))$ in $\mathrm{Br}_2(E_A)/\langle A \rangle$ is equal to $\mathrm{clif}_A(q_L)$, hence the proposition is proved.

We conclude this section with an example where $c_A(L) \neq 0$, but $\mathrm{Res}_{E_A/k}(c_A(L)) = 0$ (and hence $\mathrm{clif}_A(q_L) = 0$) :

Example 3.6. Let $G = A_5$, the alternating group, and assume that $k = Q$. Let A be a factor of $k[G]$ corresponding to a degree 3 orthogonal representation of G; then $A = M_3(E_A)$ with $E_A = k(\sqrt{5})$, and the involution σ_A is induced by the unit form $\langle 1,1,1\rangle$. Let $\epsilon \in G$ be a product of two disjoint transpositions.

Let $z \in k^\times$, and let $\psi : \Gamma_k \to \{1,\epsilon\}$ be the corresponding quadratic character. Let $\phi : \Gamma_k \to G$ be given by $\phi = \iota \circ \psi$, where $\iota : \{1,\epsilon\} \to G$ is the inclusion. Let L be the G-Galois algebra corresponding to ϕ. Set $H = \{1,\epsilon\}$, and note that the image of ϕ is contained in H. Set $N = k[X]/(X^2 - z)$; then we have $L = \mathrm{Ind}_H^G(N)$.

Note that ϵ lifts to an element of order 4 in $\tilde{A}_5$, hence also in $\tilde{U}_A(E_A)$. Therefore the extension $1 \to Z/2Z \to V_A^H \to H \to 1$ is not trivial; the group V_A^H is cyclic of order 4. Recall that e_A is the class of this extension in $H^2(H)$; hence e_A is the only non-trivial element of $H^2(H)$. By definition, we have $c_A(L) = \phi^*(e_A)$, and this is equal to the cup product $(z)(z) = (-1)(z)$ in $H^2(k)$.

Set $z = 11$. Then $c_A(L) = (-1)(11)$ is not trivial in $H^2(k)$. On the other hand, since $E_A = k(\sqrt{5})$, we have $\mathrm{Res}_{E_A/k}(c_A(L)) = 0$ in $H^2(E_A)$. Note that the subgroup $\langle A\rangle$ of $\mathrm{Br}_2(E_A)$ is trivial, and recall that $\mathrm{clif}_A(q_L) = \mathrm{Res}_{E_A/k}(c_A(L))$ in $\mathrm{Br}_2(E_A) \simeq H^2(E_A)$ by Theorem 3.3; therefore we have $\mathrm{clif}_A(q_L) = 0$.

§4. Unitary invariants

We keep the notation of the previous sections : G is a finite group, L is a G–Galois algebra, and $\phi : \Gamma_k \to G$ is a homomorphism associated to L. We suppose that the H^1-condition is satisfied by $\phi : \Gamma_k \to G$, hence $\phi(\Gamma_k)$ is a subgroup of G^2. Let A be a *unitary* σ^s-stable central simple factor of $k[G]^s$ (see 1.3). We denote by F_A be the center of A; note that F_A is a quadratic extension of E_A.

Using the same strategy as in §3, we first define an element of $H^2(k)$ which is an invariant of the G-Galois algebra L. We then consider the hermitian form h_A over (A,σ) determined by q_L, and recall the definition of the discriminant of this form, thereby obtaining an element of $\mathrm{Br}_2(E_A)$. This is an invariant of the hermitian form h_A, and hence also of the G–form q_L. We then show that the restriction of the first invariant to $H^2(E_A)$ is equal to the second one (see Theorem 4.5).

We start by recording some facts from Galois cohomology.

Let E be a field of characteristic $\neq 2$, and let E_s be a separable closure of E. Let F be a quadratic extension of E, let $x \mapsto \overline{x}$ the non-trivial automorphism of F over E, and let $F^{\times 1}$ be the subgroup of $F^\times$ consisting of the $x \in F$ such that $x\overline{x} = 1$. Let $\mathrm{N} : F \to E$, given by $\mathrm{N}(x) = x\overline{x}$, be the norm map. We denote by $[F]$ the class of the quadratic extension F/E in $H^1(E)$. For all $x \in E^\times$, we denote by (x) the class of x in $E^\times/E^{\times 2}$, and by $[x]$ the class of x in $E^\times/\mathrm{N}(F^\times)$.

Lemma 4.1. (a) *The connecting homomorphism* $E^\times \to H^1(E, \mathrm{R}^1_{F/E}G_m)$ *associated to the exact sequence* $1 \to \mathrm{R}^1_{F/E}G_m \to \mathrm{R}_{F/E}G_m \xrightarrow{\mathrm{N}} G_m \to 1$ *induces an isomorphism* $\alpha : E^\times/\mathrm{N}(F^\times) \to H^1(E, \mathrm{R}^1_{F/E}G_m)$.
(b) *Let* $x \in E^\times$, *and let* $f_x : \Gamma_E \to \mathrm{R}^1_{F/E}G_m(E_s)$ *be defined by* $f_x(\gamma) = y^{-1}\gamma(y)$, *where* $y \in (F \otimes_E E_s)^\times$ *is such that* $\mathrm{N}(y) = x$. *Then we have* $\alpha((x)) = [f_x]$.

Proof. (a) follows from Hilbert's theorem 90, and (b) from the definition of the connecting homomorphism.

¿From now on, we identify $E^\times/\mathrm{N}(F^\times)$ and $H^1(E, \mathrm{R}^1_{F/E}G_m)$ via the isomorphism α.

Lemma 4.2. *Let* $1 \to Z/2Z \to \mathrm{R}^1_{F/E}G_m \xrightarrow{s} \mathrm{R}^1_{F/E}G_m \to 1$ *be the exact sequence of linear algebraic groups with s the squaring map. Let* $\delta : H^1(E, \mathrm{R}^1_{F/E}G_m) \to H^2(E)$ *be the connecting homomorphism associated to this exact sequence. Identifying* $H^1(E, \mathrm{R}^1_{F/E}G_m)$ *with* $E^\times/\mathrm{N}(F^\times)$ *via* α, *we have*

$$\delta([x]) = (x)[F] \in H^2(E)$$

for all $x \in E^\times$, *where* $(x)[F]$ *denotes the cup product of* $(x), [F] \in H^1(E)$.

Proof. A 2-cocycle associated to $(x)[F] \in H^2(E)$ is given by $f(\sigma, \tau)$ such that $f(\sigma, \tau) = 1$ if the restriction of σ to $E(\sqrt{x})$ is the identity, or if the restriction of τ to F is the identity, and $f(\sigma, \tau) = -1$ otherwise. Let us check that the cohomology class of f in $H^2(E)$ is equal to $\delta([x])$. Let $y \in (F \otimes_E E_s)^\times$ be such that $\mathrm{N}_{F\otimes_E E_s/E_s}(y) = y\overline{y} = x$. A 1-cocycle g in $Z^1(E, \mathrm{R}^1_{F/E}G_m)$ associated to $[x]$ is given by $g(\sigma) = y^{-1}\sigma(y)$ for $\sigma \in \Gamma_E$. For all $\tau \in \Gamma_E$, set $z_\tau = y^{-1}\sqrt{x}$ if the restriction of τ to F is not the identity, and $z_\tau = 1$ otherwise. Then $\mathrm{N}_{F\otimes_E E_s/E_s}(z_\tau) = z_\tau\overline{z_\tau} = (y^{-1}\sqrt{x})(\overline{y}^{-1}\sqrt{x})$ if the restriction of τ to F is not the identity. Since $y\overline{y} = x$, we have $z_\tau \in \mathrm{R}^1_{F/E}G_m(E_s)$. Further, $s(z_\tau) = y^{-2}x = y^{-1}\tau(y)$ if the restriction of τ to F is not the identity, and $s(z_\tau) = 1 = y^{-1}\tau(y)$ otherwise. Thus $\delta(g)(\sigma, \tau) = z_\sigma{}^\sigma(z_\tau)z_{\sigma\tau}^{-1}$. It is straightforward to check that $\delta(g)(\sigma, \tau) = 1$ if the restriction of σ to $E(\sqrt{x})$ is the identity, or the restriction of τ to F is the identity, and that $\delta(g)(\sigma, \tau) = -1$ otherwise. This is precisely the cocycle f, hence we have $\delta([x]) = (x)[F]$ in $H^2(E)$. This concludes the proof of the lemma.

Lemma 4.3. *We have an injective homomorphism* $E^\times/\mathrm{N}(F^\times) \to \mathrm{Br}_2(E)$ *defined by* $[x] \mapsto (x, F/E)$.

Proof. Indeed, the class of the quaternion algebra $(x, F/E)$ is trivial in $\mathrm{Br}_2(E)$ if and only if $x \in \mathrm{N}(F^\times)$.

We now define an invariant $d_A(L) \in H^2(k, Z/2Z)$ of the G-Galois algebra L.

The invariant $d_A(L)$

Recall that $F_A^{\times 1}$ is the subgroup of $F_A^\times$ consisting of the $x \in F_A$ such that $x\sigma_A(x) = 1$; in other words, $F_A^{\times 1} = \mathrm{R}^1_{F_A/E_A}G_m(E_A)$. We denote by

$s : \mathrm{R}^1_{F_A/E_A} G_m \to \mathrm{R}^1_{F_A/E_A} G_m$ the squaring map, and by $n : U_A \to \mathrm{R}^1_{F_A/E_A} G_m$ the reduced norm. Recall that $i_A : G \to U_A(E_A)$ is the homomorphism defined in 1.5; we have $n(i_A(G^2)) \subset s(F_A^{\times 1})$.

Let H be a subgroup of G^2. Let $V_A^H = F_A^{\times 1} \times_{F_A^{\times 1}} H$ be the fibered product of $s : F_A^{\times 1} \to F_A^{\times 1}$ and $n \circ i_A : H \to F_A^{\times 1}$. Then the sequence

$$1 \to Z/2Z \to V_A^H \to H \to 1$$

is exact. Note that the surjectivity follows from the fact that $n(i_A(H)) \subset s(F_A^{\times 1})$. Therefore V_A^H is a central extension of H by $Z/2Z$. Recall that the H^1-condition implies that $\phi(\Gamma_k) \subset G^2$.

Proposition 4.4. *Let $\psi : \Gamma_k \to G$ be another continuous homomorphism corresponding to the G–Galois algebra L. Set $H_\phi = \phi(\Gamma_k)$ and $H_\psi = \psi(\Gamma_k)$. Then we have*

$$\phi^*(e_A^{H_\phi}) = \psi^*(e_A^{H_\psi}) \quad in \quad H^2(k).$$

Proof. We have $\psi = \mathrm{Int}(g) \circ \phi$ for some $g \in G$. The map $F_A^{\times 1} \times_{F^{\times 1}} H_\phi \to F_A^{\times 1} \times_{F^{\times 1}} H_\psi$, given by $(x, y) \to (x, gyg^{-1})$, gives rise to an isomorphism $V_A^{H_\phi} \to V_A^{H_\psi}$ that is the identity on $Z/2Z$ and sends H_ϕ to H_ψ. This implies that $\phi^*(e_A^{H_\phi}) = \psi^*(e_A^{H_\psi})$ in $H^2(k)$.

We now choose for H the image $\phi(\Gamma_k)$ of Γ_k in G, and set $V_A = V_A^H$, $e_A = e_A^H$.

Notation. Let us denote by $d_A(L)$ the class of $\phi^*(e_A)$ in $H^2(k)$; Proposition 4.4 shows that this class is independent of the choice of $\phi : \Gamma_k \to G$ defining the G–Galois algebra L.

We define the discriminant of the G-form q_L at A, and compare it with the cohomology class $d_A(L)$.

The invariant $\mathrm{disc}_A(q_L)$

Recall that composing $\phi_A : \Gamma_{E_A} \to H$ with the map $i_A : H \to U_A(k_s)$ we obtain a 1-cocycle $\Gamma_{E_A} \to U_A(k_s)$, the class of which in $H^1(E_A, U_A)$ is $u_A(L)$. The reduced norm $n : U_A \to \mathrm{R}^1_{F_A/E_A} G_m$ induces a map $n : H^1(E_A, U_A) \to E_A^\times/\mathrm{N}(F_A^\times)$.

Notation. Set $\mathrm{disc}_A(q_L) = (n(u_A(L)), F_A/E_A)$ in $\mathrm{Br}_2(E_A)$.

Note that this is well–defined by Lemma 4.3. Since we have $\mathrm{Br}_2(E_A) \simeq H^2(E_A)$, we can also consider $\mathrm{disc}_A(q_L)$ as an element of $H^2(E_A)$. Then $\mathrm{disc}_A(q_L)$ is given by the cup product $n(u_A(L)).[F_A]$ in $H^2(E_A)$. This invariant is related to the previously defined invariant $d_A(L)$ as follows :

Theorem 4.5. *We have $\mathrm{disc}_A(q_L) = \mathrm{Res}_{E_A/k}(d_A(L))$ in $H^2(E_A)$.*

Proof. Let $\partial : H^1(E_A, H) \to H^2(E_A)$ be the connecting map of the exact sequence

$$1 \to Z/2Z \to V_A \to H \to 1$$

with all the groups having trivial Γ_{E_A}-action. By Lemma 3.4 we have

$$\partial([\phi_A]) = \phi_A^*(e_A) = \mathrm{Res}_{E_A/k}(\phi^*(e_A)) = \mathrm{Res}_{E_A/k}(d_A(L)).$$

We have the commutative diagram

$$\begin{array}{ccccccccc} 1 & \to & Z/2Z & \to & V_A & \to & H & \to & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \to & Z/2Z & \to & \mathrm{R}^1_{F_A/E_A}G_m(k_s) & \xrightarrow{s} & \mathrm{R}^1_{F_A/E_A}G_m(k_s) & \to & 1 \end{array}$$

where the second vertical map is the projection on the first factor, and the third one is $H \xrightarrow{i_A} U_A(E_A) \xrightarrow{n} \mathrm{R}^1_{F_A/E_A}G_m(E_A)$.

Let $\delta : H^1(E, \mathrm{R}^1_{F_A/E_A}G_m) \to H^2(E_A)$ be the connecting homomorphism associated to the exact sequence

$$1 \to Z/2Z \to \mathrm{R}^1_{F_A/E_A}G_m \xrightarrow{s} \mathrm{R}^1_{F_A/E_A}G_m \to 1.$$

By the commutativity of the above diagram, we have $\delta([n(u_A(L))]) = \partial([\phi_A])$. Hence we have $\mathrm{Res}_{E_A/k}(d_A(L)) = \delta([n(u_A(L)]))$. We have $\delta([n(u_A(L))]) = (n(u_A(L))).[F_A]$ by Lemma 4.2 and hence $\mathrm{Res}_{E_A/k}(d_A(L)) = \mathrm{disc}_A(q_L)$, as claimed.

Lemma 4.6. *If q_L corresponds to the hermitian form $\langle z_A\rangle$ over (A, σ_A), then we have*

$$\mathrm{disc}_A(q_L) = (n(z_A), F_A/E_A) \quad \textit{in} \quad \mathrm{Br}_2(E_A).$$

Proof. Set $z = z_A$. Let $z = w\sigma_A(w)$ with $w \in A \otimes_{E_A} k_s$. The cocycle $\tau \mapsto w^{-1}\tau(w)$ represents the class of the hermitian form $\langle z\rangle$ in $H^1(E_A, U_A)$. Let us denote this class by $u_z \in H^1(E_A, U_A)$, and note that we have $u_z = u_A(L)$ by definition. The cocycle $\tau \mapsto n(w)^{-1}\tau(n(w))$ represents the class $n(u_z) \in H^1(E_A, \mathrm{R}^1_{F_A/E_A}G_m)$. By Lemma 4.1 this class is mapped by α^{-1} to $[n(z)] \in E_A^\times/\mathrm{N}(F_A^\times)$. Therefore we have $(n(z), F_A/E_A) = (n(u_A(L)), F_A/E_A) = \mathrm{disc}_A(q_L)$, as claimed.

Proposition 4.7. *If L has a self-dual normal basis over k, then $\mathrm{Res}_{E_A/k}(d_A(L))$ is trivial in $\mathrm{Br}_2(E_A)$.*

Proof. Since L has a self-dual normal basis, q_L corresponds to the hermitian form $\langle 1\rangle$ over (A, σ_A). By Lemma 4.6 this implies that $\mathrm{disc}_A(q_L)$ is trivial. Since by Theorem 4.5 we have $\mathrm{disc}_A(q_L) = \mathrm{Res}_{E_A/k}(d_A(L))$, the Proposition is proved.

Remark. There are examples where $d_A(L) \neq 0$ but $\mathrm{Res}_{E_A/k}(d_A(L)) = 0$ (hence also $\mathrm{disc}_A(q_L) = 0$); see for instance Example 5.2 (i).

§5. Self-dual normal bases

We keep the notation of the previous sections. In particular, G is a finite group, L is a G-Galois algebra over k, and $\phi : \Gamma_k \to G$ is a homomorphism associated to L. We now apply the results of the previous sections to give necessary conditions for the existence of a self-dual normal basis, and to show that these are also sufficient when k has cohomological dimension ≤ 2, see Proposition 5.1 and Theorem 5.3.

Putting together the results of §2 - §4, we have the following :

Proposition 5.1. *Suppose that L has a self-dual normal basis over k. Then the H^1-condition is satisfied, and*

(i) *For all orthogonal σ^s-stable central simple factors A of $k[G]^s$, we have*

$$\mathrm{Res}_{E_A/k}(c_A(L)) = 0 \quad \textit{in } \mathrm{Br}_2(E_A)/\langle A \rangle.$$

(ii) *For all unitary σ^s-stable central simple factors A of $k[G]^s$, we have*

$$\mathrm{Res}_{E_A/k}(d_A(L)) = 0 \quad \textit{in } \mathrm{Br}_2(E_A).$$

Proof. This follows from Propositions 2.1, 3.5 and 4.7.

Example 5.2. (i) The aim of this example is to reinterpret and complete Exemple 10.2 of [BSe 94] using the results of the present paper. Assume that G is cyclic of order 8, and let s be a generator of G; let $\epsilon = s^4$ be the element of order 2 of G. Let $z \in k^\times$, and let $\sigma : \Gamma_k \to \{1, \epsilon\}$ be the corresponding quadratic character. Let $\phi : \Gamma_k \to G$ be given by $\phi = \iota \circ \sigma$, where $\iota : \{1, \epsilon\} \to G$ is the inclusion. Let L be the G-Galois algebra corresponding to ϕ. Set $H = \{1, \epsilon\}$, and note that the image of ϕ is contained in H. Set $N = k[X]/(X^2 - z)$; then we have $L = \mathrm{Ind}_H^G(N)$. Set $A = k[X]/(X^4+1)$, and let us write $k[G] = A' \times A$. It is easy to see that the image of H in A' is trivial. The involution σ_A sends the class of X to the class of X^{-1}. If k contains the 4th roots of unity, then A is a product of two factors exchanged by the involution, hence there $k[G]$ has no involution invariant factor in which the image of H is non trivial. In this case, L has a self-dual normal basis. Assume that k does not contain the 4th roots of unity. Then A is a field; we have $F_A = A$, and $E_A = k[X]/(X^2 - 2)$. Note that A is unitary. We have $i_A(\epsilon) = -1$, hence $i_A(H) = \{1, -1\}$.

Let $i \in F_A$ be a primitive 4th root of unity. By the definition of the extension

$$1 \to Z/2Z \to V_A \to H \to 1$$

(cf. §4), we see that $V_A = \{(1,1),(-1,1),(i,\epsilon),(-i,\epsilon)\}$, a cyclic group of order 4. Recall that e_A is the class of this extension in $H^2(H)$; hence e_A is the only non-trivial element of $H^2(H)$. We have $d_A(L) = \phi^*(e_A) = (z,z) = (z,-1)$, and $\mathrm{Res}_{E_A/k}(d_A(L)) = (z,-1)_E = (z, F_A/E_A)$. Therefore we have

$$d_A(L) = 0 \iff z \text{ is a sum of two squares in } k,$$

and

$$\mathrm{Res}_{E_A/k}(d_A(L)) = 0 \iff z \text{ is a sum of two squares in } E_A = k(\sqrt{2}).$$

It is easy to find examples where $d_A(L) \neq 0$ and $\mathrm{Res}_{E_A/k}(d_A(L)) = 0$; for instance, we can take $k = Q$ and $z = 3$.

By Proposition 5.1 the existence of a self-dual normal basis implies that we have $\mathrm{Res}_{E_A/k}(d_A(L)) = 0$. On the other hand, in [BSe 94], Exemple 10.2 it is checked by direct computation that if z is a sum of two squares in $k(\sqrt{2})$, then L has a self-dual normal basis. Hence we have

$$L \text{ has a self-dual normal basis over } k \iff z \text{ is a sum of two squares in } k(\sqrt{2}).$$

(ii) Assume that $G = D_4$, the dihedral group of order 8. Then a G-Galois algebra L has a self-dual normal basis if and only if either L is split or $L = \mathrm{Ind}_H^G(N)$ with H of order 2, and $N = k[X]/(X^2 - z)$ for some $z \in k^\times$ such that z is a sum of two squares in k.

Indeed, let $\phi : \Gamma_k \to G$ be a homomorphism associated to L. Note that G^2 is of order 2, hence the H^1-condition holds if and only if the image of ϕ is trivial, or equal to G^2; in other words, L is split, or induced from a G^2-Galois algebra. If L is split, then L has a self-dual normal basis. Set $H = G^2$, and assume that $L = \mathrm{Ind}_H^G(N)$, with $N = k[X]/(X^2 - z)$ for some $z \in k^\times$. It remains to show that L has a self-dual normal basis if and only if z is a sum of two squares in k.

The group G has one degree 2 and four degree 1 orthogonal representations. Since the H^1-condition holds, the image of G is trivial in the factors of $k[G]$ corresponding to the degree 1 representations. Let $A = M_2(k)$, and let σ_A be the involution induced by the 2-dimensional unit form; then the factor of $k[G]$ corresponding to the degree 2 orthogonal representation of G is equal to A.

Let $q_A(L)$ be the 2-dimensional quadratic form corresponding to the cohomology class $u_A(L)$. Note that L has a self-dual normal basis if and only if $q_A \simeq \langle 1,1\rangle$; this is equivalent with q_A having trivial determinant and trivial Hasse-Witt invariant. Recall that the H^1-condition is satisfied by hypothesis; hence we have $u_A(L) \in H^1(k, U_A^0)$, and this implies that $\det(q_A(L)) = 1$ in $k^\times/k^{\times 2}$. Since A is a matrix algebra over k, we have $w_2(q_A(L)) = \mathrm{clif}(q_A(L))$. By Theorem 3.3, this implies that $w_2(q_A(L)) = c_A(L)$; hence it remains to prove that $c_A(L) = 0$ if and only if z is a sum of two squares in k.

If k contains the 4-th roots of unity, then $U_A^0 = \tilde{U}_A = G_m$. If k does not contain the 4-th roots of unity, then $U_A^0 = \tilde{U}_A = R^1_{K/k} G_m$, where $K = k[X]/(X^2+1)$.

In both cases, $s : \tilde{U}_A \to U_A^0$ is the squaring map. Using this, we see that the extension $1 \to Z/2Z \to V_A \to H \to 1$ is non-trivial, and that $c_A(L) = (z, -1)$. Therefore $c_A(L) = 0$ if and only if z is a sum of two squares in k, and hence

$$L \text{ has a self-dual normal basis over } k \iff z \text{ is a sum of two squares in } k.$$

(iii) Let $G = A_4$, the alternating group of order 12, and assume for simplicity that $char(k) \neq 3$ and that k contains the third roots of unity. Then $k[G] = k \times k \times k \times M_3(k)$, where the first factor corresponds to the unit representation, the second and the third to the two representations of degree 1 with image of order 3, and the fourth one to the irreducible representation of degree 3. Let $A = M_3(k)$ be the fourth factor, and note that the restriction of σ to A is induced by the 3-dimensional unit form. The extension $1 \to Z/2Z \to V_A \to G \to 1$ defined in §3 is

$$1 \to Z/2Z \to \tilde{A}_4 \to A_4 \to 1,$$

corresponding to the unique non-trivial element $e \in H^2(A_4)$ (see [Se 84], 2.3). Let L be a G-Galois algebra, and note that the H^1-condition is satisfied, since G has no quotient of order 2. Let E be the subalgebra of L fixed by the subgroup A_3 of $G = A_4$; then E is an étale algebra of rank 4. Let $\phi : \Gamma_k \to A_4$ be a homomorphism corresponding to L. By [Se 84], Theorem 1 we have $\phi^*(e) = w_2(q_E)$, the Hasse-Witt invariant of the quadratic form q_E; hence the invariant $c_A(L)$ is equal to $w_2(q_E)$. Let $q_A(L)$ be the 3-dimensional quadratic form corresponding to the cohomology class $u_A(L)$. Then $q_E \simeq q_A(L) \oplus \langle 1 \rangle$, and it is easy to check that $q_A(L) \simeq \langle 1, 1, 1 \rangle \iff w_2(q_E) = 0$, hence $u_A(L) = 0 \iff w_2(q_E) = 0$. Therefore we have

$$L \text{ has a self-dual normal basis over } k \iff w_2(q_E) = 0,$$

recovering a result of [BSe 94] (see [BSe 94], Exemple 1.6).

The case of cyclic groups of order a power of 2 is further developed in §6; we now look at fields of low cohomological dimension. Recall that the *2-cohomological dimension* of Γ_k, denoted by $\mathrm{cd}_2(\Gamma_k)$, is the smallest integer d such that $H^i(k, C) = 0$ for all $i > d$ and for every finite 2-primary Γ_k-module C. For fields of cohomological dimension ≤ 1, the question of existence of self-dual normal bases is settled in [BSe 94], 2.2.

Theorem 5.3. *Assume that* $\mathrm{cd}_2(\Gamma_k) \leq 2$. *Then L has a self-dual normal basis over k if and only if the H^1-condition is satisfied, and the conditions* (i) *and* (ii) *below hold :*

(i) *For all orthogonal σ^s-stable central simple factors A of $k[G]^s$, we have*

$$\mathrm{Res}_{E_A/k}(c_A(L)) = 0 \quad \textit{in } \mathrm{Br}_2(E_A)/\langle A \rangle.$$

(ii) *For all unitary σ^s-stable central simple factors A of $k[G]^s$, we have*

$$\mathrm{Res}_{E_A/k}(d_A(L)) = 0 \quad \textit{in } \mathrm{Br}_2(E_A).$$

Proof. If L has a self-dual normal basis over k, then by Proposition 5.1 the H^1-condition, as well as conditions (i) and (ii) are satisfied. Conversely, let us assume that the H^1-condition, as well as conditions (i) and (ii) hold. Since the H^1-condition holds, we can define $c_A(L)$ and $d_A(L)$, cf. §3 and §4. By Theorems 3.3 and 4.5 we have $\mathrm{clif}_A(q_L) = \mathrm{Res}_{E_A/k}(c_A(L))$ and $\mathrm{disc}_A(q_L) = \mathrm{Res}_{E_A/k}(d_A(L))$. Therefore, conditions (i) and (ii) imply that $\mathrm{clif}_A(q_L)$ is trivial for all orthogonal factors A, and $\mathrm{disc}_A(q_L)$ is trivial for all unitary factors A. Let us prove that L has a self-dual normal basis over k. Let us denote by h_A the hermitian form over (A, σ_A) corresponding to $u_A(L)$. It is enough to show that for all factors A, the class $u_A(L)$ is trivial; this is equivalent with saying that the hermitian form h_A is isomorphic to the unit form 1_A over (A, σ_A). By Witt cancellation (see for instance [BPS 13], Theorem 2.5.2) this in turn is equivalent to saying that $h_A \oplus -1_A$ is hyperbolic. Let us prove this successively for symplectic, orthogonal and unitary characters.

Assume first that A is symplectic. Then by [BP 95], Theorem 4.3.1 every even dimensional non-degenerate hermitian form over a central simple algebra with involution is hyperbolic. This implies that $h_A \oplus -1_A$ is hyperbolic. Assume now that A is orthogonal, and note that the H^1-condition implies that $u_A(L)$ is the image of a class $u^0_A(L)$ of $H^1(E_A, U^0_A)$. This implies that h_A has trivial discriminant. As we saw above, $\mathrm{clif}_A(q_L)$ is trivial, hence the form $h_A \oplus -1_A$ has trivial Clifford invariant. By [BP 95], Theorem 4.4.1 every even dimensional non-degenerate hermitian form over a central simple algebra having trivial discriminant and trivial Clifford invariant is hyperbolic, hence $h_A \oplus -1_A$ is hyperbolic. Assume finally that A is a unitary character. We have seen above that $\mathrm{disc}_A(q_L)$ is trivial, therefore the form $h_A \oplus -1_A$ has trivial discriminant. By [BP 95], Theorem 4.2.1 every even dimensional non-degenerate hermitian form over a central simple algebra having trivial discriminant is hyperbolic, hence $h_A \oplus -1_A$ is hyperbolic.

This implies that L has a self-dual normal basis over k, hence the theorem is proved.

Recall that $\phi : \Gamma_k \to G$ is a homomorphism associated to the G-Galois algebra L, and that for all $x \in H^n(G)$, we denote by x_L the image of x by $\phi^* : H^n(G) \to H^n(k)$. Let $H = \phi(\Gamma_k)$. For $n = 2$, we also need the image of x by the homomorphism $\phi^* : H^n(H) \to H^n(k)$; we denote this image by x^H_L.

Corollary 5.4. *Assume that* $\mathrm{cd}_2(\Gamma_k) \leq 2$*, that the* H^1*-condition is satisfied, and that we have* $x^H_L = 0$ *for all* $x \in H^2(H)$*. Then* L *has a self-dual normal basis over* k*.*

Proof. This follows immediately from Theorem 5.3. Indeed, the H^1-condition is satisfied by hypothesis. Moreover, the classes $c_A(L)$ and $d_A(L)$ are by definition in the image of $\phi^* : H^2(H) \to H^2(k)$, hence the hypothesis $x^H_L = 0$ for all $x \in H^2(H)$ implies that $c_A(L) = 0$ for all orthogonal factors A, and $d_A(L) = 0$ for all unitary factors A. Therefore conditions (i) and (ii) of Theorem 5.3 are satisfied, and hence L has a self-dual normal basis over k.

Remarks. (i) Corollary 5.4 suggests the following question : Assume that $\mathrm{cd}_2(\Gamma_k) \leq 2$, and that the H^1-condition is satisfied. If $x_L = 0$ for all $x \in H^2(G)$, does it follow that L has a self-dual normal basis over k ? This follows from Corollary 5.4 when L is a field extension, in other words, when ϕ is surjective : indeed, then $H = G$.

(ii) The question above (see (i)) has a negative answer for fields of higher cohomological dimensions. Indeed, by [BSe 94], III. 10.1, there exist examples of G-Galois algebras L over fields of cohomological dimension 3 such that for all $n > 0$ we have $x_L = 0$ for all $x \in H^n(G)$, but L does not have a self-dual normal basis over k.

(iii) The converse of the question raised in (i) also has a negative answer : indeed, there exist examples of G-Galois algebras L over Q having a self-dual normal basis such that there exists $x \in H^2(G)$ with $x_L \neq 0$ (see [BSe 94], III. 10.2).

The following result was proved in [BSe 94], Corollaire 3.2.2 in the case where k is an imaginary number field; the proof also applies for fields of cohomological dimension ≤ 2, using the results of [BP 95]. We give here an alternative proof.

Corollary 5.5. *Assume that* $\mathrm{cd}_2(\Gamma_k) \leq 2$*, and that*

$$H^1(G) = H^2(G) = 0.$$

Then L has a self-dual normal basis over k.

Proof. Since $H^1(G) = 0$, we have $G = G^2$. Let A be orthogonal or unitary, and let us construct a central extension V_A' of G by $Z/2Z$, as follows. If A is orthogonal, set $V_A' = V_A^G = \tilde{U}_A(E_A) \times_{U_A^0(E_A)} G$, with the notation of §3. If A is unitary, then we set $V_A' = V_A^G = F_A^{\times 1} \times_{F_A^{\times 1}} G$, the notation being as in §4. In each case, we get a central extension V_A' of G by $Z/2Z$. Since $H^2(G) = 0$, this extension is split. Note that the central extension V_A of H by $Z/2Z$ constructed in §3 and §4 is a subgroup of V_A', and that the restriction of the projection $V_A' \to G$ is the projection $V_A \to H$. Hence the extension V_A is also split. This implies that we have $c_A(L) = 0$ for every orthogonal A, and $d_A(L) = 0$ for every unitary A. By Theorem 5.3 this implies that L has a self-dual normal basis over k.

§6. Cyclic groups of 2-power order

In this section, G is assumed to be *cyclic of order* 2^n, with $n \geq 2$. We start by giving necessary and sufficient conditions for two G–Galois algebras to have isomorphic trace forms in terms of cohomological invariants of degree 1 and 2 (see Proposition 6.2), namely the degree 1 invariants introduced in [BSe 94], and the discriminants of the hermitian forms at the unitary factors (see §4).

We then use the invariants defined in the first part of §4 to give necessary and sufficient conditions for the existence of a self–dual normal basis. We start with settling the case where k contains the 4th roots of unity :

Proposition 6.1. *Assume that k contains the 4th roots of unity. Let L and L' be two G–Galois algebras. Then $q_L \simeq_G q_{L'}$ if and only if $x_L = x_{L'}$ for all $x \in H^1(G)$.*

Proof. The algebra $k[G]$ has two orthogonal factors k; since k contains the 4th roots of unity, there are no other involution invariant factors. Therefore $u(L) = u(L')$ if and only if the cohomology classes u associated to the two degree 1 orthogonal factors coincide, and this is equivalent with the condition $x_L = x_{L'}$ for all $x \in H^1(G)$. Hence, by [BSe 94], Proposition 1.5.1, we have $q_L \simeq_G q_{L'}$.

More generally, we have :

Proposition 6.2. *Let L and L' be two G–Galois algebras. Then $q_L \simeq_G q_{L'}$ if and only if the following conditions hold :*

(i) *$x_L = x_{L'}$ for all $x \in H^1(G)$.*

(ii) *$\mathrm{disc}_A(q_L) = \mathrm{disc}_A(q_{L'})$ for all unitary factors A of $k[G]$.*

Before proving Proposition 6.2, note that when k contains the 4th roots of unity, then Proposition 6.2 follows from Proposition 6.1. Hence we only need to prove the proposition when k does not contain the 4th roots of unity.

From now on, we assume that k *does not contain the 4th roots of unity.* We start by introducing some notation. Set $A(i) = k[X]/(X^{2^{i-1}} + 1)$, for $i = 1, \dots, n$; then the factors of $k[G]$ are k, and $A(1), \dots, A(n)$. Note that k and $A(1)$ are orthogonal, and $A(2), \dots, A(n)$ are unitary. For $i = 2, \dots, n$, we have $A(i) = F_{A(i)}$.

Proof of Proposition 6.2. Recall that we are assuming that k does not contain the 4th roots of unity (otherwise, the proposition follows from Proposition 6.1). For all factors A of $k[G]$, let us denote by h_A, respectively h'_A, the hermitian form over (A, σ_A) determined by q_L, respectively $q_{L'}$.

Assume that $q_L \simeq_G q_{L'}$. Then (i) holds by [BSe 94], Proposition 2.2.1. Let A be a unitary factor; then the hermitian forms h_A and h'_A are isomorphic. Since $\mathrm{disc}_A(q_L)$ and $\mathrm{disc}_A(q_{L'})$ are invariants of these hermitian forms, condition (ii) holds as well.

Conversely, suppose that (i) and (ii) hold. Let us show that $u_A(L) = u_A(L')$ for all factors A. Condition (i) implies that this is true for $A = k$ and $A = A(1)$; indeed, in both cases the group U_A is of order 2. Let us assume that A is a unitary factor, that is, $A = A(i)$ for some $i = 2, \dots, n$. Note that $A = F_A$, hence the hermitian forms h_A and h'_A are one dimensional hermitian forms over the commutative field F_A. Such a form is determined up to isomorphism by its discriminant; hence condition (ii) implies that $h_A \simeq h'_A$. Therefore we have $u_A(L) = u_A(L')$ for all factors A, hence $u(L) = u(L')$, and by [BSe 94], Proposition 1.5.1 we have $q_L \simeq_G q_{L'}$. This completes the proof of the Proposition.

Let us recall a notation from [Se 84], 1.5 or [Se 92], 9.1.3 : if m is an integer, $m \geq 1$, we denote by $s_m \in H^2(S_m)$ the element of $H^2(S_m)$ corresponding to the central extension

$$1 \to Z/2Z \to \tilde{S}_m \to S_m \to 1$$

which is characterized by the properties :

1. A transposition in S_m lifts to an element of order 2 in $\tilde{S}_m$.
2. A product of two disjoint transpositions lifts to an element of order 4 in $\tilde{S}_m$.

Note that $s_m = 0$ if and only if $m \leq 3$ (see [Se 84], 1.5).

If m is a power of 2, $m \geq 2$, let us denote by C_m the cyclic group of order m, and by e_m be the unique non-trivial element of $H^2(C_m)$. Sending a generator of C_m to an m-cycle of S_m defines an injective homomorphism $f : C_m \to S_m$; we denote by $f^* : H^2(S_m) \to H^2(C_m)$ the homomorphism induced by f.

If q is a quadratic form over k, we denote by $w_2(q)$ its Hasse-Witt invariant (see for instance [Se 84], 1.2 or [Se 92], 9.1.2); it is an element of $H^2(k)$.

Lemma 6.3. *Let m be a power of 2.*

(i) *We have $f^*(s_m) = e_m$ in $H^2(C_m)$.*

(ii) *Let $\psi : \Gamma_k \to C_m$ be a continuous homomorphism, and let K be the étale algebra over k corresponding to ϕ. Then the obstruction to the lifting of ϕ to a homomorphism $\Gamma_k \to C_{2m}$ is*

$$w_2(q_K) + (2)(D_K)$$

where D_K is the discriminant of K, and $(2)(D_K)$ denotes the cup product of the elements (2) and (D_K) of $H^1(k)$.

Proof. (i) Let $\tilde{C}_m$ be the inverse image of C_m in $\tilde{S}_m$; it suffices to show that $\tilde{C}_m \simeq C_{2m}$, in other words that $\tilde{C}_m$ is a non-trivial extension of C_m. Raising an m-cycle of S_m to the $\frac{m}{2}$-th power yields a product of $\frac{m}{2}$ disjoint transpositions, and the inverse image of such an element in $\tilde{S}_m$ is of order 4. Hence $\tilde{C}_m$ is a non-trivial extension of C_m.

(ii) The obstruction to the lifting of ψ is $\psi^*(e_m) \in H^2(k)$. Since $f^*(s_m) = e_m$ by (i), we have

$$(f \circ \psi)^*(s_m) = \psi^*(e_m).$$

On the other hand, $(f \circ \psi)^*(s_m) = w_2(q_K) + (2)(D_K)$ by [Se 84], Theorem 1.

Proposition 6.4. *Let L be a G-Galois algebra, and assume that the H^1–condition holds. Then we have*

(i) *Let A be a unitary factor of $k[G]$. If $A \neq A(n)$, then $d_A(L) = 0$.*

(ii) *Let $L = K \times \cdots \times K$, where K is a field extension of k. Then*

$$d_{A(n)}(L) = w_2(q_K) + (2)(D_K).$$

Proof. Let $\phi : \Gamma_k \to G$ be a homomorphism associated to L, let $H = \phi(\Gamma_k)$, and let us denote by $|H|$ its order. Recall from §4 that the extension

$$(*) \qquad 1 \to Z/2Z \to V_A \to H \to 1$$

is defined by $V_A = \{(x, h) \in F_A^{\times 1} \times H \mid x^2 = i_A(h)\}$. Let us show that this extension is split if $A \neq A(n)$. Note that the group V_A is abelian, and hence $(*)$ is not split if and only if V_A is a cyclic group of order $2|H|$. On the other hand, if $A \neq A(n)$, then the order of $i_A(H)$ is strictly less than $|H|$, hence the group V_A does not have any elements of order $2|H|$. Therefore the extension $(*)$ is split, and hence $d_A(L) = 0$; this completes the proof of (i).

Let us prove (ii). If L is split, then (ii) obviously holds, hence we may assume that $|H| \geq 2$. If $A = A(n)$, then the group V_A is cyclic of order $2|H|$, and the extension $(*)$ is not split. Recall that we denote by $e_A \in H^2(H)$ the class of this extension, and that $d_A = \phi^*(e_A) \in H^2(k)$. Note that $\phi^*(e_A)$ is also the obstruction for the lifting of $\phi : \Gamma_k \to H$ to a continuous homomorphism $\Gamma_k \to V_A$; by Lemma 6.3 (ii) this obstruction is equal to $w_2(q_K) + (2)(D_K)$, hence (ii) is proved.

Corollary 6.5. *Let L be a G-Galois algebra, and assume that the H^1–condition holds. Then L has a self-dual normal basis if and only if* $\mathrm{Res}_{E_{A(n)}/k}(d_{A(n)}(L)) = 0$ *in* $\mathrm{Br}_2(E_{A(n)})$.

Proof. Proposition 6.2 implies that L has a self-dual normal basis if and only if the H^1-condition holds and if $\mathrm{disc}_A(q_L) = 0$ for all unitary factors A of $k[G]$. By Theorem 4.5 we have $\mathrm{Res}_{E_A/k}(d_A(L)) = \mathrm{disc}_A(q_L)$, and Proposition 6.4 (i) implies that $d_A(L) = 0$ if $A \neq A(n)$. This completes the proof of the corollary.

Corollary 6.6. *Let L be a G-Galois algebra, and assume that the H^1–condition holds. Let $L = K \times \cdots \times K$, where K is a field extension of k, with $Gal(K/k)$ cyclic of order m. If K can be embedded in a Galois extension of k with cyclic Galois group of order $2m$, then L has a self-dual normal basis.*

Proof. Assume that K can be embedded in a Galois extension of k with cyclic Galois group of order $2m$. Then by Lemma 6.3 (ii) we have $w_2(q_K) + (2)(D_K) = 0$. By Proposition 6.4 (ii), this implies that $d_{A(n)}(L) = 0$, and hence by Corollary 6.5 the G-Galois algebra L has a self-dual normal basis.

Example 6.7. Assume that G is of order 8. Let $a, b, c, \epsilon \in k$ with $a^2 - b^2\epsilon = c^2\epsilon$; assume c non-zero, and ϵ not a square. Set $x = \sqrt{\epsilon}$, and let $K = k(\sqrt{a+bx})$; note that $D_K = \epsilon$, and that K/k is a cyclic extension of degree 4 (see for instance [Se 92], Theorem 1.2.1). Let L be the G-Galois algebra induced from K. Let us prove that

$$L \text{ has a self-dual normal basis } \iff a \text{ is a sum of two squares in } k(\sqrt{2}).$$

Indeed, set $A = A(3)$; by Corollary 6.5 the G-Galois algebra L has a self-dual normal basis if and only if $\mathrm{Res}_{E_A/k}(d_A(L)) = 0$. We have $d_A(L) = w_2(q_K) + (2)(\epsilon)$ by Proposition 6.4 (ii).

Let us show that $w_2(q_K) = (-1)(a)$. Set $y = \sqrt{a+bx}$. Then $\{1, x, y, xy\}$ is a basis of K over k, and in this basis the quadratic form q_K is the orthogonal sum of the diagonal form $\langle 1, \epsilon\rangle$ and of the quadratic form q given by $aX^2 + 2b\epsilon XY + a\epsilon Y^2$. The form q represents a, and its determinant is $\epsilon(a^2 - b^2\epsilon) = c^2\epsilon^2$, hence $\det(q) = 1$ in $k^2/k^{\times 2}$. This implies that $q \simeq \langle a, a\rangle$, hence $q_K \simeq \langle 1, \epsilon, a, a\rangle$, and $w_2(q_K) = (a)(a) = (-1)(a)$.

Therefore $d_A(L) = (-1)(a) + (2)(\epsilon)$. Note that $E_A = k(\sqrt{2})$; hence $\mathrm{Res}_{A/k}(d_A(L)) = \mathrm{Res}_{k(\sqrt{2})/k}((-1)(a))$, and this element is 0 if and only if a is a sum of two squares in $k(\sqrt{2})$.

Note that combining this example with Example 5.2 (i) we get a necessary and sufficient condition for a C_8-Galois algebra to have a self-dual normal basis.

§7. Self-dual normal bases over local fields

We keep the notation of the previous sections, and assume that k is a (non-archimedean) local field. The aim of this section is to give a necessary and sufficient condition for the existence of self-dual normal bases in terms of invariants defined over k.

We say that A is *split* if it is a matrix algebra over its center.

Theorem 7.1. *The G-Galois algebra L has a self-dual normal basis if and only if the H^1-condition holds, and*

(i) *For all orthogonal A such that $[E_A : k]$ is odd and A is split, we have $c_A(L) = 0$ in $\mathrm{Br}_2(k)$.*

(ii) *For all unitary A such that $[E_A : k]$ is odd, we have $d_A(L) = 0$ in $\mathrm{Br}_2(k)$.*

Proof. Assume that the H^1-condition is satisfied and that (i) and (ii) hold. Note that if A is not split, then we have $\mathrm{Br}_2(E_A)/\langle A\rangle = 0$, and that if $[E_A : k]$ is even, then the map $\mathrm{Res}_{E_A/k} : \mathrm{Br}_2(k) \to \mathrm{Br}_2(E_A)$ is trivial. Therefore for all orthogonal A we have $\mathrm{Res}_{E_A/k}(c_A(L)) = 0$ in $\mathrm{Br}_2(E_A)/\langle A\rangle$, and for all unitary A we have $\mathrm{Res}_{E_A/k}(d_A(L)) = 0$ in $\mathrm{Br}_2(E_A)$. By Theorem 5.3, this implies that L has a self-dual normal basis.

Conversely, suppose that L has a self-dual normal basis. Then the H^1-condition holds by Proposition 2.1. By Theorem 5.1 we have $\mathrm{Res}_{E_A/k}(c_A(L)) = 0$ in $\mathrm{Br}_2(E_A)/\langle A\rangle$ for all orthogonal A. Since $\mathrm{Res}_{E_A/k} : \mathrm{Br}_2(k) \to \mathrm{Br}_2(E_A)$ is injective if $[E_A : k]$ is odd, condition (i) holds. Moreover, Theorem 5.1 implies that if A is unitary, then $\mathrm{Res}_{E_A/k}(d_A(L)) = 0$ in $\mathrm{Br}_2(E_A)$. Applying again the injectivity of $\mathrm{Res}_{E_A/k}$ when $[E_A : k]$ is odd, we obtain condition (ii). This completes the proof of the theorem.

§8. Self-dual normal bases over global fields

We keep the notation of the previous sections. Assume that k is a global field, and let Ω_k be the set of places of k. For all $v \in \Omega_k$, we denote by k_v the completion of k at v. For all k-algebras R, set $R^v = R \otimes_k k_v$. We say that a G-Galois algebra is *split* if it is isomorphic to a direct product of copies of k permuted by G. We now apply the Hasse principle of [BPS 13] together with Theorem 7.1 above to give necessary and sufficient conditions for the existence of a self-dual normal basis over k.

Note that the fields E_A are abelian Galois extensions of k (cf. 1.2).

For all finite places v, let us write $E_A^v = K_A(v) \times \cdots \times K_A(v)$, where $K_A(v)$ is a field extension of k_v. Set $n_A^v = [K_A(v) : k_v]$.

We need additional notation in the case when A is unitary. Note that while A is a central simple algebra over F_A, and F_A/E_A is a quadratic extension, for some places $v \in \Omega_k$ we may have $F_A^v = E_A^v \times E_A^v$ with σ_A permuting the components, and $A^v = B \times B$ for some k_v-algebra B. In order to take this into account, we set $\epsilon_A^v = 0$ if $F_A^v = E_A^v \times E_A^v$, and $\epsilon_A^v = 1$ otherwise.

Theorem 8.1. *The G-Galois algebra L has a self-dual normal basis if and only if the H^1-condition holds, if L^v is split for all real places v, and if for all finite places v we have*

(i) *For all orthogonal A such that n_A^v is odd and A^v is split, we have $c_A(L) = 0$ in $\mathrm{Br}_2(k_v)$.*

(ii) *For all unitary A such that n_A^v is odd and $\epsilon_A^v = 1$, we have $d_A(L) = 0$ in $\mathrm{Br}_2(k_v)$.*

Proof. If L has a self-dual normal basis, then L^v is split for all real places v by [BSe 94], Corollaire 3.1.2, and conditions (i) and (ii) hold for all finite places v by Theorem 7.1. Conversely, assume that L^v is split for all real places v, and that for all finite places v conditions (i) and (ii) hold. Then [BSe 94], Corollary 3.1.2 (for real places) and Theorem 7.1 (for finite places) imply the existence of a self-dual normal basis for L^v, for all $v \in \Omega_k$. By the Hasse principle result of [BPS 13], Theorem 1.3.1, the G-Galois algebra L has a self-dual normal basis over k.

Bibliography

[BL 90] 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.

[B 94] E. Bayer-Fluckiger, Multiplicateurs de similitudes, *C.R. Acad. Sci. Paris*, 319 (1994), 1151-1153.

[BF 15] E. Bayer-Fluckiger and U. First, Patching and weak approximation in isometry groups, *Trans. Amer. Math. Soc.*, to appear.

[BP 95] E. Bayer-Fluckiger and R. Parimala, Galois cohomology of the classical groups over fields of cohomological dimension ≤ 2, *Invent. math.* 122 (1995), 195-229.

[BPS 13] E. Bayer-Fluckiger, R. Parimala and J-P. Serre, Hasse principle for G-trace forms, *Izvestiya Math.* 77 (2013), 437-460 (= *Izvestiya RAN*, 77 (2013), 5-28).

[BSe 94] E. Bayer-Fluckiger and J-P. Serre, Torsions quadratiques et bases normales autoduales, *Amer. J. Math.* 116 (1994), 1-64.

[K 69] M. Kneser, *Galois Cohomology of the Classical Groups*, Tata Lecture Notes in Mathematics 47 (1969).

[KMRT 98] M. Knus, A. Merkurjev, M. Rost and J-P. Tignol, *The Book of Involutions*, AMS Colloquium Publications 44, 1998.

[L 05] T. Y. Lam, *Introduction to quadratic forms over fields*, Graduate Studies in Mathematics 67 Amer. Math. Soc. Providence, RI (2005).

[O 84] J. Oesterlé, Nombres de Tamagawa et groupes unipotents en caractéristique p, *Invent. math.* 78 (1984), 13-88.

[Sa 81] J-J. Sansuc, Groupe de Brauer et arithmétique des groupes algebriques linéaires sur un corps de nombres, *J. reine angew. Math.* 327 (1981), 12-80.

[Sch 85] W. Scharlau, *Quadratic and Hermitian Forms*, Grundlehren der Math. Wiss. Springer-Verlag (1985).

[Se 64] J-P. Serre, *Cohomologie galoisienne*, Lecture Notes in Mathematics, Springer-Verlag (1964 and 1994).

[Se 68] J-P. Serre, *Corps locaux*, Hermann (1968).

[Se 84] J-P. Serre, L'invariant de Witt de la forme $\mathrm{Tr}(x^2)$, *Comment. Math. Helv.* 59 (1984), 651-676.

[Se 92] J-P. Serre, *Topics in Galois Theory*, Research Notes in Mathematics, Jones and Barlett Publishers (1992).

E. Bayer-Fluckiger
École Polytechnique Fédérale de Lausanne
EPFL/FSB/MATHGEOM/CSAG
Station 8
1015 Lausanne, Switzerland
eva.bayer@epfl.ch

R. Parimala
Department of Mathematics & Computer Science
Emory University
Atlanta, GA 30322, USA.
parimala@mathcs.emory.edu