Multiples of Trace Forms in Number Fields

EVA BAYER-FLUCKIGER AND JORGE MORALES

ABSTRACT. Let L/K be a Galois G-algebra over a number field K and let q_L be its trace form. In this paper we give necessary and sufficient conditions for the orthogonal sum of two and four copies of q_L to be G-isometric to the standard unit form.

1. Introduction

Let G be a finite group and let L be a Galois G-algebra over a number field K. The trace form q_L is the symmetric bilinear form on L defined by $q_L(x,y) = \mathrm{Tr}_{L/K}(xy)$. The group G acts by isometries on q_L , and it is natural to ask whether L admits a self-dual normal basis, that is, whether there exists an element $e \in L$ such that $\{g(e) : g \in G\}$ is an orthonormal basis for q_L .

It is known that if G has odd order then there is always a self-dual normal basis (Conner-Perlis [3] for $K = \mathbb{Q}$ and [1] in general). A natural question is whether there are other cases for which this is true. It is shown in [2] that if $H^1(G, \mathbb{Z}/2\mathbb{Z}) = H^2(G, \mathbb{Z}/2\mathbb{Z}) = 0$ and if L splits at all infinite primes then L possesses a self-dual normal basis ([2, Théorème 3.2.1]).

In this paper we discuss the following variation of the self-dual normal basis problem: Let q_0 be the trace form of the split G-algebra $\operatorname{Map}(G,K)$ (we shall refer to this form as the $\operatorname{unit}\ G$ -form). When is the orthogonal sum $q_L \oplus q_L$ isometric to $q_0 \oplus q_0$ as G-forms? It is not difficult to see that necessary conditions are that the algebra L_v is split for all real places v of K and that the discriminants $\det(q_F)$ of all quadratic subalgebras of fixed points $F \subset L$ are sums of two squares. Our main result is that these

¹⁹⁹¹ Mathematics Subject Classification. Primary 11E12; Secondary 11E57.

The second author was partially supported by National Science Foundation grant DMS-9205129.

This paper is in final form and no version of it will be submitted for publication elsewhere.

conditions are also sufficient (Theorem 2.2).

2. Algebras with involution and cohomology

Throughout this paper $\overline{\mathbb{Q}}$ will denote the algebraic closure of \mathbb{Q} in \mathbb{C} . By number field it is meant here a subfield of $\overline{\mathbb{Q}}$ of finite degree over \mathbb{Q} . For a number field F we will denote by Ω_F the absolute Galois group $\operatorname{Gal}(\overline{\mathbb{Q}}/F)$.

Let E be a number field and let B be a central simple E-algebra of index n equipped with an involution $b \to b^*$. If the involution restricted to E is the identity, then we say that the involution is of type I; otherwise we say that it is of type II. Let $F \subseteq E$ be the field fixed by the involution. We shall denote by U_B the algebraic group over F defined by the equation $u^*u = 1$.

For an extension L/F we denote by $U_B(L)$ the group of rational points over L; that is, $U_B(L) = \{u \in B \otimes_F L : u^*u = 1\}$. The connected component of the identity in U_B will be denoted by U_B^0 .

The reduced norm $N: B \to E$ induces a homomorphism $N: U_B \to U_E$. Its kernel will be denoted throughout by U_B^1 . The structure of U_B^1 over an algebraic closure is as follows (see [7]).

If the involution is of type II then U_B^1 is isomorphic over an algebraic closure to SL_n .

If the involution is of type I then U_B^1 is isomorphic over an algebraic closure either to the symplectic group Sp_n or to the special orthogonal group SO_n .

In the case when U_B^1 is of type SO_n , we shall define the Hasse-Witt map $\partial: H^1(F, U_B^1) \to H^2(F, \mu_2)$ as follows.

Let \widetilde{U}_B^1 be the universal covering of U_B^1 (this group is of course a twisted form of Spin_n).

For n > 2 consider the exact sequence

(1)
$$0 \longrightarrow \mu_2 \longrightarrow \widetilde{U}_B^1 \longrightarrow U_B^1 \longrightarrow 0$$
, and for $n=2$ consider the sequence

$$(2) 0 \longrightarrow \mu_2 \longrightarrow U_B^1 \stackrel{2}{\longrightarrow} U_B^1 \longrightarrow 0.$$

The Hasse-Witt map is the map $\partial: H^1(F, U_B^1) \to H^2(F, \mu_2)$ induced in cohomology by sequence (1) if n > 2 and by sequence (2) if n = 2.

The involution on B can be extended in a natural way to any matrix algebra $M_m(B)$ by setting $(b_{ij})^* = (b_{ji}^*)$. For simplicity, we shall denote by $U_{B,m}$ the unitary group of the algebra $M_m(B)$. Replacing B by $M_m(B)$ in the definition above we obtain a Hasse-Witt map $\partial: H^1(F, U_{B,m}^1) \to H^2(F, \mu_2)$ for every positive integer m.

Let $d: U_{B,m} \to U_{B,2m}$ be the diagonal homomorphism $u \mapsto \begin{pmatrix} u & 0 \\ 0 & u \end{pmatrix}$.

(1.1) LEMMA. The composite map

$$H^1(F, U_B^1) \xrightarrow{d_*} H^1(F, U_{B,2}^1) \xrightarrow{\partial} H^2(F, \mu_2)$$

is trivial.

PROOF. Let $i_k: U_B^1 \to U_{B,2}^1$ (k=1,2) be the natural inclusions $i_1(u) = \begin{pmatrix} u & 0 \\ 0 & 1 \end{pmatrix}$ and $i_2(u) = \begin{pmatrix} 1 & 0 \\ 0 & u \end{pmatrix}$. Let $\widetilde{i}_k: \widetilde{U}_B^1 \to \widetilde{U}_{B,2}^1$ be the lifting of i_k to the universal covering. It can be easily seen, for instance using the Clifford algebra description of the universal covering, that the following diagram commutes:

Let $\widetilde{d}: \widetilde{U}_B^1 \to \widetilde{U}_{B,2}^1$ be the lifting of the diagonal map. Clearly $\widetilde{d}(x) = \widetilde{i}_1(x)\widetilde{i}_2(x)$. Hence we obtain a commutative diagram

$$0 \longrightarrow \mu_{2} \longrightarrow \widetilde{U}_{B}^{1} \longrightarrow U_{B}^{1} \longrightarrow 0$$

$$\downarrow \downarrow d$$

$$0 \longrightarrow \mu_{2} \longrightarrow \widetilde{U}_{B,2}^{1} \longrightarrow U_{B,2}^{1} \longrightarrow 0.$$

Applying cohomology, we get

$$H^{1}(F, U_{B}^{1}) \xrightarrow{\partial} H^{2}(F, \mu_{2})$$

$$\downarrow^{2}$$

$$H^{1}(F, U_{B,2}^{1}) \xrightarrow{\partial} H^{2}(F, \mu_{2}).$$

Hence $\partial d_{\perp} = 1$.

Since the definition of ∂ is different for n=2, a separate argument is needed in this case. We leave to the reader to verify that for n=2 a diagram similar to (3) may be obtained by replacing the projection $\widetilde{U}_B^1 \to U_B^1$ by the two-fold covering $U_B^1 \xrightarrow{2} U_B^1$. \square

(1.2) Proposition 1.2. Let c be an element in the kernel of the natural map

$$H^1(F, U_B^1) \longrightarrow \prod_{v \text{ real}} H^1(F_v, U_B^1).$$

- (a) If the involution on B is of orthogonal type and $\partial(c) = 1$ then c = 1.
- (b) If the involution on B is of type II then c = 1.

PROOF. By [4, Chapter V, Theorem 1 and remarks at the bottom of page 77], the Hasse Principle holds for $H^1(F, U_B^1)$ (even though it may not hold for $H^1(F, U_B)$). Hence it is sufficient to show that $c_v = 1$ for all finite places v of K.

(a) Suppose first that the index n is greater than 2.

The cohomology set $H^1(F_v, \widetilde{U}_B^1)$ is trivial for all finite primes v (see [4, Chapter 4, Theorem 1]). This implies immediately that the local Hasse-Witt map $\partial_v: H^1(F_v, U_B^1) \to H^2(F_v, \mu_2)$ is injective.

If n=2 then U_B^1 is an algebraic torus split by a quadratic extension L/K. Thus $H^1(F, U_B^1)$ is an elementary abelian 2-group. It follows from the cohomology exact sequence associated to (2) that the homomorphism ∂ is injective.

(b) Since U_B^1 is simply connected we have $H^1(F_v, U_B^1) = 1$ for all finite places v [4, Chapter 4, Theorem 1]. \square

Let G be a finite group and let $\alpha: G \to B^{\times}$ be a group homomorphism compatible with the involution, i.e. such that the condition $\alpha(g)\alpha(g)^* = 1$ holds for all $g \in G$.

Let $\phi \in H^1(F, G)$ and define $c = d_*\alpha_*(\phi) \in H^1(F, U_{B,2}^0)$ (note that d maps U_B into $U_{B,2}^0$; see Lemma 1.6a below). If the involution on B is of orthogonal type, the composition

$$\Omega_F \xrightarrow{\phi} G \xrightarrow{\alpha} U_R \xrightarrow{N} \mu_2$$

defines an element a in $H^1(F, \mu_2) = F^{\times}/F^{\times 2}$.

- (1.3) THEOREM. The cohomology class $c \in H^1(F, U_{B,2}^0)$ is trivial if and only if the following conditions hold:
 - (a) $c_v = 1$ for all real places v of F.
 - (b) If the involution on B is of orthogonal type then the element $a \in F^{\times}$ defined up to squares by (4) can be written in the form $a = x^2 + y^2$ with $x, y \in F$.

Before proving Theorem 1.3, we shall establish three technical lemmas.

(1.4) Lemma. The map $H^1(F, U_B^1) \to H^1(F, U_B^0)$ induced by the inclusion $U_B^1 \to U_B^0$ is injective.

PROOF. If the involution on B is of type I, there is nothing to prove, since $U_B^1 = U_B^0$. Suppose that the involution is of type II. In this case U_B is connected, i.e. $U_B^0 = U_B$ and the reduced norm gives an exact sequence

$$0 \longrightarrow U_B^1 \longrightarrow U_B \stackrel{N}{\longrightarrow} U_E \longrightarrow 0.$$

This sequence induces an exact sequence in cohomology

$$U_B(F) \xrightarrow{N} U_E(F) \xrightarrow{M} H^1(F, U_B^1) \xrightarrow{M} H^1(F, U_B).$$

It follows from [4, §5.6 Proposition a)] that the norm homomorphism $U_B(F) \to U_E(F)$ is surjective. It is easy to see that this implies that $H^1(F, U_B^1) \to H^1(F, U_B)$ is injective. \square

- (1.5) **Remark.** If the involution is of orthogonal type, the map $H^1(F, U_B^0) \to H^1(F, U_B)$ is in general not injective. This happens when U_B is the automorphism group of a skew-hermitian form over a quaternion algebra with center F (see [4, p. 135]).
 - (1.6) LEMMA. (a) $d\alpha(G) \subset U_{B,2}^0$.
- (b) The image of $d_*\alpha_*: H^1(F,G) \to H^1(F,U^0_{B,2})$ is contained in $H^1(F,U^1_{B,2})$.

PROOF. (a) U_B is disconnected only in orthogonal case. It is obvious that the image of the diagonal map $O_m \to O_{2m}$ is contained in SO_{2m} .

Thus d maps U_B into $U_{B,2}^0$.

(b) Let $N: U_B \to U_E$ be the reduced norm map. It is easy to see that the diagram

$$\begin{array}{ccc} U_B & \stackrel{d}{\longrightarrow} & U_{B,2}^0 \\ \downarrow N & & \downarrow N \\ U_E & \stackrel{2}{\longrightarrow} & U_E \end{array}$$

commutes. Since $H^1(F,U_E)$ is an elementary 2-group, the composite map $N_*\circ d_*:H^1(F,U_B)\to H^1(F,U_E)$ is trivial. Hence the image of $H^1(F,G)$ in $H^1(F,U_{B,2})$ is actually contained in $H^1(F,U_{B,2})$. \square

(1.7) LEMMA. Let F be a field and let $u: F^{\times}/F^{\times^2} \to \operatorname{Br}_2(F)$ be the map given by u(a) = (a, -1). Let Q be a fixed quadratic form over F. Then the following diagram commutes:

$$H^{1}(F, O(Q)) \xrightarrow{d} H^{1}(F, SO(Q \oplus Q))$$

$$\det \downarrow \qquad \qquad \downarrow \vartheta$$

$$H^{1}(F, \mu_{2}) = F^{\times}/F^{\times^{2}} \xrightarrow{u} H^{2}(F, \mu_{2}) = \operatorname{Br}_{2}(F)$$

PROOF. Let $c \in H^1(F, O(Q))$ and let q be the quadratic form over F associated to c. With this notation $d_*(c)$ corresponds to the orthogonal sum $q \oplus q$. By [6, 4.7], we have

$$\partial(d_{\star}c)=h(q\oplus q)h(Q\oplus Q),$$

where h denotes the Hasse symbol. Combining this with the elementary identity $h(q \oplus q) = h(q)^2(\det(q), \det(q)) = (\det(q), -1)$ (see [5, Chapter 2, Lemma 12.6]), we obtain

$$\partial(d_*c) = (\det(q)\det(Q), -1) = (\det(c), -1). \quad \Box$$

PROOF OF THEOREM 1.3. By Lemma 1.6(b) we may regard c as a class in $H^1(F, U_{B,2}^1)$. We shall show that c fulfills the hypotheses of Proposition

1.2 (applied to $M_2(B)$) and therefore it is trivial. We need only to consider the orthogonal case and show that $\partial(c) = 1$.

Assume that the involution on B is of orthogonal type. Two cases need to be distinguished:

- (i) B is a matrix algebra over a quaternion algebra D/E. In this case U_B is the automorphism group of a skew-hermitian form over D. It is known (see [4, 2.6 Lemma 1a]) that $U_B(F) = U_B^1(F)$. Hence the image of G lies in U_B^1 . By Lemma 1.1 we have $\partial(c) = \partial(d_*\alpha_*(\phi)) = 1$.
- (ii) B is a matrix algebra over E. In this case $U_B = O(Q)$, where Q is some quadratic form with coefficients in E. By Lemma 1.7, $\partial(c) = (a, -1)$. Our hypothesis on a says precisely that (a, -1) = 1. \square

3. Application to trace forms

In this section we shall apply the previous results to the study of the trace forms. Although many of the definitions below make sense for any field, we shall restrict ourselves for simplicity to the case of number fields.

Let G be a finite group and let K be a number field. The set $\operatorname{Map}(G, K)$ of all set-theoretical maps $G \to K$ is naturally a K-algebra with respect to pointwise addition and multiplication. Moreover, the group G acts on $\operatorname{Map}(G, K)$ as algebra automorphisms by the rule $(g\alpha)(x) = \alpha(g^{-1}x)$. We shall refer to $\operatorname{Map}(G, K)$ as the split Galois G-algebra over K.

In general, a Galois G-algebra over K is a K-algebra L on which G acts by algebra automorphisms and such that there exists an isomorphism of $\overline{\mathbb{Q}}$ -algebras

$$L \otimes_{\kappa} \overline{\mathbb{Q}} \simeq \operatorname{Map}(G, \overline{\mathbb{Q}})$$

commuting with the action of G. For other equivalent definitions of Galois algebras, we refer to [2, Section 1.3].

Standard descent theory shows that the set of isomorphism classes of Galois G-algebras over K is in one-to-one correspondence with the set $H^1(K,G)$ of G-conjugacy classes of homomorphisms $\Omega_K \to G$ (the Galois group Ω_K acts trivially on G). Under this correspondence, Galois field extensions L/K with group G correspond to conjugacy classes of surjective homomorphisms $\Omega_K \to G$.

DEFINITION. Let L be a Galois G-algebra over K. A subalgebra $F \subset L$ is called subalgebra of fixed points if there exists a subgroup $H \subset G$ such that $F = L^H$.

Let L/K be a Galois G-algebra. We will be interested in describing the isometry class of the symmetric bilinear form

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

as a G-form. For example, if L is the split algebra, then q_L is the standard unit form over K. In general, q_L defines a cohomology class u_L in

 $H^1(K, U_A)$. The following lemma relates this class to the element $\phi_L \in H^1(K, G)$ defining L.

(2.1) Lemma. Let $\iota: G \to U_A$ be the natural inclusion and let $\iota_*: H^1(K, G) \to H^1(K, U_A)$ be the induced map. Then $u_L = \iota_*(\phi_L)$.

Proof. See [2, Théorème 1.5.3].

For a (G-) quadratic form q we shall denote by [m]q the orthogonal sum $q \oplus \cdots \oplus q$ (m-times). The standard unit G-form (i.e. the trace form of the split G-algebra) will be denoted by q_0 .

We are now ready to state and prove our main theorem.

- (2.2) Theorem. Let L/K be a Galois G-algebra. The forms $[2]q_L$ and $[2]q_0$ are G-isometric if and only if the two following conditions are satisfied:
 - (a) $L \otimes_K K_v$ is split for all real places v of K.
 - (b) For all quadratic subalgebras of fixed points $K \subset F \subset L$, the discriminant $\delta_{F/K} = \det(q_F) \in K^{\times}/K^{\times^2}$ is a sum of two squares.

PROOF. We first show the necessity of conditions (a) and (b). If $[2]q_L$ is isometric to $[2]q_0$, then q_L must be positive definite at all real places. This can only happen if L is split at all real places, that is, Condition (a) is satisfied. We shall next see that Condition (b) must also be satisfied

Let $\epsilon:G\to\mu_2$ be a surjective homomorphism and let $F=L^{\ker(\epsilon)}$. After identification of $H^1(K,\mu_2)$ with K^\times/K^{\times^2} , the discriminant $\delta_{F/K}$ coincides with $\epsilon_*(\phi_L)$.

The map ϵ induces an algebra homomorphism $A:=K[G]\to K$, which in turn induces homomorphisms $\epsilon_m:U_{A,m}\to U_{K,m}=O_m$.

Clearly the following diagram commutes:

(5)
$$G \longrightarrow U_{A} \xrightarrow{d} U_{A,2}^{1}$$

$$\epsilon \downarrow \qquad \qquad \epsilon_{1} \downarrow \qquad \qquad \epsilon_{2} \downarrow$$

$$\mu_{2} \longrightarrow O_{1} \xrightarrow{d} SO_{2}.$$

On the one hand, by Lemma 1.7, $\partial(d_*\epsilon_*(\phi_L))=(\delta_{F/K},-1)$. On the other hand, since $d_*(\phi_L)=1$ by hypothesis, diagram (5) shows that $d_*\epsilon_*(\phi_L)=1$. Thus $(\delta_{F/K},-1)=1$; that is, $\delta_{F/K}$ is the sum of two squares.

We shall now show that Conditions (a) and (b) imply that $[2]q_L$ is isomorphic to $[2]q_0$. By Lemma 2.1, this is equivalent to $d_*\iota_*(\phi_L)=1$. The group algebra K[G] has a decomposition as algebras with involution

$$K[G] = B_1 \times \dots B_r \times \dots \times (C_1 \times C_1^{op}) \times \dots \times (C_s \times C_s^{op}),$$

where the algebras B_i , C_j are simple. The involution preserves the factors B_i and switches the two components of $C_j \times C_j^{op}$. It is very easy to see that $U_{C_j \times C_j^{op}}$ is isomorphic to the multiplicative group of C_i , and therefore, by

Hilbert 90, has trivial H^1 . Let E_i be the center of B_i and let $F_i \subset E_i$ be the field fixed by the involution. With the notation of Section 1 we have

$$H^{1}(K, U_{A, m}) = \prod_{i=1}^{r} H^{1}(K, \operatorname{Res}_{F_{i}/K} U_{B_{i}, m})$$

(here $\operatorname{Res}_{F_i/K}$ is the restriction of scalars functor).

The set $H^1(K, \operatorname{Res}_{F_i/K} U_{B_i, m})$ can be canonically identified with $H^1(F_i, U_{B_i, m})$ via restriction of cocycles. Let $\alpha: G \to B_i^{\times}$ be the restriction to G of the canonical projection $K[G] \to B_i$. The following diagram commutes:

$$H^1(K,G) \xrightarrow{\alpha_*} H^1(K,\operatorname{Res}_{F_i/K}U_{B_i})$$
restriction $\downarrow \qquad \qquad \qquad \parallel$
 $H^1(F_i,G) \xrightarrow{\alpha} H^1(F_i,U_{B_i})$

Let $\phi \in H^1(K,G)$ be the homomorphism associated to L. By the diagram above, it is sufficient to show that the restriction ϕ_i of ϕ to Ω_{F_i} satisfies the hypothesis of Theorem 1.3 for all i. Condition (a) implies that $\alpha_*(\phi_i)$ is trivial at all real places. In view of Theorem 1.3, it is enough to consider the case when the involution on B_i is of orthogonal type.

Let N be the reduced norm and let ν be the composite map

$$G \xrightarrow{\alpha} U_{B_i} \xrightarrow{N} \mu_2.$$

By Condition (b), $\nu_*(\phi) \in H^1(K, \mu_2) = K^\times/(K^\times)^2$ is the sum of two squares in K. The restriction $\nu_*(\phi_i)$ is a fortiori the sum of two squares in F_i . Hence the hypotheses of Theorem 1.3 are fulfilled, and therefore $d_*\alpha_*(\phi_i) = 1$. \square

- (2.3) Corollary (Compare [2, Théorème 3.2.1]). Assume that G has no quotient of order 2. Then $[2]q_L \simeq [2]q_0$ as G-forms if and only if L is splits at all real places of K.
- (2.4) COROLLARY (Compare [2, Théorème 3.2.2]). If G has no quotient of order 2 and K is totally imaginary then $[2]q_L = [2]q_0$ for all Galois Galgebras L/K.

A weaker result may be obtained without any condition on the quadratic subalgebras of fixed points (Condition (b) of Theorem 2.2).

(2.5) **THEOREM.** The forms $[4]q_L$ and $[4]q_0$ are G-isometric if and only if L splits at all real places of K.

PROOF. With the notation of the proof of Theorem 2.2, let $\phi_i \in H^1(F_i, G)$ be the restriction of ϕ to Ω_{F_i} . By virtue of Theorem 1.3, we can restrict ourselves to the case where the involution on B_i is orthogonal.

Clearly the composite map

$$U_{B_i} \xrightarrow{d} U_{B_i,2} \xrightarrow{N} \mu_2$$

is trivial; hence, applying Theorem 1.3 to the algebra $M_2(B)$, we conclude that $d_*d_*\alpha_*(\phi_i)$ is trivial in $H^1(F_i,U^1_{B,4})$. \square

REFERENCES

- 1. E. Bayer-Fluckiger and H. W. Lenstra, Forms in odd degree extensions and self-dual normal bases, American J. Math 112 (1990), 359-373.
- 2. E. Bayer-Fluckiger and J.-P. Serre, Torsions quadratiques et bases normales autoduales, Amer. J. Math 116 No. 1 (1994), 1-64.
- 3. P. E. Conner and R. Perlis, A survey of trace forms of algebraic number fields, World Scientific Publishing, Singapore, 1984.
- 4. M. Kneser, Galois cohomology of classical groups, Tata Inst. Lecture Notes, Bombay, 1969.
- 5. W. Scharlau, Quadratic and Hermitian forms, Springer-Verlag, Berlin, 1985.
- 6. T. A. Springer, On the equivalence of quadratic forms, Indag. Math. 21 (1959), 241-253.
- 7. A. Weil, Algebras with involution and the classical groups, J. Indian Math. Soc. 24 (1960), 589-623.

LABORATOIRE DE MATHÉMATIQUES, UNIVERSITÉ DE FRANCHE-COMTÉ, 25030 BESANÇON, FRANCE

E-mail address: bayer@grenet.fr

DEPARTMENT OF MATHEMATICS, LOUISIANA STATE UNIVERSITY, BATON ROUGE, LOUISIANA 70803

E-mail address: morales@marais.math.lsu.edu