Forms in Odd Degree Extensions and Self-Dual Normal Bases
Author(s): E. Bayer-Fluckiger and H. W. Lenstra, Jr.
Source: *American Journal of Mathematics*, Vol. 112, No. 3 (Jun., 1990), pp. 359-373
Published by: The Johns Hopkins University Press
Stable URL: http://www.jstor.org/stable/2374746
Accessed: 14/04/2009 06:15

FORMS IN ODD DEGREE EXTENSIONS AND SELF-DUAL NORMAL BASES

By E. Bayer-Fluckiger and H. W. Lenstra, Jr.

Introduction. Let K be a field. Springer has proved that an anisotropic quadratic form over K is also anisotropic over any odd degree extension of K (see [31], [14]). If the characteristic of K is not 2, this implies that two nonsingular quadratic forms that become isomorphic over an extension of odd degree of K are already isomorphic over K (see [31]). In [27], Serre reformulated the latter statement as follows: if O is an orthogonal group over K, then the canonical map of Galois cohomology sets

$$H^1(K, O) \to H^1(L, O)$$

is injective provided the degree of the field extension L/K is odd. He also asked whether a similar statement holds for other linear algebraic groups (see [27], p. 67, Question 2).

In the present paper we prove the following (see Section 2 for a precise statement):

Theorem. *Let K be a field of characteristic not 2. Let N be the norm-one-group of a finite dimensional K-algebra with a K-linear involution. Then, for any extension L of odd degree of K, the canonical map*

$$H^1(K, N) \to H^1(L, N)$$

is injective.

This result has several applications:

Theorem (see (3.2)). *If two systems of bilinear forms over a field*

Manuscript received 1 October 1988.

K of characteristic not 2 become isomorphic over an extension of odd degree of K, then they are already isomorphic over K.

The second application concerns the existence of self-dual normal bases. Let L be a Galois extension of finite degree of K, and let

$$T : L \times L \rightarrow K$$

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

be the trace form. A basis $(e_1, \ldots, e_n)$ of the K-vector space L is said to be *self-dual* if $T(e_i, e_j) = \delta_{i,j}$. Let $G = \mathrm{Gal}(L/K)$. There exists $x \in G$ such that the elements $g(x)$, $g \in G$, form a basis for L as a vector space over K (see [21], [9]). Such a basis is called a *normal basis*. Conner and Perlis proved that if $K = Q$ and the degree of L over Q is odd, then L has a self-dual normal basis over Q (see [7], (V.3.3)). They asked which ground fields K have the property that any Galois extension of odd degree has a self-dual normal basis. The following result is a consequence of (2.1):

THEOREM (see (5.6)). *Any finite Galois extension of odd degree of a field of characteristic not 2 has a self-dual normal basis.*

It would be interesting to know whether this holds for fields of characteristic 2 as well. The following theorem implies that this is the case for abelian extensions. The proof of this result (see Section 6) can be read independently from the rest of the paper.

THEOREM (see (6.1)). *Let L/K be an abelian extension of degree n and group G.*

(a) *If* char$(K) \neq 2$, *then L has a self-dual normal basis over K if and only if n is odd.*

(b) *If* char$(K) = 2$, *then L has a self-dual normal basis over K if and only if the exponent of G is not divisible by* 4.

For finite fields this is proved in [17].

1. Witt groups of algebras.

This section contains some results on Witt groups that are needed in the proof of the main theorem (see (2.1)). It is based on W. Scharlau's paper [25], especially on Section 5. We begin by recalling some definitions and basic results about hermitian and symmetric forms (see also [26] and [15]).

Let K be a field and let A be a K-algebra with a K-linear involution $J : A \to A$. Let M be a finitely generated left A-module. A map $h : M \times M \to A$ is called a *sesquilinear form* if it is biadditive and satisfies $h(am, bn) = ah(n, m)J(b)$ for all a, b in A and all m, n in M. Let $\epsilon = 1$ or -1. A sesquilinear form (M, h) is said to be ϵ-*hermitian* if $J[h(m, n)] = \epsilon h(n, m)$ for all m and n in M. Set $M^* = \mathrm{Hom}_A(M, A)$. Given an ϵ-hermitian form (M, h), we associate to any m in M an element H_m of M^* defined by $H_m(n) = h(n, m)$. We say that (M, h) is *nonsingular* if the map

$$(1.1) \qquad H : M \to M^*$$

$$m \mapsto H_m$$

is bijective. This map is A-linear if $(a.f)(m) = f(m)J(a)$ for all $a \in A$, $f \in M^*$ and $m \in M$. A *morphism* from (M, h) to (M', h') is a homomorphism of left A-modules $f : M \to M'$ such that $h'(fm, fn) = h(m, n)$ for all m, n in M. The *unitary group* $U(M, h)$ is the group of all automorphisms of (M, h). An ϵ-hermitian form (M, h) is called *metabolic* if M has an A-submodule N that is equal to its orthogonal (i.e. $h(n, m) = 0$ for all n in N if and only if $n \in N$). Let $\boxplus$ stand for orthogonal sum. The *Witt group* $W^\epsilon(A, J)$ is the quotient of the Grothendieck group (with respect to $\boxplus$) of the isomorphism classes of nonsingular ϵ-hermitian forms by the subgroup generated by the metabolic forms. For any nonsingular ϵ-hermitian form (M, h), the form $(M, h) \boxplus (M, -h)$ is metabolic (take for N the diagonal). This implies that two ϵ-hermitian forms (M, h) and (M', h') are in the same Witt class if and only if there exist metabolic forms (N, g) and (N', g') such that

$$(M, h) \boxplus (N, g) \cong (M', h') \boxplus (N', g').$$

If $A = K$ and $\epsilon = 1$ then we obtain the Witt group $W(K)$ of the field K. It is well known that the tensor product of forms induces a ring structure on $W(K)$ (see for instance [26], Chapter 2, Section 1). As Scharlau points out ([25], Section 5), one can take the tensor product of a K-valued form with an A-valued form and thereby obtain a left $W(K)$-module structure on $W^\epsilon(A, J)$.

If L/K is a field extension, we extend the involution J to an involution J_L of $A_L = A \otimes_K L$. For any ϵ-hermitian form (M, h), set $M_L =$

$M \otimes_K L$ and let $h_L : M_L \times M_L \to A_L$ be the extension of h to M_L. We obtain a canonical homomorphism

$$r^* : W^\epsilon(A, J) \to W^\epsilon(A_L, J_L)$$

$$(M, h) \mapsto (M_L, h_L) = (M, h) \otimes_K L.$$

PROPOSITION 1.2. *If L is a finite extension of odd degree of K, then the homomorphism*

$$r^* : W^\epsilon(A, J) \to W^\epsilon(A_L, J_L)$$

is injective.

Proof. Let $s : L \to K$ be a nonzero K-linear homomorphism. We extend s to an A-linear homomorphism $s_A : A_L \to A$ and we obtain a group homomorphism

$$s_* : W^\epsilon(A_L, J_L) \to W^\epsilon(A, J)$$

defined by sending (M, h) to $(M, s_A h)$. Likewise, we have

$$s_* : W(L) \to W(K).$$

An easy computation shows that

$$s_*[b \otimes r^*(h)] = s_*(b) \otimes h \tag{1.3}$$

for all b in $W(L)$ and h in $W^\epsilon(A, J)$.

It suffices to prove the proposition in the case where L is a simple extension, say $L = K(a)$. Following Scharlau [24] define a K-linear homomorphism $s : L \to K$ by $s(1) = 1$ and $s(a^i) = 0$ for $i = 1, \ldots, n - 1$ where n is the degree of L over K. Set $b = 1$ in (1.3). As n is odd, it is easy to check (see [24] or [26], Chapter 2, (5.8)), that $s_*(1) = 1$ in $W(K)$. So $s_*[r^*(h)] = h$ for all h in $W^\epsilon(A, J)$, which shows that r^* is injective.

We say that two ϵ-hermitian forms (M, h) and (M', h') *become isomorphic* over an extension L of K if (M_L, h_L) and (M'_L, h'_L) are isomorphic over A_L.

COROLLARY 1.4. *Assume that the characteristic of K is not 2 and that A is a skew field. Let L be a finite extension of odd degree of K. If two nonsingular ϵ-hermitian forms become isomorphic over L, then they are isomorphic.*

Proof. Let (M, h) and (M', h') be two nonsingular ϵ-hermitian forms that become isomorphic over L. Let w be the Witt class of $(M, h) \boxplus (M', -h')$. Then $r^*(w) = 0$, so by Proposition 1.2, we have $w = 0$. Therefore there exist metabolic forms (N, g) and (N', g') such that

$$(M, h) \boxplus (N, g) \cong (M', h') \boxplus (N', g'). \tag{1.5}$$

Since N and N' are A-vector spaces of the same dimension, they are isomorphic. It is well known that the metabolic forms (N, g) and (N', g') are then also isomorphic. We give a proof of this fact for the convenience of the reader. Let $G : N \to N^*$ be the isomorphism associated to g as in (1.1). Since (N, g) is metabolic, there exists a sub-A-vector space P of N that is equal to its orthogonal. Let $G_P : N \to P^*$ be the composition of G with the projection of N^* onto P^*. The kernel of G_P is P. Therefore $\dim_A(P) = 1/2 \dim_A(N)$. Let P' be a direct complement of P in N. As P is totally isotropic, $G(P)$ is contained in P'^*. The map G is injective and $\dim_A(P) = \dim_A(P')$, hence $G : P \to P'^*$ is an isomorphism. The restriction of g to P' defines a (possibly singular) ϵ-hermitian form $k : P' \times P' \to A$. Let $F : P' \to P'^*$ be the map corresponding to $-1/2.k : P' \times P' \to A$ as defined in (1.1). Set $f = G^{-1} \circ F : P' \to P$. Let Q be the sub-A-vector space of N given by

$$Q = \{(f(p'), p') \mid p' \in P'\}.$$

Then $N = P \oplus Q$, and an easy computation shows that $g(Q, Q) = 0$. The form g is given by the duality between P and Q. Such a form is completely determined by $\dim_A(P)$.

Hence (N, g) and (N', g') are isomorphic. By (1.5) and Witt's cancellation theorem (see e.g. [4], Section 4, n° 3, Théorème 1, or [26], Chapter 7, Theorem 9.1) this implies that $(M, h) \cong (M', h')$, so the corollary is proved.

2. Forms in odd degree extensions. Let K be a field of characteristic not 2. Let A be a finite dimensional K-algebra together with a

K-linear involution $J : A \to A$. Let the algebraic group N be the *norm-one-group* of A, i.e.

$$N(L) = \{a \in A_L \mid aJ_L(a) = 1\}$$

for any field extension L of K. Let K_s be a separable closure of K. We use the standard notation $H^1(K, N) = H^1(\mathrm{Gal}(K_s/K), N(K_s))$. For any field extension L/K, we obtain a canonical map $H^1(K, N) \to H^1(L, N)$, see for instance [10], Section 2.

THEOREM 2.1. *If L is a finite extension of odd degree of K, then the canonical map*

$$H^1(K, N) \to H^1(L, N)$$

is injective.

We say that N is a *general linear group* if there exist a skew field D and an integer n such that $N(L) \cong \mathrm{GL}_n(D \otimes_K L)$ for all field extensions L/K (functorially in L). The group N is called a *unitary group* if there exist a skew field D, a K-linear involution $I : D \to D$, a finite dimensional left D-vector space W, an element $\epsilon = 1$ or -1, and a nonsingular ϵ-hermitian form $h : W \times W \to D$ such that likewise $N(L) \cong U(W_L, h_L)$, the group of automorphisms of the form (W_L, h_L).

LEMMA 2.2. *If N is a general linear group, then $H^1(K, N) = 0$.*

Proof. See for instance [28], Chapter X, Section 1, Exercise 2, or [32], Appendix. In terms of "forms" (see [28], Chapter X, Section 2 or [29], Chapter III, Section 1) this means that if D is a skew field and n a positive integer, then there exists a unique isomorphism class of n-dimensional left D-vector spaces.

LEMMA 2.3. *Let L be a finite extension of odd degree of K. If N is a unitary group, then the canonical map*

$$F : H^1(K, N) \to H^1(L, N)$$

is injective.

Proof. Let D, W, h and ϵ be such that N is the unitary group of (W, h). Then $H^1(K, N)$ is in one-to-one correspondence with the set of isomorphism classes of nonsingular ϵ-hermitian forms $g : W \times W \to D$

that become isomorphic to (W, h) over K_s (see [28], Chapter X, Section 2 or [29], Chapter III, Section 1). Let (W, g) and (W, g') be two such forms. Then they have the same image under F if and only if they become isomorphic over L. By Corollary 1.4 this implies that they are isomorphic. Therefore F is injective.

Proof of Theorem 2.1. There exists an exact sequence of algebraic groups

$$1 \to U \to N \to N_1 \times \cdots \times N_r \to 1$$

where U is a split unipotent group, and N_i is either a unitary group or a general linear group (see [1], Section 1 and Wagner [33], Lemma 6). This induces a map

$$H^1(K, N) \to H^1(K, N_1) \times \cdots \times H^1(K, N_r).$$

As U is split unipotent, this map is bijective ([23], Lemme 1.13). Therefore the theorem follows from the two preceding lemmas.

Remark 2.4. Sansuc proved (2.1) for number fields ([23], Corollaire 4.6).

3. Systems of bilinear forms. Let K be a field, and let V be a finite dimensional K-vector space. Let I be a set, and let $S = \{b_i\}$ be a system of K-bilinear forms $b_i : V \times V \to K$, $i \in I$. The system S is said to be *isotropic* if there exists a nonzero x in V such that $b_i(x, x) = 0$ for all i. Let $S' = \{b'_i\}$ be a system of K-bilinear forms $b'_i : V' \times V' \to K$, $i \in I$, where V' is a finite dimensional K-vector space. An *isomorphism* between S and S' is a K-linear isomorphism $f : V \to V'$ such that $b'_i(fx, fy) = b_i(x, y)$ for all x, y in V and all i.

Let us recall a well-known result of Springer:

THEOREM 3.1 (Springer, [34]).

(a) *If a quadratic form becomes isotropic over a finite extension of odd degree, then it is isotropic.*

(b) *Assume that the characteristic of K is not* 2. *Then, if two nonsingular quadratic forms become isomorphic over a finite extension of odd degree, they are isomorphic.*

Part (a) generalizes only to pairs of quadratic forms (see Brumer

[5]) but not to systems of at least 3 quadratic forms (Cassels [6], Coray [8]). On the other hand, we now show that part (b) generalizes to all systems:

THEOREM 3.2. *Suppose that the characteristic of K is not 2. If two systems of bilinear forms become isomorphic over a finite extension of odd degree, then they are isomorphic.*

Proof. Let $S = \{b_i\}$ be a system of K-bilinear forms. Following [1], set

$$A_S = \{(f, g) \in \mathrm{End}(V) \times \mathrm{End}(V) \mid b(fx, y) = b(x, gy) \text{ and } b(x, fy) = b(gx, y) \text{ for all } x, y \text{ in } V \text{ and all } b \text{ in } S\}.$$

Let us give A_S a structure of K-algebra by setting $(f, g) + (f', g') = (f + f', g + g')$ and $(f, g)(f', g') = (ff', g'g)$. Define a K-linear involution $J : A_S \rightarrow A_S$ by $J(f, g) = (g, f)$. Sending f to (f, f^{-1}) defines an isomorphism between the group of automorphisms of S and the norm-one-group N of A_S (see [1]). Let L be a finite extension of odd degree of K. The set of isomorphism classes of K-bilinear forms that become isomorphic to S over L is in bijection with the kernel of the canonical map of pointed sets $H^1(K, N) \rightarrow H^1(L, N)$. By Theorem 2.1 this kernel is trivial, so the theorem is proved.

Remark 3.3. Theorem 3.2 and its proof can be generalized to systems of sesquilinear forms over algebras with involution, to systems of equivariant forms (see Section 4) and even to systems of hermitian forms in an additive category in the sense of Quebbemann, Scharlau and Schulte (see [22] or [26], Chapter 7, [2]) provided that the rings of endomorphisms of the objects are finite dimensional vector spaces over a field of characteristic not 2.

4. Equivariant forms. Let K be a field of characteristic not 2, let G be a group and let $K[G]$ be the group ring. Let M be a left $K[G]$-module that is a finite dimensional K-vector space. An *equivariant* form is a K-bilinear form $b : M \times M \rightarrow K$ such that $b(gm, gn) = b(m, n)$ for all g in G and all m, n in M.

THEOREM 4.1. *If two equivariant forms become isomorphic over a finite extension of odd degree, then they are isomorphic.*

Proof. The proof is similar to the proof of Theorem 3.2. Let (M, b) be an equivariant form. As in the preceding section, one associates to this form a subalgebra with involution of $\mathrm{End}_{K[G]}(M) \times \mathrm{End}_{K[G]}(M)$ such that the group of automorphisms of (M, b) is the norm-one-group of this algebra. The result now follows from Theorem 2.1.

5. Self-dual normal bases. Let K be a field, and let L be a separable extension of finite degree n of K. The trace form

$$T : L \times L \rightarrow K$$

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

is a nonsingular, symmetric K-bilinear form on the K-vector space L. A K-basis $(e_1, \ldots, e_n)$ of L is said to be *self-dual* if $T(e_i, e_j) = \delta_{i,j}$ for all i, j. A field extension has a self-dual basis if and only if the trace form is isomorphic to the standard form $\langle 1, \ldots, 1\rangle$.

At least part (b) of the following proposition is well known (see for instance [7], (I.6.5)):

PROPOSITION 5.1.

(a) *Any finite separable extension of a field of characteristic* 2 *has a self-dual basis.*

(b) *Any finite Galois extension of odd degree of a field of characteristic not* 2 *has a self-dual basis.*

Proof.

(a) Assume that $\mathrm{char}(K) = 2$. Let $(L, T) \cong (V_1, T) \boxplus (V_2, T)$, where (V_1, T) is a diagonal form. Suppose that $r = \dim_K(V_1)$ is maximal with the above property. This implies that $T(v, v) = 0$ for all v in V_2 (see for instance [19], Chapter 1, (3.5)). Notice that

$$(5.2) \qquad T(x, x) = \mathrm{Tr}_{L/K}(x^2) = [\mathrm{Tr}_{L/K}(x)]^2 \text{ for all } x \text{ in } L.$$

There exists an x in L such that $\mathrm{Tr}_{L/K}(x) = T(x, x) = 1$, therefore $r \neq 0$. Let $(e_1, \ldots, e_r)$ be a K-basis of V_1 such that $T(e_i, e_j) = a_i\delta_{i,j}$ for all i, j. Set $b_i = \mathrm{Tr}_{L/K}(e_i)$ and $f_i = (1/b_i)e_i$. Then (5.2) shows that $T(f_i, f_j) = \delta_{i,j}$, so (V_1, T) is the standard form. Set $x = e_1$ and let U be the sub K-vector space of V_1 with basis $(e_1, \ldots, e_r)$. Suppose that $V_2 \neq 0$, and let y be a nonzero vector of V_2. As (V_2, T) is nonsingular, there exists z in V_2 such that $T(y, z) = 1$. Let W be the sub K-vector space of L spanned by x, y and z. Then (W, T) is the standard form: $(x + y, x + z, x + y + z)$ is an orthonormal basis. Hence $(U, T) \boxplus (W, T)$ is a diagonal orthogonal summand of (L, T) of dimension $r + 2$. This contradicts the maximality of r. Therefore $V_2 = 0$, and $(L, T) = (V_1, T)$ is the standard form.

(b) It is easy to see that (L, T) becomes isomorphic to the standard form over L. Indeed, $L \otimes_K L \cong L \times \cdots \times L$, and the extended trace form T_L is the orthogonal sum of the trace forms of the factors (see for instance [7], (I.5.4)). By Springer's theorem (3.1) b) this implies that (L, T) is isomorphic to the standard form.

Remark 5.3. If $\operatorname{char}(K) \neq 2$ and if L is a quadratic extension of K, then L does not have any self-dual basis over K. Indeed, the discriminant of T is the discriminant of the field extension. As the latter is not a square, T is not isomorphic to the standard form. More results about the existence of self-dual bases can be found in Serre [30] and Kahn [12], [13].

Assume moreover that L is a Galois extension of K with group G. The normal basis theorem says that there exists x in L such that the set $\{g(x) \mid g \in G\}$ is a basis for L as a vector space over K (see [21], [9]). Equivalently, L is free with one generator as a left $K[G]$-module.

Observe that T is a G-equivariant form: $T(gx, gy) = T(x, y)$ for all g in G and x, y in L. Therefore the dual of a normal basis is also normal. So it is natural to ask whether L has a self-dual normal basis. This question has been studied in [3], [7] Chapter V, [11], [16], [17], [18] Chapter 4, Section 9 and [20].

Let $\bar{\ }$ be the K-linear involution of $K[G]$ defined by $\bar{g} = g^{-1}$ for all g in G. Let $p_1 : K[G] \to K$ be the K-linear homomorphism such that $p_1(g) = \delta_{g,1}$ for all $g \in G$. We denote by t the standard G-equivariant form on $K[G]$:

$$t : K[G] \times K[G] \to K$$

$$t(x, y) = p_1(x\bar{y}).$$

LEMMA 5.4. *There exists a self-dual normal basis of L over K if and only if (L, T) and $(K[G], t)$ are isomorphic as G-equivariant forms.*

Proof. This is clear.

LEMMA 5.5 (Conner-Perlis, [7], (V.3)). *The G-equivariant forms (L, T) and $(K[G], t)$ become isomorphic over L.*

Proof. Let

$$f : L \otimes_K L \to L[G]$$

$$a \otimes b \mapsto \sum_{g \in G} g^{-1}(a)b.g.$$

It is easy to check that f is an isometry between $(L, T) \otimes_K L$ and $(K[G], t) \otimes_K L$. See [7], pp. 227–228 for details.

THEOREM 5.6. *Any finite Galois extension of odd degree of a field of characteristic not* 2 *has a self-dual normal basis.*

Proof. Apply (5.5), (4.1) and (5.4).

6. Self-dual normal bases for abelian extensions. This section can be read independently from the rest of the paper. Theorem 6.1 below is partly a special case of (5.6). The proof given here—for abelian extensions—is much simpler than the earlier proof of (5.6).

THEOREM 6.1. *Let L be a Galois extension of finite degree n of K, and let $G = \mathrm{Gal}(L/K)$. Suppose that G is abelian.*

(a) *Assume that* $\mathrm{char}(K) \neq 2$. *Then there exists a self-dual normal basis of L over K if and only if n is odd.*
(b) *Assume that* $\mathrm{char}(K) = 2$. *Then there exists a self-dual normal basis of L over K if and only if the exponent of G is not divisible by* 4.

Proof of the nonexistence part. If L has a self-dual normal basis over K, then so has any subfield that is Galois over K. To see this, it suffices to take the trace of an element of a self-dual normal basis. Therefore it suffices to show the following two assertions:

(i) If $\mathrm{char}(K) \neq 2$ and $n = 2$, then L does not have any self-dual normal basis over K.
(ii) If G is cyclic of order 4, then L does not have any self-dual normal basis over K.

Proof of (i). Let $G = \{1, g\}$ and assume that $a \in L$ generates a self-dual normal basis. Then $0 = \mathrm{Tr}_{L/K}[ag(a)] = 2ag(a)$. This implies that $a = 0$, which is a contradiction. For another proof, see Remark 5.3.

Proof of (ii). Let g be a generator of G and assume that $B = (a, g(a), g^2(a), g^3(a))$ is a self-dual K-basis of L. We have

$$0 = \mathrm{Tr}_{L/K}[ag(a)] = [a + g^2(a)][g(a) + g^3(a)].$$

As the second factor of this product is the image under g of the first one, both have to be zero. This implies that $a = -g^2(a)$, contradicting that B is a basis.

PROPOSITION 6.2. *Any abelian extension of odd degree has a self-dual normal basis.*

For fields of characteristic not 2 this is a special case of (5.6). Before proving the proposition, we use it to complete the proof of (6.1).

Proof of the existence part. If $\mathrm{char}(K) \neq 2$, then the assertion follows from (6.2). Assume that $\mathrm{char}(K) = 2$. Then L is a composite of linearly disjoint extensions L_i such that $[L_i : K] = 2$ or is odd. In the second case (6.2) implies that L_i has a self-dual normal basis over K. If L_i is a quadratic extension of K, then by (5.2) it is easy to see that any element of trace 1 generates a self-dual normal basis. Therefore all the L_i's have self-dual normal bases over K. Multiplying out one obtains a self-dual normal basis of L over K, and (6.1) is proved.

Recall that for any group G we denote by $K[G]$ the group ring and by $\bar{\ }: K[G] \to K[G]$ the K-linear involution that sends g to g^{-1} for all g in G.

LEMMA 6.3. *Let G be a finite abelian group and let u be a unit of $K[G]$. Let L be a finite extension of odd degree n of K. Suppose that there exists y in $L[G]$ with $u = \bar{y}y$. Then there also exists x in $K[G]$ such that $u = \bar{x}x$.*

Proof. As G is commutative, and $L[G]$ is free over $K[G]$, we have a norm map $N = N_{L[G]/K[G]} : L[G] \to K[G]$. Then $u^n = N(u) = N(\bar{y}y) = \overline{N(y)}N(y)$. Set $x = N(y)/u^{(n-1)/2}$. It is easy to check that $\bar{x}x = u$, so the lemma is proved.

Let L be a finite Galois extension of K with group G. Then $T(ga, b) = T(a, g^{-1}b)$ for all g in G and a, b in L. Therefore

(6.4) *$T(xa, b) = T(a, \bar{x}b)$ for all x in $K[G]$ and all a, b in L.*

If $a \in L$ is an element of a normal basis, we denote by a^* the element of the dual normal basis satisfying $T(a, a^*) = 1$. For all $b \in L$ there exists $x \in K[G]$ such that $b = xa$. Moreover, b belongs to a normal basis if and only if x is a unit.

Let a be an element of a normal basis of L over K, and let u be the unit of $K[G]$ such that $a^* = ua$.

LEMMA 6.5. *The extension L has a self-dual normal basis over K if and only if there exists a unit x of $K[G]$ such that $u = \bar{x}x$.*

Proof. Let x be a unit of $K[G]$. Using (6.4) we see that $(xa)^* = (\bar{x})^{-1}a^* = (\bar{x})^{-1}ua$. Therefore $(xa)^* = xa$ if and only if $u = \bar{x}x$.

LEMMA 6.6. *There exists a unit y of $L[G]$ such that $u = \bar{y}y$.*

Proof. The proof of (5.5) shows that $L \otimes_K L$ has a self-dual normal basis over L. Therefore the argument leading to (6.5) proves the existence of y with the desired property.

Proof of 6.2. The proposition follows from (6.6), (6.3) and (6.5).

Remark 6.7. The only step in the proof of Proposition (6.2) where we use that the extension is abelian is Lemma 6.3. We do not know whether (6.3) is true for noncommutative groups G if $\mathrm{char}(K) = 2$. If the characteristic of K is not 2 and G is any finite group, then one can deduce (6.3) from Theorem 2.1. In this application of (2.1) the algebraic group N is given by $N(L) = \{x \in L[G] \mid \bar{x}x = 1\}$ for all field extensions L of K.

Acknowledgments. The first named author was supported by the Fonds National Suisse de la recherche scientifique. The second named author was supported by the National Science Foundation, grant number DMS-8706176.

Added in proofs. Theorem 5.6 can be generalized to fields of characteristic 2 (see E. Bayer-Fluckiger, *Indag. Math.*, **51** (1989), 379–383). In other words, every Galois extension of odd degree has a self-dual normal basis. This answers a question raised in the introduction.

UNIVERSITÉ DE GENÈVE, SWITZERLAND
UNIVERSITY OF CALIFORNIA AT BERKELEY

REFERENCES

[1] E. Bayer-Fluckiger, Principe de Hasse faible pour les systèmes de formes quadratiques, *J. Reine Angew. Math.*, **378** (1987), 53–59.

[2] ———, C. Kearton, and S. M. J. Wilson, Hermitian forms in additive categories: finiteness results, *J. Algebra*, (to appear).

[3] T. Beth, W. Fumy, and R. Mühlfeld, Zur algebraischen diskreten Fourier-Transformation, *Arch. Math.* (Basel), **40** (1983), 238–244.

[4] N. Bourbaki, Algèbre, Chapitre 9: Formes sesquilinéaires et formes quadratiques, Hermann, Paris (1959).

[5] A. Brumer, Remarques sur les couples de formes quadratiques, *C. R. Acad. Sci. Paris*, Sér. A-B **286** (1978), A679–A681.

[6] J. W. S. Cassels, On a problem of Pfister about systems of quadratic forms, *Arch. Math.* (Basel), **33** (1979), 29–32.

[7] P. Conner and R. Perlis, A survey of trace forms of algebraic number fields, World Scientific, Singapore (1984).

[8] D. Coray, On a problem of Pfister about intersections of three quadrics, *Arch. Math.* (Basel), **34** (1980), 403–411.

[9] M. Deuring, Galoissche Theorie und Darstellungstheorie, *Math. Ann.*, **107** (1933), 140–144.

[10] G. Harder, Bericht über neuere Resultate der Galoiskohomologie halbeinfacher Matrizengruppen, *Jahresber. Deutsch. Math.-Verein.*, **70** (1968), 182–216.

[11] K. Imamura, On self-complementary bases of $GF(q^n)$ over $GF(q)$, *Trans. IECE Japan*, **E66** (1983), 717–721.

[12] B. Kahn, La deuxième classe de Stiefel-Whitney d'une représentation régulière, I., II., *C. R. Acad. Sci. Paris*, série I., **297** (1983), 313–316, **316** (1983), 573–576.

[13] ———, Classes de Stiefel-Whitney de formes quadratiques, *Invent. Math.*, **78** (1984), 223–256.

[14] M. Knebusch, Grothendieck- und Wittringe von nichtausgearteten symmetrischen Bilinearformen, *S.-Ber. Heidelberg. Akad. Wiss. math.-naturw. Kl.*, 1969/70 3 Abh. (1970).

[15] T. Y. Lam, *The Algebraic Theory of Quadratic Forms*, W. A. Benjamin Publ., Reading, Mass., (1973).

[16] A. Lempel, Characterisation and synthesis of self-complementary normal bases in finite fields, *Lin. Alg. App.*, **98** (1988), 331–346.

[17] ——— and M. J. Weinberger, Self-complementary normal bases in finite fields, *SIAM J. Disc. Math.*, **1** (1988), 193–198.

[18] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North Holland, Amsterdam, (1977).

[19] J. Milnor and D. Husemoller, Symmetric bilinear forms, Ergebnisse der Math. Band 73, Springer-Verlag, (1973).

[20] A. Morii and K. Imamura, A theorem that $GF(2^{4m})$ has no self-complementary normal basis over $GF(2)$ for odd m, *Trans. IECE Japan*, **E67** (1984), 655–656.

[21] E. Noether, Normalbasis bei Körper ohne höhere Verzweigung, *J. Reine Angew. Math.*, **167** (1932), 147–152.

[22] H.-G. Quebbemann, W. Scharlau, and M. Schulte, Quadratic and hermitian forms in additive and abelian categories, *J. Algebra*, **59** (1979), 264–289.

[23] J.-J. Sansuc, Groupe de Brauer et arithmétique des groupes algébriques linéaires, *J. Reine Angew. Math.*, **327** (1981), 12–80.

[24] W. Scharlau, Zur Pfisterschen theorie der quadratischen formen, *Invent. Math.*, **6** (1969), 327–328.

[25] ———, Induction theorems and the structure of the Witt group, *Invent. Math.*, **11** (1970), 37–44.

[26] ———, Quadratic and hermitian forms, Grundlehren der Math. Wiss. 270, Springer-Verlag, (1985).

[27] J.-P. Serre, Cohomologie galoisienne des groupes algébriques linéaires, Colloque sur les groupes algébriques, Bruxelles, (1962), 53–68 (= Oeuvres Vol. II, n° 53, 153–167).

[28] ———, Corps locaux, Hermann, Paris, (1968).

[29] ———, Cohomologie galoisienne, *Lecture Notes in Mathematics 5*, Springer-Verlag, (1973).

[30] ———, L'invariant de Witt de la forme $\mathrm{Tr}(x^2)$, *Comm. Math. Helv.*, **59** (1984), 651–676 (= Oeuvres Vol. III, n° 131, 675–700).

[31] T. Springer, Sur les formes quadratiques d'indice zéro, *C. R. Acad. Sci. Paris*, **234** (1952), 1517–1519.

[32] ———, On the equivalence of quadratic forms, *Indag. Math.*, **21** (1959), 241–253.

[33] A. Wagner, On the classification of the classical groups, *Math. Z.*, **97** (1967), 66–76.