SELF-DUAL NORMAL BASES AND TRACE FORMS OF GALOIS ALGEBRAS

E. Lequeu
Mathematisches Institut, Georg-August-Universität Göttingen, Bunsenstrasse 3-5, 37073 Göttingen, Germany • E-mail : lequeu@uni-math.gwdg.de

Abstract. In this note, we present a survey on the problem of the existence of a self-dual normal basis in a finite Galois extension and say how this problem is related to the study of trace forms of Galois algebras.

1. Self-dual normal bases

Let $K$ be a commutative field and $L$ be a finite Galois extension of $K$. We denote by $\Gamma$ the Galois group of $L/K$. A normal basis of $L/K$ is a $K$-basis of $L$ of the form $(\gamma(x_0))_{\gamma \in \Gamma}$, for some $x_0$ in $L^\times$. It is well known that every finite Galois extension has a normal basis (cf. [Bou59] and [Bou52]). The trace form of $L/K$ is the non-degenerate symmetric bilinear form $b_L : L \times L \rightarrow K$ defined by

$$b_L(x,y) = \text{tr}_{L/K}(xy)$$

for all $x, y \in L$.

A normal basis $(\gamma(x_0))_{\gamma \in \Gamma}$ of $L/K$ is said to be self-dual if

$$b_L(\gamma(x_0), \gamma'(x_0)) = \delta_{\gamma, \gamma'}$$

for all $\gamma, \gamma' \in \Gamma$.

As we will see (cf. Theorem 1.2), not every Galois extension has a self-dual normal basis. So, one can ask the following...
Question 1.1. Which finite Galois extensions have a self-dual normal basis?

No complete answer to this question is known. Let us recall the main results on this topic. E. Bayer-Fluckiger and H. W. Lenstra, Jr. gave a complete criterion for the existence of a self-dual normal basis in an abelian extension (cf. [BFL90]):

Theorem 1.2. Let $L/K$ be a finite abelian extension with Galois group $\Gamma$.

a) Assume that $\text{char}(K) \neq 2$. Then $L/K$ has a self-dual normal basis if and only if $[L : K]$ is odd.

b) Assume that $\text{char}(K) = 2$. Then $L/K$ has a self-dual normal basis if and only if the exponent of $\Gamma$ is not divisible by 4.

They proved also that every Galois extension of odd degree has a self-dual normal basis (cf. [BF89] and [BFL90]):

Theorem 1.3. Let $L/K$ be a finite Galois extension. If $L/K$ is of odd degree, then $L/K$ has a self-dual normal basis.

E. Bayer-Fluckiger and J.-P. Serre provided still partial results for the self-dual normal basis problem for Galois extensions of characteristic not 2 and of even degree (cf. [BFS94]).

2. A reformulation of the problem

We will see that the self-dual normal basis problem for a Galois extension with Galois group $\Gamma$ can be reformulated in terms of $\Gamma$-symmetric spaces.

Let $G$ be a finite group and $K$ a commutative field. A $G$-symmetric space over $K$ is a pair $(V, q)$, where $V$ is a finite dimensional $K$-vector space with an operation of $G$ by automorphisms of $V$ and $b : V \times V \to K$ is a non-degenerate symmetric bilinear form such that

$$b(g \cdot u, g \cdot v) = b(u, v)$$

for all $u, v \in V$ and $g \in G$.

Examples 2.1.

a) Let $L/K$ be a finite Galois extension with Galois group $\Gamma$. Then the pair $(L, b_L)$ is a $\Gamma$-symmetric space over $K$ for the natural operation of $\Gamma$ on $L$.

b) Let $K[G]$ be the group algebra of $G$ over $K$ with the natural operation of $G$. We denote by $b_0 : K[G] \times K[G] \to K$ the symmetric bilinear form defined by

$$b_0(g, h) = \delta_{g,h}$$
for all \( g, h \in G \).

Then the pair \((K[G], b_0)\) is a \( G \)-symmetric space over \( K \) called the unit \( G \)-symmetric space.

Let \((V, b)\) and \((V', b')\) two \( G \)-symmetric spaces over \( K \). One says that \((V, b)\) and \((V', b')\) are isomorphic if there exists an isomorphism of \( K \)-vector spaces \( f : V \to V' \) such that

\[
f(g \cdot v) = g \cdot f(v)
\]

for all \( v \in V \) and \( g \in G \);

\[
b'(f(u), f(v)) = b(u, v)
\]

for all \( u, v \in V \).

If so, one writes \((V, b) \simeq_G (V', b')\).

The following fact (cf. [BFL90]) leads to a reformulation of the self-dual normal basis problem:

**Proposition 2.2.** Let \( L/K \) be a finite Galois extension with Galois group \( \Gamma \). The following conditions are equivalent:

a) \( L/K \) has a self-dual normal basis.

b) \((L, b_L)\) and \((K[G], b_0)\) are isomorphic as \( \Gamma \)-symmetric spaces.

### 3. Some notations

From now, \( G \) is a finite group and \( K \) is a commutative field of \( \text{char}(K) \neq 2 \). Then symmetric bilinear forms over \( K \) correspond bijectively to quadratic forms over \( K \). We will consider quadratic forms instead of symmetric bilinear forms and \( G \)-quadratic spaces instead of \( G \)-symmetric spaces.

If \( L \) is a finite Galois extension of \( K \), we denote by \( q_L : L \to K \) the quadratic form associated with the symmetric bilinear form \( b_L : L \times L \to K \). We denote by \( q_0 : K[G] \to K \) the quadratic form associated with the symmetric bilinear form \( b_0 : K[G] \times K[G] \to K \).

Let \( \text{Quadr}(G, K) \) be the category of \( G \)-quadratic spaces over \( K \). We will need the following functors, which are defined as usual (cf. [Leq03]):

- the scalar extension functor
  \[
  \text{Quadr}(G, K) \to \text{Quadr}(G, E), \ (V, q) \mapsto (V, q)_E,
  \]
  for any field extension \( E/K \);

- the restriction functor
  \[
  \text{Quadr}(G, K) \to \text{Quadr}(S, K), \ (V, q) \mapsto \text{Res}_S^G(V, q),
  \]
  for any subgroup \( S \) of \( G \);

- the induction functor
Quadr$(S, K) \to \text{Quadr}(G, K)$, $(V, q) \mapsto \text{Ind}_{S}^{G}(V, q)$, for any subgroup $S$ of $G$.

4. Odd degree extensions

One has the following result (cf. [CP84]):

**Lemma 4.1.** Let $L$ be a finite Galois extension of $K$ with Galois group $\Gamma$. Then the $\Gamma$-quadratic spaces $(L, q_{L})_{L}$ and $(K[\Gamma], q_{0})_{L}$ over $L$ are isomorphic.

Moreover, in [BFL90], E. Bayer-Fluckiger and H. W. Lenstra, Jr. prove the

**Theorem 4.2.** Let $(V, q)$ and $(V', q')$ be two $G$-quadratic spaces over $K$. Let $E$ be an extension of $K$ of odd degree. Then $(V, q) \simeq_{G} (V', q')$ if and only if $(V, q)_{E} \simeq_{G} (V', q')_{E}$.

It follows from Lemma 4.1, Theorem 4.2 and Proposition 2.2 that every Galois extension $L$ of $K$ of odd degree has a self-dual normal basis (cf. th. 1.3).

5. Galois algebras

In the previous section, we have seen that it can be useful to pass to finite extensions of the base field. In order to do this, one has to consider not only Galois extensions but Galois algebras.

A Galois algebra over $K$ is an étale $K$-algebra $L$ with an operation of $G$ by automorphisms of $L$ such that $G$ acts simply and transitively on the set $\text{Hom}_{K}^{\text{alg}}(L, K_{s})$, where $K_{s}$ is a separable closure of $K$.

Two $G$-Galois algebras $L$ and $L'$ over $K$ are said to be isomorphic if there exists an isomorphism of $K$-algebras $f : L \to L'$ such that

$$f(g \cdot x) = g \cdot f(x)$$

for all $x \in L$ and $g \in G$.

Let $L$ be a $G$-Galois algebra over $K$. We still denote by $q_{L} : L \to K$ the (quadratic) trace form of $L$. Then $(L, q_{L})$ is a $G$-quadratic space over $K$.

**Example 5.1.** The split $G$-Galois algebra over $K$ is $L_{0} = K \times \ldots \times K$, where $G$ acts by permuting the factors simply and transitively. One has $(L_{0}, q_{L_{0}}) \simeq_{G} (K[G], q_{0})$. 
Let $\text{Gal}(G, K)$ be the category of $G$-Galois algebras over $K$. One defines as usual the two following functors (cf. [Leq03]):

- the scalar extension functor
  
  \[ \text{Gal}(G, K) \to \text{Gal}(G, E), L \mapsto L_E, \]

  for any field extension $E/K$;

- the induction functor
  
  \[ \text{Gal}(S, K) \to \text{Gal}(G, K), M \mapsto \text{Ind}_G^S M, \]

  for any subgroup $S$ of $G$.

6. The induction problem

Of course, the self-dual normal basis problem can be raised in the context of Galois algebras. The reformulation of this problem leads to study the classification of the $G$-quadratic spaces $(L, q_L)$, for $L$ a $G$-Galois algebra (cf. Proposition 2.2 and Example 5.1). In order to do this, E. Bayer-Fluckiger and J.-P. Serre developed in [BFS94] the following method.

**Proposition 6.1.** Let $L$ be a $G$-Galois algebra over $K$. Let $S$ be a 2-Sylow subgroup of $G$. Then there exist $E$ an extension of $K$ of odd degree and $M$ a $S$-Galois algebra over $E$ such that $L_E$ and $\text{Ind}_G^S M$ are isomorphic as $G$-Galois algebras over $E$.

Let $L$ and $L'$ be two $G$-Galois algebras over $K$. Let $S$ be a 2-Sylow subgroup of $G$. It follows from Proposition 6.1 that there exist $E$ an extension of $K$ of odd degree and $M$ and $M'$ two $S$-Galois algebras over $E$ such that the $G$-Galois algebras $L_E$ and $\text{Ind}_G^S M$ are isomorphic and the $G$-Galois algebras $L'_E$ and $\text{Ind}_G^S M'$ are isomorphic. Then, from th. 4.2, one has:

\[ (L, q_L) \cong_G (L', q_{L'}) \iff (L, q_L)_E \cong_G (L', q_{L'})_E \]
\[ \iff \text{Ind}_G^S(M, q_M) \cong_G \text{Ind}_G^S(M', q_{M'}). \]

This leads to raise the induction problem:

**Problem 6.2.** Let $S$ be a 2-Sylow subgroup of $G$. Let $(V_1, q_1)$ and $(V_2, q_2)$ be two $S$-quadratic spaces over $K$. Could one give necessary and sufficient conditions for the $G$-quadratic spaces $\text{Ind}_G^S(V_1, q_1)$ and $\text{Ind}_G^S(V_2, q_2)$ to be isomorphic?

E. Bayer-Fluckiger and J.-P. Serre gave such conditions in the case where $S$ is elementary abelian (cf. [BFS94]). Their result can be generalized to the case where $S$ is abelian (cf. [Leq03]) and be formulated as follows:
**Theorem 6.3.** Let $S$ be a 2-Sylow subgroup of $G$. Suppose that $S$ is abelian. Let $N$ be the normalizer of $S$ in $G$. Let $(V_1, q_1)$ and $(V_2, q_2)$ be two $S$-quadratic spaces over $K$. Then the following conditions are equivalent:

a) The $G$-quadratic spaces $\text{Ind}_S^G(V_1, q_1)$ and $\text{Ind}_S^G(V_2, q_2)$ are isomorphic.

b) The $S$-quadratic spaces $\text{Res}_S^G\text{Ind}_S^G(V_1, q_1)$ and $\text{Res}_S^G\text{Ind}_S^G(V_2, q_2)$ are isomorphic.

c) The $N$-quadratic spaces $\text{Ind}_S^N(V_1, q_1)$ and $\text{Ind}_S^N(V_2, q_2)$ are isomorphic.

Under certain additional hypotheses, these results let to state cohomological criteria for the isomorphy of the $G$-quadratic spaces $(L, q_L)$ and $(L', q_{L'})$, for $L$ and $L'$ two $G$-Galois algebras, and, consequently, for the existence of a self-dual normal basis in a $G$-Galois algebra (cf. [BFS94] and [Leq03]).

### References


