Self-Dual Normal Bases and Related Topics

Eva Bayer-Fluckiger

Laboratoire de Mathématiques de Besançon
UMR 6623 du CNRS
16, route de Gray
25030 Besançon
France
e-mail: bayer@math.univ-fcomte.fr

1 Introduction

It is known since more than 20 years that an odd degree extension of finite fields has a self-dual normal basis (cf. [14]). This result can be reformulated in terms of G-forms, that is forms invariant by the action of a group G. It is easy to check that the trace form of a Galois extension with group G is a G-form, and the above result is equivalent to saying that this G-form is isomorphic to the unit G-form. More generally, one can ask for the classification of trace forms of extensions with group G as G-forms.

It is more natural, and also more useful, to study this problem in the more general framework of *Galois algebras* rather than just of Galois extensions. This is the point of view of the papers [1]–[5], where some partial results are proved. For instance, if G is a group of odd order, then any G-Galois algebra has a self-dual normal basis (cf. [1], [2]). §2–5 of the present paper contains a survey of the basic notions and results in this topic. Further results, obtained for fields of characteristic $\neq 2$, are often formulated in terms of cohomological invariants. This is the subject matter of §6, where the notion of *G-discriminant* is introduced (this invariant is implicit in [5]). For the fields of cohomological dimension 1 (for instance, finite fields) the G-discriminant is a complete invariant.

In the case of extensions of finite fields, the G-discriminant can take at most two values, hence there are at most two possibilities for the isomorphism class of the G-trace form. This leads to the notion of *semi-dual normal basis* (cf. §8) and the result that every extension of finite fields of characteristic $\neq 2$ has either a self-dual normal basis or a semi-dual normal basis. Some explicit models for the corresponding G-forms are given in §9.

2 Which Galois Extensions Have a Self-Dual Normal Basis ?

As pointed out in the introduction, there are several ways of formulating this question. In this section, we start with the most elementary one.

Let k be a field, and let L be a Galois extension of k with Galois group G. A *normal basis* of L over k is a basis of the form $(g(e))_{g \in G}$, for some $e \in L^*$. It is well-known that every Galois extension has a normal basis.

The extension L/k being separable, the *trace form*

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

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

is a non-degenerate symmetric bilinear form.

We say that a normal basis $(g(e))_{g \in G}$ is also *self-dual* if

$$q_L(g(e), h(e)) = \delta_{g,h}.$$

As we will see, *not* every Galois extension has a self-dual normal basis. To my knowledge, the question of deciding which Galois extensions have a self-dual normal basis was first raised in the context of *finite fields*, in the book of McWilliams and Sloane [12]. It is proved in [12] that $\mathbf{F}_{2^n}$ has a self-dual normal basis over $\mathbf{F}_2$ provided n is *odd*. In the 80's, this question was taken up by several authors : Imamura [8], Beth–Fumy–Mühlfeld [6], Morii–Imamura [13], Lempel [10], and Lempel–Weinberger [11]. This led to a complete solution to the self-dual normal basis problem for finite fields, that is (cf. [11]) :

Theorem 2.1. *Let k be a finite field. Then an extension L/k of degree n has a self-dual normal basis if and only if one of the following holds :*

1. char $(k) \neq 2$, *and n is odd ;*
2. char $(k) = 2$, *and* $n \not\equiv 0 \pmod 4$.

More recently, some other authors – in particular, Conner–Perlis [7], H.W. Lenstra, Jr. – raised the question of the existence of self-dual normal basis for more general fields. The following result of Lenstra extends th. 1.1. to *abelian* extensions of arbitrary fields (cf. [3])

Theorem 2.2. *Let L be a Galois extension of finite degree n over k, and let $G =$ (Gal)(L/k). Suppose that G is abelian.*

1. *Assume that* char $(k) \neq 2$. *Then there exists a self-dual normal basis of L over k if and only if n is odd.*
2. *Assume that* 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.

In the case of Galois extensions with non-abelian group, no complete criterion for the existence of self-dual normal bases is available. However, the fact that extensions of *odd degree* always have a self-dual normal basis does extend to this case.

Theorem 2.3. [1], [3] *Every Galois extension of odd degree has a self-dual normal basis.*

The proof of this result uses a reformulation of the self-dual normal basis problem in terms of *G-forms*. This will be the topic of the next section.

3 A Reformulation of the Self–Dual Normal Basis Problem

Let k be a field, and let L be a Galois extension of k with group G. Let us denote by $k[G]$ the group algebra. The fact that L has a normal basis over k can be reformulated by saying that the $k[G]$-module L is free of rank one, in other words we have an isomorphism of $k[G]$-modules $L \simeq k[G]$. It is natural to look for a similar "structural" formulation of the existence of a self-dual normal basis. This leads to the notion of *G-form*. Indeed, if q_L is the trace form of L/k then it is immediate that

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

for all $g \in G$, and for all $x, y \in L$. More generally, one defines the notion of G-form as follows :

For any finite group G, a *G-form* will be a pair (V, q), where V is a $k[G]$–module and also a finite dimensional k–vector space, and $q : V \times V \to k$ a non–degenerate symmetric bilinear form such that

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

for all $g \in G$, and for all $x, y \in V$.

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

The *unit G-form* will be the pair $(k[G], q_0)$, with

$$q_0(g, h) = \delta_{g,h}.$$

The unit G-form will often be denoted by q_0.

The reformulation of the self–dual basis problem is based on the following fact :

Proposition 3.1. *Let L be a Galois extension of k with group G. Then L has a self-dual normal basis over k if and only if $q_L \simeq_G q_0$*

Proof. This is clear. □

We see that the question of the existence of a self-dual normal basis is equivalent to a question about the structure of the trace form as a G–form, namely whether it is isomorphic to the simplest possible G-form, the unit G-form. More generally, one could ask for the characterisation of trace forms of Galois extensions with group G as G-forms. We will come back to this question in a slightly more general context in section 5.

4 Odd Degree Extensions

According to th. 3, every Galois extension of odd degree has a self-dual normal basis. The aim of this section is to outline a proof of this result, and to stress the importance of *base change* (extension of the base field) in the process. This again will lead us to look at the self-dual normal basis problem in a different way.

Let L be a Galois extension of k with group G. We have seen that the existence of a self-dual normal basis of L over k is equivalent to the existence of an isomorphism $(L, q_L) \simeq_G (k[G], q_0)$.

It is interesting to note that such an isomorphism *always* exists after a finite base change. Indeed, let us look at the field extension L/k, and let us base change the G-form (L, q_L) to this field extension. We have $L \otimes_k L = L \times \cdots \times L$, the number of copies being equal to $n = [L : k] = |G|$. This is an $L[G]$-module, the action of G being a transitive permutation on the factors. The extension of the G-form q_L to L/k is the unit G form q_0 over L. Hence we obtain an isomorphism $(L, q_L) \otimes_k L \simeq_G (k[G], q_0) \otimes_k L$. The two G-forms (L, q_L) and $(k[G], q_0)$ become isomorphic over the field extension L/k.

The above isomorphism holds independently of the value of the degree of the field extension $[L : k] = n$. However, if this degree is *odd*, then we have a result that enables us to deduce that the G-forms are already isomorphic over k :

Theorem 4.1. [3] *Suppose that* char $(k) \neq 2$. *If two G-forms become isomorphic over an odd degree extension of k, then they are isomorphic over k.*

Note that we recover th. 3 as a consequence of th. 5 :

Corollary 4.2. [1], [3] *Every Galois extension of odd degree has a self-dual normal basis.*

If char $(k) \neq 2$, then the corollary is an immediate consequence of th. 5. The statement still holds for fields of characteristic 2, but the proof is less direct, cf. [1].

It would be interesting to have an analogue of th. 5 for fields of characteristic 2.

5 Galois Algebras

In the last section, we have seen that it is sometimes useful to pass to finite extensions of the ground field. However, this operation does not preserve the property of being a field extension. If L/k is a separable extension of finite degree, and k'/k a finite extension, then $L \otimes_k k'$ is not a field in general. It is a product of separable extensions of k', that is, an *étale algebra.* If moreover L/k is a Galois extension with group G, then $L \otimes_k k' = L' \times \cdots \times L'$, where

L'/k' is a Galois extension with group $G' \subset G$. The group G operates on $L \otimes_k k'$, and the $k'[G]$-module $L \otimes_k k'$ is still free of rank one. In other words, we obtain a *G-Galois algebra* over k'. This notion can be defined in several ways (cf. for instance [5], [9]). For instance, one can define it as follows :

Let k_s be a separable closure of k. For any finite group G, we say that a k-algebra L of finite rank with an operation of G is a *G-Galois algebra* over k if $L \otimes_k k_s = k_s \times \cdots \times k_s$, and if the group G permutes the factors k_s simply transitively.

The category of G-Galois algebras is stable by base change : if L is a G-Galois algebra over k, then $L \otimes_k k'$ is a G-Galois algebra over k'.

Let L be a G-Galois algebra over k. We still denote by $q_L : L \times L \to k$ the trace form, defined as before by $q_L(x,y) = (\mathrm{tr}_{L/k}(xy)$. Then q_L is a G-form.

The *split G-Galois algebra* is $L_0 = k \times \cdots \times k$, where G acts by permuting the factors transitively. The trace form q_{L_0} is isomorphic to the unit G-form q_0.

We see that the self-dual normal basis question is equivalent to asking whether the trace form q_L of a Galois extension – or, more generally, of a G-Galois algebra – is isomorphic as a G-form to the trace form of a specific G-Galois algebra, namely L_0. More generally, it is natural to ask the following questions :

Question 5.1. Let L_1 and L_2 be two G-Galois algebras over k. When do we have

$$q_{L_1} \simeq_G q_{L_2} \text{ ?}$$

Question 5.2. Let q be a G-form. Does there exist a G-Galois algebra L such that

$$q_L \simeq_G q \text{ ?}$$

In the case of groups of odd order, both questions can be answered :

Theorem 5.3. *Let G be a finite group of odd order, and let L be a G-Galois algebra. Then $q_L \simeq_G q_0$.*

The proof is the same as in the case of Galois extensions, cf. section 4. For groups of even order, a few results are known, and the following sections will give a survey of these. However, questions 7 and 8 are far from being solved in general.

6 Cohomological Invariants

Classification results of quadratic forms are often formulated in terms of cohomological invariants. It is natural to try this approach also for trace forms of G-Galois algebras.

From now on, we always suppose that the field k has *characteristic different from 2.* Let k_s be a separable closure of k, and set $\Gamma_k = \mathrm{Gal}(k_s/k)$.

To any G-Galois algebra L, one associates a continuous homomorphism $\phi_L : \Gamma_k \to G$ (see for instance [5], 1.3.1.). Under this correspondence, the isomorphism classes of G-Galois algebras are in bijection with the conjugacy classes of continuous homomorphisms $\Gamma_k \to G$. The algebra L is a field if and only if ϕ_L is onto; it is split if and only if $\phi_L = 1$.

The homomorphism ϕ_L can be used in several ways to attach cohomological invariants to L, and to q_L.

6.1 Galois Descent

Recall that if U is a smooth linear algebraic group over k, then one defines a pointed set $H^1(k, U) = H^1(\Gamma_k, U(k_s))$, cf. [14], I.5. and III.1. This pointed set is very useful in classification questions when U can be identified as an automorphism group. For instance, if U is the group of automorphisms of the unit G-form q_0, then $H^1(k, U)$ is in bijection with the set of isomorphism classes of G-forms that become isomorphic to q_0 over k_s.

Let $^- : k[G] \to k[G]$ be the canonical involution of the group algebra $k[G]$. Recall that this involution is characterised by the fact that $\bar{g} = g^{-1}$ for all $g \in G$.

For any commutative k-algebra E, set

$$U_G(E) = \{x \in E[G] \mid x\bar{x} = 1 \}.$$

Then U_G is a smooth linear algebraic group defined over k. It is immediate that U_G is the group of automorphisms of q_0. Hence the isomorphism class of q_L corresponds to an element $u(L) \in H^1(k, U_G)$.

It is easy to give an explicit description of $u(L)$. Let $f_L : \Gamma_k \to U_G(k_s)$ be the composition of $\phi_L : \Gamma_k \to G$ with the inclusion $G \to U_G(k_s)$. We can regard f_L as a 1-cocycle, and its class is $u(L)$ (cf. [5], 1.5.3.).

Stated in slightly different terms, the map that associates to an isomorphism class of G-Galois algebras the isomorphism class of its trace form is given by

$$H^1(k, G) \to H^1(k, U_G).$$

This cohomological description shows that *the trace form of a G-Galois algebra determines the trace forms of all subalgebras of fixed points* of normal subgroups of G (see also [5], 1.4.1.). Indeed, let L be a G-Galois algebra, and let H be a normal subgroup of G. Let L' be the subalgebra L^H. Then L' is a G/H-Galois algebra. The canonical projection $G \to G/H$ induces a homomorphism $U_G \to U_{G/H}$, which in turn gives rise to a map

$$H^1(k, U_G) \to H^1(k, U_{G/H}).$$

This map sends $u(L)$ to $u(L')$.

6.2 Mod 2 Invariants

Set $H^r(G) = H^r(G, \mathbf{Z}/2\mathbf{Z})$, $H^r(k) = H^r(\Gamma_k, \mathbf{Z}/2\mathbf{Z})$. The homomorphism $\phi_L : \Gamma_k \to G$ induces $\phi_L^* : H^r(G) \to H^r(k)$ for all integers $r \geq 0$. Set $x_L = \phi_L^*(x)$.

Proposition 6.1. ([5], 2.2.1.) *Let L and L' be two G-Galois algebras. If $q_L \simeq_G q_{L'}$, then $x_L = x_{L'}$ for all $x \in H^1(G)$.*

Corollary 6.2. *Let L be a G-Galois algebra. If L has a self-dual normal basis over k, then $x_L = 0$ for all $x \in H^1(G)$.*

This property does not extend to $r > 1$ in general (see [5], 10.2). However, for certain groups it is possible to associate higher cohomological invariants to trace forms of G-Galois algebras in this way. This is done in some cases in [5], §§7 and 9 (see also §7 of the present paper).

Recall that $H^1(k) \simeq k^*/k^{*2}$. Hence for any $x \in H^1(G)$, we obtain an invariant $x_L \in k^*/k^{*2}$. This invariant is easy to describe in concrete terms. Indeed, any non-trivial element of $H^1(G)$ determines a quotient of order 2 of G. Let K be the corresponding subalgebra of fixed points. Then K is a quadratic subalgebra of L, and x_L is its discriminant. By the preceeding remarks the trace form q_K, and hence also its discriminant, are determined by the G-form q_L.

6.3 G-Discriminant

Reformulating the 1-dimensional cohomological invariant defined in the preceding section leads to the notion of *G-discriminant.* Let G^2 be the subgroup of G generated by the squares. The quotient G/G^2 is an elementary abelian 2-group. The projection $G \to G/G^2$ induces

$$d_G : H^1(k, G) \to H^1(k, G/G^2).$$

Recall that $H^1(k,G)$ is in bijection with the set of isomorphism classes of G-Galois algebras. The *G-discriminant* $d_G(L)$ of a G-Galois algebra is by definition the image by d_G of the cohomology class corresponding to L. With this terminology, we obtain the following reformulations of prop. 10 and cor. 11 :

Proposition 6.3. *Let L and L' be two G-Galois algebras over k. If $q_L \simeq_G q_{L'}$ then $d_G(L) = d_G(L')$.*

Corollary 6.4. *Let L be a G-Galois algebra over k. If L has a self-dual normal basis over k then $d_G(L) = 1$.*

Note that $H^1(k, G/G^2) = \mathrm{Hom}(\Gamma_k, G/G^2)$, the set of continous homomorphisms $\Gamma_k \to G/G^2$. As G/G^2 is an elementary abelian 2-group of rank r, this is also the product of r copies of the square classes k^*/k^{*2}.

7 Groups of Even Order

As in section 5, we suppose that k is a field of characteristic $\neq 2$, and G is a finite group. We have defined an invariant $x_L \in k^*/k^{*2}$ for all $x \in H^1(G)$. This invariant is an obstruction to the existence of self–dual normal bases. Using this invariant, one can show the following :

Proposition 7.1. *Let L be a Galois extension of k with group G. Suppose that G has a quotient of order 2. Then L does not have any self-dual normal basis over k.*

Proof. By hypothesis, G has a quotient of order 2. Let K be the corresponding subalgebra of fixed points, and let $x \in H^1(G)$ be the corresponding cohomology class. As noted in §5, the trace form q_K of the quadratic subalgebra K is determined by q_L, and its discriminant is x_L. As L is a field, K is also a field. But the discriminant of a quadratic extension of a field of characteristic $\neq 2$ is never trivial. Hence L cannot have a self–dual normal basis.

It is natural to ask whether this property extends to all groups of even order. As the following examples show, this is not the case in general.

If $G = \mathrm{PGL}_2(\mathbf{F}_q)$, $q \equiv \pm 3 \pmod 8$, then $H^1(G) = 0$, and $H^2(G)$ has order 2. Let us denote by x the non–trivial element of $H^2(G)$. □

Proposition 7.2. *Let $G = \mathrm{PGL}_2(\mathbf{F}_q)$, with $q \equiv \pm 3 \pmod 8$. Let L and L' be G-Galois algebras. Then $q_L \simeq_G q_{L'}$ if and only if $x_L = x_{L'}$.*

Proof. see [5], 8.1. and 7.5.4. □

Corollary 7.3. *Let L be a Galois extension of k with group $G = \mathrm{PGL}_2(\mathbf{F}_q)$, where $q \equiv \pm 3 \pmod 8$. Then L has a self-dual normal basis over k if and only if L can be embedded in a Galois extension of k with group $\mathrm{SL}_2(\mathbf{F}_q)$.*

Proof. [5], th. 8.1.1. and Remarque.

If $G = \mathrm{SL}_2(\mathbf{F}_8)$ or $G = J_1$, the first Janko group, then $H^1(G) = H^2(G) = 0$, and $H^3(G)$ is cyclic of order 2. Let us denote by x the non–trivial element of $H^3(G)$.

Proposition 7.4. *Let $G = \mathrm{SL}_2(\mathbf{F}_8)$ or $G = J_1$. Let L and L' be two G-Galois algebras over k. Then $q_L \simeq_G q_{L'}$ if and only if $x_L = x_{L'}$.*

Proof. See [5], 8.2 and 7.5.4.

Note that the groups of prop. 15 and 17 have elementary abelian 2–Sylow subgroups (of rank 2 and 3, respectively). More generally, if G has elementary abelian or quaternionian 2–Sylow subgroups then one obtains complete criteria for the G–isomorphism of the trace forms of G–Galois algebras : see [5], §§7, 8 and 9. The criteria can often be expressed in terms of higher cohomological invariants. A survey of these results is given in [2], 7.7 and 7.8., as well as in [14], III, Appendice 2.

8 Semi-Dual Normal Bases

We have seen in §1 that an extension of finite fields of char $\neq 2$ has a self-dual normal basis if and only if the degree of the extension is odd. The aim of this section is to propose a substitute of self-dual normal bases, called *semi-dual normal bases*, for extensions of even degree.

Several of the results that we need for this are valid in a much more general context. Even though the main emphasis here is on finite fields, we will state the results in a greater generality.

As in the preceeding sections, k will be a field of characteristic $\neq 2$ and G a finite group.

8.1 Fields of Dimension ≤ 1

Let k_s be a separable closure of k, and set $\Gamma_k = \mathrm{Gal}(k_s/k)$. We say that the 2-cohomological dimension of Γ_k is ≤ 1, written $\mathrm{cd}_2(\Gamma_k) \leq 1$, if $H^n(\Gamma_k, C) = 0$ for all $n > 1$ and for all finite 2-primary Γ_k-modules C (cf. [14], II.3.). For instance, finite fields have this property.

It is proved in [5], 2.2., that when $\mathrm{cd}_2(\Gamma_k) \leq 1$, the criteria of prop. 10 and cor. 11 are necessary and sufficient. More precisely, we have :

Theorem 8.1. *Suppose that* $\mathrm{cd}_2(\Gamma_k) \leq 1$. *Let L and L' be two G-Galois algebras over k. Then $q_L \simeq_G q_{L'}$ if and only if $x_L = x_{L'}$ for all $x \in H^1(G)$.*

Proof. See [5], th.2.2.3.

This can be reformulated as follows :

Theorem 8.2. *Suppose that* $\mathrm{cd}_2(\Gamma_k) \leq 1$. *Let L and L' be two G-Galois algebras over k. Then $q_L \simeq_G q_{L'}$ if and only if $d_G(L) = d_G(L')$.*

Corollary 8.3. *Suppose that* $\mathrm{cd}_2(\Gamma_k) \leq 1$. *Let L be a G-Galois algebra over k. Then L has a self-dual normal basis over k if and only if $d_G(L) = 1$.*

We also obtain a converse of prop. 14 in the case where $\mathrm{cd}_2(\Gamma_k) \leq 1$:

Corollary 8.4. *Suppose that* $\mathrm{cd}_2(\Gamma_k) \leq 1$. *Let L be a Galois extension of k with group G. Then L has a self-dual normal basis over k if and only if $H^1(G, \mu_2) = 0$, i.e. G has no quotient of order 2.*

The preceding results show that the G-discriminant provides a complete invariant when $\mathrm{cd}_2(\Gamma_k) \leq 1$. It remains to see which elements of $H^1(k, G/G^2)$ $= \mathrm{Hom}(\Gamma_k, G/G^2)$ are realised as G-discriminants of G-Galois algebras. This is done in [4] :

Theorem 8.5. *Suppose that* $\mathrm{cd}_2(\Gamma_k) \leq 1$. *Then*

$$d_G : H^1(k, G) \to H^1(k, G/G^2) = \mathrm{Hom}(\Gamma_k, G/G^2)$$

is onto.

Combining th. 18 and 22 we obtain (cf. [4]) :

Corollary 8.6. *Suppose that* $\mathrm{cd}_2(\Gamma_k) \leq 1$. *Then the set of isomorphism classes of trace forms of G-Galois algebras is in bijection (as pointed sets) with* $\mathrm{Hom}(\Gamma_k, G/G^2)$.

Suppose that G is a cyclic group of even order. Then G/G^2 has order 2, we have $H^1(k, G/G^2) \simeq k^*/k^{*2}$, and the G-discriminant becomes

$$d_G : H^1(k, G) \to k^*/k^{*2}.$$

Suppose also that $\mathrm{cd}_2(\Gamma_k) \leq 1$. Then by th. 22, the G-discriminant is onto. For all $d \in k^*/k^{*2}$, there exist G-Galois algebras with G-discriminant d. Let us choose a G-Galois algebra L_d with $d_G(L_d) = d$, and let us denote $Q_d = q_{L_d}$ its trace form. As the G-discriminant is a complete invariant (cf. th. 19), the trace form of any G-Galois algebra is isomorphic to Q_d for some d. We have $Q_1 = q_0$, the trace form of the split G-Galois algebra.

Note that in the case of cyclic groups, the G-discriminant coincides with the usual discriminant of the étale algebra (cf. [4]).

If moreover k has only two square classes, $k^*/k^{*2} = \{1, D\}$, then there are only two possible discriminants, hence only two possible G-trace forms, Q_1 and Q_D. By definition, L has a self-dual normal basis if and only if $q_L \simeq Q_1$ ($=q_0$). We say that a G-Galois algebra has a *semi-dual normal basis* if $q_L \simeq Q_D$. Hence every G-Galois algebra has either a self-dual normal basis, or a semi-dual normal basis.

Extensions of even degree of finite fields satisfy all the above hypotheses, hence we obtain

Proposition 8.7. *Let q be an odd prime number. Then*

1. *If n is odd,* $\mathbf{F}_{q^n}$ *has a self-dual normal basis;*
2. *If n is even,* $\mathbf{F}_{q^n}$ *has a semi-dual normal basis.*

The above results raise the problem of constructing explicit models for Q_D, and hence for semi-dual normal bases. This will be done in the next section.

9 Models for G–Trace Forms

Let k be a field of char $\neq 2$, and such that $\mathrm{cd}_2(\Gamma_k) \leq 1$. Let G be a cyclic group, and let L be a G-Galois algebra over k with discriminant d. As usual, we denote by q_L its trace form. If G has odd order, then L has a self-dual normal basis over k and the G-form q_L is isomorphic to the split G-form q_0. If G has even order, then no self-dual normal basis exists in general. In particular, if L is a field, Galois extension of k with group G of even order, then L does not have any self-dual normal basis over k. However, we saw in §8 that the G-form q_L is uniquely determined by the discriminant of L. In other words, q_L is isomorphic to a G-form that we denoted by Q_d in §7. The aim of this section is to give explicit models for the G-form Q_d.

All the above hypothesis are satisfied in the case of extensions of finite fields, which is the main case of interest here. The essential case is the one where G is a cyclic group of prime power order. We consider this case first, and then come back to the case of arbitrary cyclic groups.

9.1 Cyclic Groups of 2-Power Order

Suppose that G is cyclic of order $N = 2^n$, and let σ be a generator of G. Let V be the free $k[G]$-module of rank one with k-basis $e_1, \dots, e_N$, satisfying $\sigma(e_i) = e_{i+1}$ (indices mod N). Let $d \in k^*$. Set $a = \frac{1-d}{N}$, and let $Q_d : V \to k$ be defined by $Q_d(e_i, e_i) = a + 1$, $Q_d(e_i, e_j) = (-1)^{|i-j|}a$ if $i \neq j$. It is easy to check that Q_d is a G-form and has determinant d.

Note that $d = 1$ if and only if $a = 0$, and this happens if and only if Q_d is the unit G-form.

Expressed in coordinates, we have

$$Q_d(X_1, \dots, X_d) = \Sigma_{i=1,\dots,N} X_i^2 + a(X_1 - X_2 + \dots - X_N)^2.$$

Another possible model for Q_d gives a diagonal quadratic form, but it is no longer expressed in a normal basis. It is obtained by writing $k[G]$ as $k[X]/(X^N - 1)$, factorising $X^N - 1$ as a product of cyclotomic polynomials, and decomposing $k[G]$ accordingly. We obtain in this way a natural basis $f_1, \dots, f_N$ together with the action of σ. We have $Q_d(f_i) = 1$ if $i \neq 2$ and $Q_d(f_2) = d$.

Example 9.1. $N = 8$, $\sigma(f_1) = f_1$, $\sigma(f_2) = -f_2$, $\sigma(f_3) = f_4$, $\sigma(f_4) = -f_3$, $\sigma(f_5) = f_6$, $\sigma(f_6) = f_7$, $\sigma(f_7) = f_8$, $\sigma(f_8) = -f_5$.

9.2 Arbitrary Cyclic Groups

Let G be a cyclic group of order mN, where m is odd and N is a power of 2. Then G has a unique cyclic subgroup H of order N. A model of Q_d for the group G, denoted by Q_d^G, is obtained by taking the orthogonal sum of m copies of a model Q_d^H for H.

Example 9.2. Let G be of order $2m$, m odd. Let $d = -1$. A model for the cyclic group of order 2 is obtained by $\sigma(e_1) = e_2$, $\sigma(e_2) = e_1$, quadratic form given by the matrix $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. A model for Q_d will be the orthogonal sum of m copies of this model. The quadratic form is then hyperbolic, and one might call this basis a *hyperbolic normal basis.*

References

1. Bayer-Fluckiger, E. : Self-dual normal bases. Indag. Math. **51** (1989) 379-383
2. Bayer-Fluckiger, E. : Galois cohomology and the trace form. Jahresber. DMV **96** (1994) 35-55
3. Bayer-Fluckiger, E., Lenstra, H.W., Jr. : Forms in odd degree extensions and self-dual normal bases. Amer. J. Math. **112** (1990) 359-373
4. Bayer-Fluckiger, E., Monsurro, M., Parimala, R., Schoof, R. : Trace forms of G-Galois algebras over fields of cohomological dimension ≤ 2. (in preparation)
5. Bayer-Fluckiger, E., Serre, J.-P. : Torsions quadratiques et bases normales autoduales, Amer. J. Math. **116** (1994) 1-64
6. Beth, T., Fumy, W., Mühlfeld, R. : Zur algebraischen diskreten Fourier-Transformation. Arch. Math. (Basel) **40** (1983) 238-244
7. Conner, P., Perlis, R. : A survey of trace forms of algebraic number fields. World scientific, Singapore (1984)
8. Imamura, K., On self-complementary normal bases of $GF(q^n)$ over $GF(q)$. Trans. IECE Japan **E66** (1983) 717-721
9. Knus, M., Merkurjev, A., Rost, M., Tignol, J.-P. : The book of involutions. AMS Colloquium Publications **44** (1998)
10. Lempel, A. : Characterisation and synthesis of self-complementary normal bases in finite fields. Lin. Alg. Appl. **98** (1988) 331-346
11. Lempel, A., Weinberger, M.J. : Self-complementary normal bases in finite fields. SIAM J. Disc. Math. **1** (1988) 193-198
12. MacWilliams, J., Sloane, N.J.A.: The theory of error-correcting codes. North-Holland, Amsterdam (1977)
13. Morii, A., Imamura, K. : 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.
14. Serre, J.-P. : Cohomologie galoisienne. 5ème édition, Lecture Notes in Mathematics **5**, Springer-Verlag (1964, 1994) ; english translation, Galois cohomology, Springer-Verlag (1997).