CADERNOS DE MATEMÁTICA **06**, 135–145 May (2005)
ARTIGO NÚMERO SMA#228

On self-dual normal bases

Dirceu Bágio

IFM-UFPEL
96010-900, Pelotas, RS, Brazil
E-mail: dirceu_bagio@ufpel.tche.br

Ires Dias

ICMC-USP
13560-970, São Carlos, SP, Brazil
E-mail: iresdias@icmc.sc.usp.br

Antonio Paques

IMECC-UNICAMP
13081-970, Campinas, SP, Brazil
E-mail: paques@ime.unicamp.br

We deal with the existence of self-dual normal basis for Galois extensions of a commutative ring. We consider commutative rings which are local, connected semi-local (under some suitable restrictions) or zero-dimensional. We show that for such kind of rings every Galois extension of odd degree has a self-dual normal basis. May, 2005 ICMC-USP

1. INTRODUCTION

Let R be a commutative ring and S be a commutative R-algebra which is a finitely generated projective R-module. Let G be a finite group of R-algebra automorphisms of S. We say that S is a *Galois extension of R with Galois group G* if the map $\psi : S \otimes_R S \to S \times \cdots \times S$ given by $\psi(x \otimes y) = (x\sigma(y))_{\sigma \in G}$ for $x, y \in S$, is an isomorphism of S-algebras. By *degree* of S over R we mean the order of the group G. It is clear from the definition that the order of G is just the rank of S over R. A *self-dual normal basis* for such a Galois extension S of R is a basis of S, as a free R-module, consisting of the elements $\sigma(\alpha)$, $\sigma \in G$, for a fixed element $\alpha \in S$, which is orthonormal with respect to the non-singular symmetric bilinear form $\varphi_t : (x, y) \mapsto \mathrm{t}(xy) = \sum_{\sigma \in G} \sigma(xy)$, $x, y \in S$ (that is, the basis is its own dual with respect to this form).

The existence problem of self-dual normal basis is closely related to the structure of certain bilinear forms associated with the Galois extension S of R and the G-invariant

Publicado pelo ICMC-USP
Sob a supervisão CPq/ICMC

bilinear space (S, φ_t). This problem was firstly considered by P. Conner and R. Perlis in [6]. They proved that any Galois field extension of odd degree of the rational number field $\mathbb{Q}$ has a self-dual normal basis. Later, E. Bayer and H. W. Lenstra ([3], [4]) proved the same assertion for any ground field.

Our aim in this note is to obtain similar results in the context of commutative rings. More precisely we are interested in the following question: the assertion

($\star$) *If S is a Galois extension of R with Galois group G of odd order then it has a self-dual normal basis.*

is true for any commutative ring R and any finite group G of odd order?

Of course this question is restricted to rings for which Galois extensions have normal basis. This question was already pointed out in [17] and it has been answered affirmatively in the case that G is either cyclic [11] or abelian [17], provided that S possesses a normal basis.

We will prove that the above assertion ($\star$) is true for any finite group G of odd order and any commutative ring which is local, connected semi-local in which either 2 or the order of G is a unity or zero-dimensional.

Throughout this note by ring we mean an associative and not necessarily commutative ring with identity. For any ring R we will denote by $R^\times$ the multiplicative group of its unities. For basic facts on Galois theory of commutative rings we refer, for instance, to [5], [7] or [8].

2. PREREQUISITES

2.1. A Generalized Primitive Element Theorem: semi-local case

Theorem 2.1.1 below improves and extends Theorem 1.1 of [19] to the context of commutative semi-local rings which are connected and provides a useful tool to prove Lemma 2.2.2, which is crucial for our purposes. Theorem 2.1.1 allow us to use, in the context of connected semi-local rings, classical arguments due to W. Scharlau [21] in order to obtain Lemma 2.2.2. By a connected commutative ring we mean a commutative ring whose unique idempotents are 0 and 1.

In this subsection all rings considered are commutative. Let $i : R \hookrightarrow S$ be a ring extension. We say that S is a *strongly separable extension* of R if S is separable as R-algebra and finitely generated and projective as R-module. If for any finite subset $N \subseteq S$ there exists a subalgebra L of S which contains N and is a strongly separable extension of R, we say that S is a *locally strongly separable extension* of R. We say that a connected ring is *separably closed* if its unique connected strongly separable extension is itself. We will denote by $\Omega(R)$, up to isomorphism, the (connected) separable closure of a connected ring R, that is, $\Omega(R)$ is a locally strongly separable extension of R which is connected

Publicado pelo ICMC-USP
Sob a supervisão da CPq/ICMC

and separably closed. For more about the (connected) separable closure of a connected commutative ring we refer to [16].

Given a ring extension $R \subseteq S$ we say that S has a *primitive element* over R if there exists $\alpha \in S$ such that $S = R[\alpha]$. The existence of primitive elements for strongly separable extensions holds for fields and, more generally, for some kind of commutative rings under certain restrictive conditions. For instance, any strongly separable extension S of a semi-local ring R has a primitive element over R if and only if $\left|\frac{R}{\mathfrak{m}}\right| \geq rank_R S$, for every maximal ideal $\mathfrak{m}$ of R (see [20]). Theorem 2.1.1 provides a generalization of the primitive element theorem in the case of a connected semi-local ring.

We say that a polynomial $f(X) \in R[X]$ is separable over R if $f(X)$ is monic and $\frac{R[X]}{(f(X))}$ is a separable R-algebra. A monic polynomial $f(X) \in R[X]$ is defined to be *indecomposable* in $R[X]$ if whenever there exist monic polynomials $g(X), h(X) \in R[X]$ such that $f(X) = g(X)h(X)$ it follows that $g(X) = 1$ or $h(X) = 1$.

Theorem 2.1.1 *Let R be a connected commutative semi-local ring and $S \subseteq \Omega(R)$ be a strongly separable extension of R. Then there exist a polynomial $f(X) \in R[X]$ and $\alpha \in \Omega(R)$ such that:*

(i) *$f(X)$ is separable and indecomposable,*

(ii) *$f(\alpha) = 0$, $S \subseteq R[\alpha]$ and $R[\alpha] \simeq \frac{R[X]}{(f(X))}$,*

(iii) *$rank_R R[\alpha] = p^{\epsilon}.rank_R S$, with p a odd prime integer and $\epsilon = 0$ or $\epsilon = 1$,*

(iv) *$f(0) \in R^{\times}$.*

Proof: Let $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$ be all the maximal ideals of R. We will proceed by steps.

Step 1: $\left|\frac{R}{\mathfrak{m}_i}\right| = \infty$, $1 \leq i \leq n$

In this case S has a primitive element over R by ([20], Theorem 2.4). So, there is $\alpha \in S$ such that $S = R[\alpha]$. Consequently, there exists a separable and indecomposable polynomial $f(X) \in R[X]$ such that $f(\alpha) = 0$ and $\frac{R[X]}{(f(X))} \simeq S$ ([18], Theorem 3.3).

By the assumption on the cardinality of the residual fields $\frac{R}{\mathfrak{m}_i}$, for each $1 \leq i \leq n$ there exists $r_i \in R$ such that $f(r_i) \notin \mathfrak{m}_i$. So, there exits $r \in R$ such that $f(r) \in R^{\times}$, by chinese remainder theorem. Now, taking $g(X) = f(X + r)$ we have $g(0) \in R^{\times}$. Clearly, g is separable and indecomposable and $S = R[\alpha] = R[\alpha - r] \simeq \frac{R[X]}{(g(X))}$. Therefore, replacing $f(X)$ by $g(X)$, if necessary, we can assume that $f(0) \in R^{\times}$.

Step 2: $\left|\frac{R}{\mathfrak{m}_i}\right| < \infty$, $1 \leq i \leq n$.

For each $1 \leq i \leq n$, let $\mathfrak{M}_{ij_i}$, with $1 \leq j_i \leq n_i$, be the maximal ideals of S over $\mathfrak{m}_i$ and $q_i = \left|\frac{R}{\mathfrak{m}_i}\right|$. Take $p \in \mathbb{Z}$ a odd prime integer such that p does not divide $\left[\frac{S}{\mathfrak{M}_{ij_i}} : \frac{R}{\mathfrak{m}_i}\right]$ and $\frac{q_i^p - q_i}{n_i} \geq p$, for every $1 \leq j_i \leq n_i$ and $1 \leq i \leq n$. Now consider, for each $1 \leq i \leq n$, a separable and indecomposable polynomial $g_i(X) \in \frac{R}{\mathfrak{m}_i}[X]$ with degree p. Via chinese remainder theorem we get a polynomial $g(X) \in R[X]$ such that $g(X) = g_i(X) \pmod{\mathfrak{m}_i[X]}$,

for every $1 \leq i \leq n$. So, g is separable over R ([10], Theorem 2.2) and over S, since $\frac{S[X]}{(g(X))} \simeq S \otimes_R \frac{R[X]}{(g(X))}$. Furthermore, each polynomial $g_i(X)$ is also indecomposable in $\frac{S}{\mathfrak{M}_{ij_i}}[X]$ by construction and consequently $g(X)$ is indecomposable in $S[X]$. Then it follows that the S-algebra $T = \frac{S[X]}{(g(X))}$ is strongly separable and also connected by ([10], Corollary 2.10). Note that $S \hookrightarrow T$ and by Theorem III 3.3 of [7] we can assume that $T \subseteq \Omega(R)$.

Let $N_{q_i}(p)$ denote the number of all separable and indecomposable polynomials of degree p in $\frac{R}{\mathfrak{m}_i}[X]$. By Theorem 3.25 of [15] we have $N_{q_i}(p) = \frac{q_i^p - q_i}{p}$. Since $N_{q_i}\left(p\left[\frac{S}{\mathfrak{M}_{ij_i}} : \frac{R}{\mathfrak{m}_i}\right]\right) \geq N_{q_i}(p)N_{q_i}\left(\left[\frac{S}{\mathfrak{M}_{ij_i}} : \frac{R}{\mathfrak{m}_i}\right]\right) \geq N_{q_i}(p) \geq n_i$, there exist at least n_i polynomials $h_{i1}(X), \ldots, h_{in_i}(X) \in \frac{R}{\mathfrak{m}_i}[X]$ of degree $p\left[\frac{S}{\mathfrak{M}_{ij_i}} : \frac{R}{\mathfrak{m}_i}\right]$, which are separable and indecomposable, for each $1 \leq i \leq n$. On the other hand, there exists a unique maximal ideal $\mathfrak{Q}_{ij_i}$ of T over $\mathfrak{M}_{ij_i}$ and $\left[\frac{T}{\mathfrak{Q}_{ij_i}} : \frac{S}{\mathfrak{M}_{ij_i}}\right] = p$ ([18],Theorem 3.5). So, $\left[\frac{T}{\mathfrak{Q}_{ij_i}} : \frac{R}{\mathfrak{m}_i}\right] = p\left[\frac{S}{\mathfrak{M}_{ij_i}} : \frac{R}{\mathfrak{m}_i}\right]$ and $\frac{T}{\mathfrak{Q}_{ij_i}} \simeq \frac{\frac{R}{\mathfrak{m}_i}[X]}{(h_{j_i}(X))}$, for every $1 \leq i \leq n$. Since $\mathfrak{m}_i T = \bigcap_{j_i=1}^{n_i} \mathfrak{Q}_{ij_i}$ ([18], Theorem 2.1), we have $\frac{T}{\mathfrak{m}_i T} \simeq \frac{\frac{R}{\mathfrak{m}_i}[X]}{(h_{i1}(X)\cdots h_{in_i}(X))}$. Consequently $\frac{T}{\mathfrak{m}_i T}$ has a primitive element over $\frac{R}{\mathfrak{m}_i}$, for every $1 \leq i \leq n$. So, as in Step 1, there exist $\alpha \in \Omega(R)$ and $f(X) \in R[X]$ satisfying (i)-(iii). Finally, if $f(0) \in \mathfrak{m}_i$, for some $1 \leq i \leq n$, then $f(X) = Xh(X)(\text{mod } \mathfrak{m}_i[X])$, for some $h(X) \in R[X]$ and, by ([18], Theorem 3.5), $\left[\frac{T}{\mathfrak{Q}_{ij_i}} : \frac{R}{\mathfrak{m}_i}\right] = 1$, for some $1 \leq j_i \leq n_i$, which is a contradiction.

Step 3: $\left|\frac{R}{\mathfrak{m}_i}\right| < \infty$ and $\left|\frac{R}{\mathfrak{m}_j}\right| = \infty$, for some $1 \leq i, j \leq n$.

Let $\mathfrak{m}_i$, $1 \leq i \leq l$ (resp. $l+1 \leq i \leq n$) be the maximal ideals of R satisfying $\left|\frac{R}{\mathfrak{m}_i}\right| < \infty$ (resp. $\left|\frac{R}{\mathfrak{m}_i}\right| = \infty$). As in Step 2, consider $p \in \mathbb{Z}$ a odd prime integer such that p does not divide $\left[\frac{S}{\mathfrak{M}_{ij_i}} : \frac{R}{\mathfrak{m}_i}\right]$ and $\frac{q_i^p - q_i}{p} \geq n_i$, for every $1 \leq j_i \leq n_i$ and $1 \leq i \leq l$, where $\mathfrak{M}_{ij_1}, \ldots, \mathfrak{M}_{ij_{n_i}}$ are the maximal ideals of S over $\mathfrak{m}_i$ and $q_i = \left|\frac{R}{\mathfrak{m}_i}\right|$. Take separable and indecomposable polynomials $g_i(X) \in \frac{R}{\mathfrak{m}_i}[X]$ of degree p, for every $1 \leq i \leq l$. As above, there exist separable and indecomposable polynomials $h_{ij_i}(X) \in \frac{R}{\mathfrak{m}_i}[X]$ of degree $p\left[\frac{S}{\mathfrak{M}_{ij_i}} : \frac{R}{\mathfrak{m}_i}\right]$, for every $1 \leq j_i \leq n_i$ and $1 \leq i \leq l$. On the other hand, take polynomials $g_i(X) = \prod_{t=1}^{p}(X - x_{it}) \in \frac{R}{\mathfrak{m}_i}[X]$, with $x_{it} \neq x_{it'}$, for every $1 \leq t \neq t' \leq p$ and $l+1 \leq i \leq n$. Applying again chinese remainder theorem we obtain a separable and indecomposable polynomial $g(X) \in R[X]$ such that $g(X) = g_i(X)(\text{mod } \mathfrak{m}_i[X])$, for every $1 \leq i \leq n$. Considering $T = \frac{S[X]}{(g(X))}$ we have $\frac{T}{\mathfrak{m}_i T} \simeq \frac{\frac{R}{\mathfrak{m}_i}[X]}{(h_{i1}(X)\cdots h_{in_i}(X))}$ and, consequently, $\frac{T}{\mathfrak{m}_i T}$ has a primitive element over $\frac{R}{\mathfrak{m}_i}$, for every $1 \leq i \leq l$. Since $\left|\frac{R}{\mathfrak{m}_i}\right| = \infty$, $\frac{T}{\mathfrak{m}_i T}$ also has a primitive element over $\frac{R}{\mathfrak{m}_i}$, for every $l+1 \leq i \leq l$. Then T has a primitive element over R (Theorem 2.4 of [20]) and so there exist $f(X) \in R[X]$ and $\alpha \in \Omega(R)$ satisfying (i)-(iii). If $1 \leq i \leq l$

Publicado pelo ICMC-USP
Sob a supervisão da CPq/ICMC

(resp. $l+1 \leq i \leq n$) we have $f(0) \notin \mathfrak{m}_i$ (resp. $f(r_i) \notin \mathfrak{m}_i$, for some $r_i \in R$). Hence there exists $r \in R$ such that $f(r) \in R^{\times}$. □

The following example due to Dedekind ([23], page 170) illustrates Theorem 2.1.1 in the case $\left|\frac{R}{\mathfrak{m}}\right| < rank_R S$, for some maximal ideal $\mathfrak{m}$ of R, where the rank condition is non-trivial, that is, $\epsilon = 1$.

Example 2.1.2 Let $\mathbb{Q}$ denotes the rational number field, $E = \mathbb{Q}[\alpha]$, where α is a root of the indecomposable polynomial $f(X) = X^3 + X^2 - 2X + 8 \in \mathbb{Q}[X]$, and $\mathbb{O}$ the integral closure in E of the ring $\mathbb{Z}$ of the rational integers. Note that $2\mathbb{O} = Q_1Q_2Q_3$ where Q_j, $1 \leq j \leq 3$, are the unique maximal ideals of $\mathbb{O}$ over $2\mathbb{Z}$. Take $R = \mathbb{Z}_{(2)}$ the localization of $\mathbb{Z}$ at $2\mathbb{Z}$, $\mathfrak{m} = 2R$ and $S = \mathbb{O}_{(2)} = R \otimes_{\mathbb{Z}} \mathbb{O}$. Clearly S is a free R-module and $2 = \left|\frac{R}{\mathfrak{m}}\right| < rank_R S = 3$. Furthermore, if $M_j = Q_j S$ then $\mathfrak{m}S = M_1M_2M_3$, $\frac{S}{mS} \simeq \frac{S}{M_1} \oplus \frac{S}{M_2} \oplus \frac{S}{M_3}$ and $\frac{S}{M_i} \simeq \frac{R}{m} \simeq \mathbb{F}_2$ for $1 \leq i \leq 3$ (by $\mathbb{F}_q$ we denote the finite field with q elements). So, S is a connected strongly separable extension of R which does not have a primitive element over R. Now consider $g(X) \in R[X]$ a monic polynomial of degree $p = 5$ such that $g(X)$ is indecomposable modulo $\mathfrak{m}[X]$. Following the same arguments used in the proof (step 2) of Theorem 2.1.1 one can easily see that $T = \frac{S[X]}{(g(X))}$ is a connected strongly separable extension of R, $T \supset S$ and $rank_R T = 5.rank_R S$. Furthermore, T has a primitive element over R since $\frac{T}{mT} \simeq \mathbb{F}_{2^5} \oplus \mathbb{F}_{2^5} \oplus \mathbb{F}_{2^5} \simeq \frac{\mathbb{F}_2[X]}{(h(X))}$ with $h(X)$ a product of three distinct monic and indecomposable polynomials over $\mathbb{F}_2$, each one of degree 5.

2.2. Hermitian spaces

Let A be a ring with an involution $^- : A \to A$ and E be a left A-module. A biadditive map $s : E \times E \to A$ is called a *sesquilinear form* if $s(ax, by) = as(x, y)\bar{b}$ for all $x, y \in E$ and $a, b \in A$. By a *hermitian form* over E we mean a sesquilinear form $h : E \times E \to A$ such that $h(x, y) = \overline{h(y, x)}$ for all $x, y \in E$. By a *hermitian space* over A we mean a pair (E, h) where E is a finite generated projective left A-module and h is a non-singular hermitian form, that is, the A-linear map $H : E \to E^* = \mathrm{Hom}_A(E, A)$, given by $H(x)(y) = h(x, y)$, $x, y \in E$, is an isomorphism. A hermitian space (E, h) is said to be *even* if there exists a sesquilinear form $s : E \times E \to A$ such that $h(x, y) = s(x, y) + \overline{s(y, x)}$, for all $x, y \in E$. A hermitian space (E, h) is *hyperbolic* if it is even and if E has a submodule F such that F is a direct summand of E and $F = F^{\perp} = \{x \in E \mid h(x, y) = 0 \text{ for all } y \in F\}$. The notion of isomorphism as well as of orthogonal sums of hermitian spaces is standard and we refer, for instance, to [3] for more details.

We denote by $G(A)$ the Grothendieck group of the isomorphism classes of even hermitian spaces over A, with respect to the orthogonal sum. The *Witt group* $W(A)$ is by definition the quotient of $G(A)$ by the subgroup generated by all the hyperbolic hermitian spaces over A. We will denote by $[E, h]$ the element in $W(A)$ represented by the hermitian space (E, h).

Note that if A is commutative and the involution is trivial, then hermitian spaces over A are symmetric bilinear spaces. The tensor product of symmetric bilinear spaces endows the corresponding Witt group $W(A)$ with an structure of commutative ring with identity element represented by (A, μ) where μ denotes the multiplication in A.

¿From now on assume that A is an R-algebra with an R-linear involution, where R is a commutative ring.

For any commutative ring extension $i : R \hookrightarrow S$ set $A_S = S \otimes_R A$. The extension of scalars induces a canonical group homomorphism $\iota^* : W(A) \to W(A_S)$. And if, in particular, the commutative ring extension $i : R \hookrightarrow S$ is a *Frobenius extension* then the corresponding trace map $t : S \to R$, and its A-linear extension τ induce group homomorphisms $t_* : W(S) \to W(R)$ and $\tau_* : W(A_S) \to W(A)$ given by $t_*([V, \varphi]) = [{}_RV, t \circ \varphi]$ and $\tau_*([E, h]) = [{}_RE, \tau \circ h]$ respectively, for all $[V, \varphi] \in W(S)$ and $[E, h] \in W(A_S)$, where ${}_RV$ (resp. ${}_RE$) denotes the R-module V (resp. E) via the homomorphism $i : R \hookrightarrow S$. The tensor product of an even hermitian space over A with a symmetric bilinear space over R is again an even hermitian space over A. Thus $W(A)$ (resp. $W(A_S)$ is a $W(R)$-module (resp. $W(S)$-module). Furthermore, it is easy to verify that

$$\tau_*([V, \varphi] \otimes \iota^*([E, h])) = t_*([V, \varphi]) \otimes [E, h]$$

for all $[E, h] \in W(A)$ and $[V, \varphi] \in W(S)$. In particular,

$$\tau_*([S, \mu] \otimes \iota^*([E, h])) = t_*([S, \mu]) \otimes [E, h]$$

for all $[E, h] \in W(A)$.

We recall that a commutative ring extension $i : R \hookrightarrow S$ is Frobenius if S is finite generated projective as R-module (with respect to i) and there exists an R-linear map $t : S \to R$ (called *trace map*) such that the corresponding symmetric bilinear form $\varphi_t : S \times S \to R$ given by $\varphi_t(s, s') = t(ss')$, $s, s' \in S$, is non-singular.

Lemma 2.2.1 *Let R be a commutative ring and A be an R-algebra with an R-linear involution. Consider the ring extension $\iota : R \hookrightarrow S = \frac{R[X]}{(f(X))}$, where $f(X) \in R[X]$ is a monic polynomial such that $f(0)$ is a unit in R. If the degree of $f(X)$ is odd then $\iota^* : W(A) \to W(A_S)$ is injective.*

Proof: Let $x = X + (f(X))$ and $t : S \to R$ the trace map given by $t(1) = 1$ and $t(x^i) = 0$ for every $1 \leq i \leq n-1$, where n denotes the degree of $f(X)$. Clearly S is a Frobenius extension of R (see [1], Ch. V, Sec. 3).

Furthermore, if $[E, h]$ is in the kernel of ι^*, then $t_*([S, \mu]) \otimes [E, h] = 0$ in $W(A)$ and by ([1], Ch. V, Proposition 3.3) we have $[E, h] = 0$, for n is odd. Hence ι^* is injective. □

Publicado pelo ICMC-USP
Sob a supervisão da CPq/ICMC

Lemma 2.2.2 *Let R be a commutative connected semi-local ring, S be a connected strongly separable extension of R and A be an R-algebra with an R-linear involution. If $rank_R(S)$ is odd then $\iota^* : W(A) \to W(A_S)$ is injective.*

Proof: By Theorem III 3.3 of [7] we can assume that $S \subseteq \Omega(R)$, where $\Omega(R)$ denotes the (connected) separable closure of R. Now the result follows by Theorem 2.1.1 and Lemma 2.2.1. □

For any hermitian space (E, h) over A and any ring extension $i : R \hookrightarrow S$ we will denote by $h_S : E_S \times E_S \to A_S$ the extension of h to E_S.

Proposition 2.2.3 *Let R, S and A be as in Lemma 2.2.2. Assume that A is also a semi-local ring. Let (E, h) and (E', h') be two even hermitian spaces over A, such that E and E' are free left A-modules of rank 1. If $(E_S, h_S) \simeq (E'_S, h'_S)$ then $(E, h) \simeq (E', h')$.*

Proof: By assumption $[E_S, h_S] = [E'_S, h'_S]$ in $W(A_S)$, so $[E, h] = [E', h']$ in $W(A)$ by Lemma 2.2.2. Thus there are hyperbolic hermitian spaces (N, g) and (N', g') over A such that $(E, h) \perp (N, g) \simeq (E', h') \perp (N', g')$. Then $E \oplus N \simeq E' \oplus N'$ and, consequently, $N \simeq N'$ by ([13], Ch. VI, Corollary 1.3.2). So $(N, g) \simeq (N', g')$ ([2], Claim 4.10.1) and hence $(E, h) \simeq (E', h')$ by ([13], Ch. VI, Corollary 5.7.4). □

2.3. Galois extensions

The following lemma is well known (see for instance [12] and [22]) and it will also used in the next section. We reproduce it here for the sake of completeness.

Given a commutative ring extension $R \hookrightarrow S$, G a subgroup of $\mathrm{Aut}_R(S)$ and $\alpha \in S$, we will denote by G_α the subgroup of all the elements $\sigma \in G$ satisfying $\sigma(\alpha) = \alpha$.

Lemma 2.3.1 *Let R be a connected commutative ring and S be a Galois extension of R with group G. Then there exists a primitive idempotent $v \in S$ such that:*

(i) $S = \bigoplus_{1 \leq i \leq n} S\sigma_i(v)$, *where $\{\sigma_1, \ldots, \sigma_n\} \subseteq G$ is a transversal for G_v in G,*

(ii) $S\sigma_i(v)$ *is a connected Galois extension of $R\sigma_i(v) \simeq R$, with group $G_{\sigma_i(v)}$, for every $1 \leq i \leq n$,*

(iii) $G_{\sigma_i(v)} = \sigma_i G_v \sigma_i^{-1}$, *for every $1 \leq i \leq n$.*

3. THE MAIN RESULTS

In this section we will prove the existence of self-dual normal basis for any Galois extension of odd degree of a commutative ring which is local, connected semi-local under some restrictions or zero-dimensional. We use "zero-dimensional" in the sense of Krull dimension. The methods used in this section are adapted to the semi-local setting from

those used by Bayer-Fluckiger in [3]. The basic idea of the proof of Theorem 3.2 below is contained in that paper.

Let R be a commutative ring and S be a Galois extension of R with Galois group G. Clearly S is a Frobenius extension of R with trace map $t : S \to R$ given by $t = \sum_{\sigma \in G} \sigma$, since S is in particular finite generated and projective of constant rank as R-module and separable as R-algebra. Note also that the action of G on S induces an obvious structure of left RG-module on S. Indeed S is a projective left RG-module ([17], Proposition 2.1).

Now take an element $\alpha \in S$. We say that α *generates a normal basis* of S over R (or S *has a normal basis* over R) if $\mathcal{B} = \{\sigma(\alpha) \,|\, \sigma \in G\}$ is a basis of S as free R-module. We say that S has a *self-dual normal basis* if such a basis $\mathcal{B}$ is orthonormal with respect to the non-singular symmetric bilinear form $\varphi_t : S \times S \to R$ associated to the trace map t given above.

Note that RG is a ring with a canonical R-linear involution $^- : RG \to RG$ given by $\overline{\rho} = \rho^{-1}$ for all $\rho \in G$. Also, the symmetric bilinear space (S, φ_t) over R is associated to the hermitian space (S, H_t) over RG, with $H_t : S \times S \to RG$ given by $H_t(x, y) = \sum_{\rho \in G} \varphi_t(\rho(x), y)\overline{\rho}$ for all $x, y \in S$. Clearly an element $\alpha \in S$ generates a normal basis (resp. a self-dual normal basis) of S over R if and only if $\{\alpha\}$ is a basis (resp. a orthonormal basis with respect to H_t) of S over RG.

Finally denote by (RG, l) the hermitian space over RG with $l : RG \times RG \to RG$ given by $l(x, y) = x\overline{y}$, for all $x, y \in RG$.

Lemma 3.1 *Let R, S, G, (S, H_t) and (RG, l) be as given above. Then the following statements are equivalent:*

(i) *S has a self-dual normal basis.*

(ii) *(S, H_t) and (RG, l) are isomorphic as hermitian spaces over RG.*

(iii) *There exists an element $\alpha \in S$ such that $\{\alpha\}$ is a basis of S over RG and $H_t(\alpha, \alpha) = x\overline{x}$ for some $x \in (RG)^\times$.*

Proof: Immediate. □

Theorem 3.2 *Let R be a commutative and connected semi-local ring and S be a Galois extension of R with Galois group G. Assume that either 2 or the order of G is a unity in R. If the order of G is odd then S has a self-dual normal basis over R.*

Proof: Since R is semi-local, there exists an element $\alpha \in S$ which generates a normal basis over R ([5], Theorem 4.2). So it is enough to prove the existence of an element $x \in (RG)^\times$ such that $w = H_t(\alpha, \alpha) = x\overline{x}$.

It follows from the definition that the Galois extension $S \otimes_R S$ of S, with Galois group G acting on the second component, has a self-dual normal basis over S, so the hermitian spaces (S, H_t) and (RG, l) become isomorphic over S.

Publicado pelo ICMC-USP
Sob a supervisão da CPq/ICMC

¿From now on we will divide the proof in two parts. Firstly we will assume that S is connected.

If $2 \in R^\times$ it is immediate that (S, H_t) and (RG, l) are even. In fact it suffices to take $\frac{1}{2}H_t$ (resp. $\frac{1}{2}l$) as the corresponding sesquilinear form. Note that RG is a semi-local ring by ([14], Proposition 20.6). Thus (S, H_t) and (RG, l) are isomorphic by Proposition 2.2.3 and the required follows by Lemma 3.1.

Suppose now that $|G| \in R^\times$. In this case we observe that the element $e = \frac{1}{|G|}\sum_{\sigma\in G}\sigma$ is a primitive central idempotent of RG and we have the following decomposition $RG = RGe \oplus RGe'$ with $e' = 1 - e$. It is immediate that $RGe \simeq R$ and $A = RGe'$ is an R-algebra with an R-linear involution given by $^-|_A$. Also, A is finitely generated as R-module, so A is semi-local ([14], Proposition 20.6). Since, as observed above, the hermitian spaces (S, H_t) and (RG, l) become isomorphic over S, there exists $y \in (SG)^\times$ such that $y\overline{y} = w$. Thus we have

$$we = (ye)\overline{(ye)} = (ye)^2 \qquad \text{and} \qquad we' = (ye')\overline{(ye')}.$$

The first relation implies the existence of an element $y_1 \in R^\times$ such that $(y_1e)^2 = (ye)^2$. In fact, note that $ye \in SGe \simeq S$, so putting $y = \sum_{\sigma\in G} y_\sigma\sigma$ in SG (resp. $w = \sum_{\sigma\in G} w_\sigma\sigma$ in RG) then we have $y_0 = \sum_{\sigma\in G} y_\sigma \in S^\times$, $w_0 = \sum_{\sigma\in G} w_\sigma \in R^\times$ and $y_0^2 = w_0$. Now, if $|G| = 2k + 1$, with $k \geq 0$, then the element $y_1 = y_0^{-2k}\prod_{\sigma\in G}\sigma(y_0)$ is in $R^\times$ and $y_1^2 = w_0^{-2k}\prod_{\sigma\in G}\sigma(w_0) = w_0^{-2k}w_0^{2k+1} = w_0$.
The second above relation implies that the hermitian spaces (A, le') and (A, h) become isomorphic over S, where $h : (a, b) \mapsto a(we')\overline{b}$ for all $a, b \in A$. On the other hand, since the order of G is odd it follows that every $1 \neq \sigma \in G$ is not conjugate to its inverse. That allow us to assure that there exists a subset U of G such that $U \cap U^{-1} = \phi$ and $G \setminus \{1\} = U \cup U^{-1}$. By taking $s = 1 + \sum_{\sigma\in U}\sigma$ one can easily see that the hermitian spaces (A, le') and (A, h) are even with the corresponding sesquilinear forms given by sle' and sh respectively. By Proposition 2.2.3 (A, le') and (A, h) are isomorphic, so there exists $z \in A^\times$ such that $we' = z\overline{z}$. Putting $x = y_1e + z \in (RG)^\times$ we have $x\overline{x} = (y_1e + z)\overline{(y_1e + z)} = (y_1e)\overline{(y_1e)} + z\overline{z} = we + we' = w$, hence the required again follows.

In this second part of the proof, we will consider the general case. We recall that in this case, by Lemma 2.3.1, there exists a primitive idempotent $v \in S$ such that $S = \bigoplus_{1\leq i\leq n} S_i$, where $S_i = Sv_i, v_i = \sigma_i(v)$ and $\{\sigma_1 = 1, \sigma_2, \ldots, \sigma_n\} \subseteq G$ is a transversal of $G_1 = \{\tau \in G \,|\, \tau(v) = v\}$ in G. Each S_i is a connected Galois extension of $R_i = Rv_i \simeq R$ with group $G_i = \sigma_i G_1 \sigma_i^{-1}$.

Now, denote by $\varphi_i : S_i \times S_i \to R_i$ the bilinear form associated to the trace form $t_i = \sum_{\tau\in G_i}\tau$, for each $1 \leq i \leq n$.

Since the order of G is odd it follows that the order of G_1 is also odd. Furthermore, R_1 is semi-local, so S_1 has a normal basis over R_1. Clearly, we have either $2v \in R_1^\times$ or $|G_1| \in R^\times$, for each $1 \leq i \leq n$. So it follows, by the first part of the proof, that there exists an element $\alpha \in S_1$ which generates a self-dual normal basis of S_1 over R_1 with respect to φ_1. It is easy to verify that $\alpha_i = \sigma_i(\alpha) \in S_i$ generates a self-dual normal basis of S_i over

R_i with respect to φ_i, for every $1 \leq i \leq n$, as well as α generates a self-dual normal basis of S over R with respect to φ_t. □

Corollary 3.3 *Every Galois extension of odd degree of a commutative local ring has a self-dual normal basis.*

Proof: Immediate. □

Corollary 3.4 *Every Galois extension of odd degree of a commutative zero-dimensional ring has a self-dual normal basis.*

Proof: Let R be a commutative zero-dimensional ring and S be a Galois extension of R with group G of odd order. By ([20], Theorem 3.2) there exists an element $\alpha \in S$ which generates a normal basis of S over R. Then, as in the proof of theorem 3.1, it is enough to find un element $x \in RG^{\times}$ such that $w = \varphi_t(\alpha, \alpha) = x\overline{x}$.

It follows from Corollary 3.3 that for any maximal ideal $\mathfrak{m}$ of R there exist elements $b_\sigma \in R$ and $c, c_\sigma \in R \setminus \mathfrak{m}$, with $\sigma \in G$, such that

$$c((\sum_{\sigma\in G}(\prod_{\tau\neq\sigma} c_\tau)b_\sigma\sigma)(\sum_{\sigma\in G}(\prod_{\tau\neq\sigma} c_\tau)b_\sigma\sigma^{-1}) - (\prod_{\sigma\in G} c_\sigma)^2 w) = 0$$

Now, proceeding as in the proof of Proposition 2 of [9] we obtain elements $b'_\sigma \in R$ and $c', c'_\sigma \in R^{\times}$, for all $\sigma \in G$, such that

$$c'((\sum_{\sigma\in G}(\prod_{\tau\neq\sigma} c'_\tau)b'_\sigma\sigma)(\sum_{\sigma\in G}(\prod_{\tau\neq\sigma} c'_\tau)b'_\sigma\sigma^{-1}) - (\prod_{\sigma\in G} c'_\sigma)^2 w) = 0.$$

Consequently there exists $x = \sum_{\sigma\in G} x_\sigma\sigma \in (RG)^{\times}$, with $x_\sigma = \frac{b'_\sigma}{c'_\sigma}$ for all $\sigma \in G$, such that $x\overline{x} = w$. The proof is complete. □

Acknowledgements

This paper was partially supported by CNPq and CAPES (Brazil).

REFERENCES

1. R. Baeza, *Quadratic forms over semilocal rings*, LNM 655, Springer Verlag, 1970.
2. H. Bass, *Unitary algebraic K-theory*, LNM 343, Springer Verlag (1973), 57-265.
3. E. Bayer-Fluckiger, *Self-dual normal bases*, Indag. Math. 51 (1989), 379-383.
4. 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.
5. S. U. Chase, D. K. Harrison and A. Rosenberg, *Galois theory and Galois cohomology of commutative rings*, Mem. Amer. Math. Soc. 52 (1968), 1-19.

Publicado pelo ICMC-USP
Sob a supervisão da CPq/ICMC

6. P. Conner and R. Perlis, *A survey of trace forms of algebraic number fields*, World Scientific, Singapore, 1984.
7. F. DeMeyer and E. Ingraham, *Separable algebras over commutative rings*, LNM 181, Springer Verlag, 1971.
8. M. Ferrero and A. Paques, *Galois theory of commutative rings revisited*, Beiträge Algebra Geom. 38 (1997), 399-410.
9. K. R. Goodearl and R. B. Warfield, Jr., *Algebras over zero-dimensional rings*, Math. Ann. 223 (1976), 157-168.
10. G. Janusz, *Separable algebras over commutative rings*, Trans. AMS 122 (1966),461-479.
11. I. Kersten and J. Michaliček, *Kubische Galoiserweiterung mit Normalbasis*, Comm. Algebra 9 (1981), 9, 1863-1871.
12. I. Kikumasa, T. Nagahara and K. Kishimoto, *On primitive elements of Galois extensions of commutative rings*, Math. J. Okayama Univ. 31 (1989), 31-55
13. M.-A. Knus, *Quadratic and Hermitian forms over rings*, GMW 294, Springer Verlag, 1991.
14. T. Y. Lam, *A first course in non-commutative rings*, GTM 131, Spring Verlag, 1991.
15. R. Lidl and H. Niederreiter, *Introduction to finite fields and their applications*, Cambridge University Press, 1986.
16. A. Magid, *The separable Galois theory of commutative rings*, Marcel Dekker, 1974.
17. M. Mazur, *Remarks on normal bases*, Colloq. Math. 87 (2001), 79–84.
18. T. McKenzie, *Separable polynomials and weak henzelizations*, Lect. Notes in Pure and Appl. Math. 159 (1994), 165-179.
19. T. McKenzie, *The separable closure of a local ring*, J. Algebra 207 (1998), 657-663.
20. A. Paques, *On the primitive and normal basis theorems*, Comm. in Algebra 16 (1988), 443-455.
21. W. Scharlau, *Zur Pfisterschen theorie der quadratischen formen*, Invent. Math. 6 (1969), 327-328.
22. O. E. Villamayor and D. Zelinsky, *Galois theory with finitely many idempotents*, Nagoya Math. J. 27 (1966), 721-731.
23. E. Weis, *Algebraic Number Theory*, McGraw-Hill, New York, 1963.

Publicado pelo ICMC-USP
Sob a supervisão CPq/ICMC