East-West J. of Mathematics: Vol. 8, No 1 (2006) pp.83-95

ON SCALED TRACE FORMS OVER COMMUTATIVE RINGS

Rosali Brusamarello*, Ires Dias† and Antonio Paques‡

* *DMA-UEM 87020-900, Maringá, PR, Brazil*
E-mail: brusama@uem.br

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

‡ *Instituto de Matemática*
Universidade Federal do Rio Grande do Sul
91509-900, Porto Alegre, RS, Brazil
E-mail: paques@mat.ufrgs.br

Abstract

We deal with bilinear forms over commutative rings which are of the type scaled trace form.

Introduction

We are interested in the following two statements:

Every bilinear space of constant rank over a commutative ring is isomorphic to a scaled trace space.

Every bilinear space of even constant rank over a commutative ring is isomorphic to a hermitian scaled trace space.

As it is well known, both the cases have been considered in the literature in the setting of hilbertian fields of characteristic different from 2. The bilinear case was independently considered by Scharlau [11] and Waterhouse [14] and the hermitian case by Berhuy [1].

In this paper we show that their underlying ideas work in a more general context and we prove that the above two statements hold for rings with many units whose residue fields are infinite of characteristic different from 2.

This paper was partially supported by CNPq and CAPES (Brazil)
Key words:
2000 AMS Mathematics Subject Classification:

Following [9] a *ring with many units* is a commutative ring R which satisfies the following local-global principle: for any polynomial $f(X_1, \ldots, X_n) \in R[X_1, \ldots, X_n]$, whenever $f(X_1, \ldots, X_n)$ represents a unit over $R_{\mathfrak{p}}$, for every maximal ideal $\mathfrak{p}$ of R, then $f(X_1, \ldots, X_n)$ represents a unit over R. Such a ring is also called in the literature a *local-global ring* (see [5]). Such kind of rings includes fields and commutative rings which are semi-local, zero-dimensional or, more generally, commutative rings which are von Neumann regular modulo their Jacobson radical.

We refer to [5] for basic facts on bilinear spaces over rings with many units and to [3] and [4] for basic facts on separable algebras and Galois theory of commutative rings.

1. The bilinear case

Throughout this paper R will denote a commutative ring with identity.

By a bilinear space over R we mean a pair (E, φ), where E is a finitely generated projective R-module and $\varphi : E \times E \to R$ is a nonsingular symmetric bilinear form over E.

Let $S \supseteq R$ be a commutative ring extension. We say that S is a strongly separable extension of R if S is separable as R-algebra and finitely generated projective as R-module. As it is well known, the trace map $\mathrm{tr}_{S/R}$ of a strongly separable extension S of R induces a nonsingular symmetric bilinear form over R. A bilinear space is called a *scaled trace space* if it is of the type (S, t_λ), where S is a strongly separable extension of R, λ is a unit of S and $t_\lambda(s, s') = \mathrm{tr}_{S/R}(\langle\lambda\rangle)(s, s') = \mathrm{tr}_{S/R}(\lambda s s')$, for all $s, s' \in S$.

Our purpose in this section is to prove the following theorem.

Theorem 1.1 *Let R be a ring with many units whose residue fields are infinite of characteristic different from 2. Then every bilinear space of constant rank over R is isomorphic to a scaled trace space.*

For this we need some preparation. We start by observing that, in the case that R is under the assumptions of Theorem 1.1, every strongly separable extensions S of R of constant rank has a *primitive element*, i.e, S is of the type $\frac{R[X]}{(f(X))}$, for some separable polynomial $f(X) \in R[X]$ [10, Theorem 2.4].

An ideal I of $R[X]$ is said to be a *separable ideal* if the R-algebra $\frac{R[X]}{I}$ is separable. A polynomial $f(X) \in R[X]$ is said to be a *separable polynomial* if $f(X)$ is monic and $(f(X))$ is a separable ideal.

Given an R-module E and $\nu \in \mathrm{End}_R(E)$, we say that ν is a *separable endomorphism* if $I(\nu) = \{f(X) \in R[X] \mid f(\nu) = 0\}$, the ideal of the relations satisfied by ν, is separable.

In the following lemma we will see that if ν is separable and E is free over

R, then $I(\nu)$ is in fact the characteristic ideal of ν.

Lemma 1.2 *Let E be a finitely generated R-module and $\nu \in \mathrm{End}_R(E)$.*
(i) *There exists $f(X) \in R[X]$ monic such that $I(\nu) = (f(X))$.*
(ii) *If ν is separable and E is projective of rank $deg(f(X))$ over R, then E is a projective $\frac{R[X]}{I(\nu)}$-module of rank one.*
(iii) *If ν is separable and E is a free R-module then $f(X)$ is the characteristic polynomial of ν over R.*

Proof (i) From Cayley-Hamilton Theorem [8, Theorem IV.17] $I(\nu)$ contains a monic polynomial. By the division algorithm it follows easily that $I(\nu)$ is generated by the monic polynomial of smallest degree in $I(\nu)$.

(ii) Take $S = \frac{R[X]}{I(\nu)}$. Clearly E is an S-module via the action $\overline{g(X)}.v = g(\nu)(v)$ for all $\overline{g(X)} = g(X)+I(\nu) \in S$ and $v \in E$. Since ν is separable, S is a separable R-algebra and then E is also a projective S-module by [6, Lemma 1.2]. Now, by comparing ranks the assertion follows.

(iii) Let $h(X)$ be the characteristic polynomial of ν over R. Note that for any maximal ideal $\mathfrak{p}$ of R, $\nu \otimes \frac{R}{\mathfrak{p}}$ is separable and $f(X)$ and $h(X)$ have the same irreducible factors modulo $\mathfrak{p}[X]$. Thus $f(X) = h(X) \pmod{\mathfrak{p}[X]}$. Now, since $f(X)$ divides $h(X)$ and both are monic, it easily follows that $f(X) = h(X)$. □

Corollary 1.3 *Let E and ν be as above. Assume that E is R-projective of constant rank and ν is separable. If R is a ring with many units, then $I(\nu)$ is generated by the characteristic polynomial of ν over R and E is a rank one free $\frac{R[X]}{I(\nu)}$-module.*

Proof The first assertion is ensured by [5, Theorem 2.10] and Lemma 1.2(iii). The second one follows from Lemma 1.2(ii), observing that $\frac{R[X]}{I(\nu)}$ is also a ring with many units [5, Corollary 2.3]. □

Lemma 1.4 *Let (E, φ) be a bilinear space over R. Assume that every strongly separable extension of R of constant rank has a primitive element. Then (E, φ) is isomorphic to a scaled trace space if and only if there exists $\nu \in \mathrm{End}_R(E)$ such that:*
(i) *ν is separable over R;*
(ii) *ν is self-adjoint with respect to φ;*
(iii) *E is a rank one free $\frac{R[X]}{I(\nu)}$-module.*

Proof By assumption there exist a separable polynomial $f(X) \in R[X]$ and a unit λ in $S = \frac{R[X]}{(f(X))} = R[\alpha]$, with $\alpha = X + (f(X))$, such that $\varphi \simeq \mathrm{tr}_{S/R}(\langle\lambda\rangle)$. Hence, there is an R-module isomorphism $\theta : S \to E$ such that $\varphi(\theta(s), \theta(s')) = \mathrm{tr}_{S/R}(\langle\lambda\rangle)(s, s') = \mathrm{tr}_{S/R}(\lambda s s')$, for all $s, s' \in S$.

Define $\psi : S \to S$ by $\psi(s) = \alpha s$ for all $s \in S$ and $\nu : E \to E$ by $\nu(v) =$

$\theta\psi\theta^{-1}(v)$ for all $v \in E$. It is easy to check that $\nu \in \mathrm{End}_R(E)$. We shall prove that ν satisfies (i),(ii) and (iii).

Since $I(\nu) = I(\theta\psi\theta^{-1}) = I(\psi) = (f(X))$ and $f(X)$ is separable, ν satisfies (i). Furthermore, for all $u, v \in E$ we have

$$\begin{aligned}\varphi(\nu(u), v) &= \varphi(\theta\psi\theta^{-1}(u), \theta\theta^{-1}(v)) = \mathrm{tr}_{S/R}(\lambda\psi\theta^{-1}(u)\theta^{-1}(v)) \\ &= \mathrm{tr}_{S/R}(\lambda\alpha\theta^{-1}(u)\theta^{-1}(v)) = \mathrm{tr}_{S/R}(\lambda\theta^{-1}(u)\alpha\theta^{-1}(v)) \\ &= \varphi(\theta\theta^{-1}(u), \theta\psi\theta^{-1}(v)) = \varphi(u, \nu(v)),\end{aligned}$$

which implies (ii).

For (iii), it is enough to show that $\theta : S \to E$ is S-linear. This is obtained from the action of S on E and the definition of ν, as follows: $\alpha(\theta(s)) = \nu(\theta(s)) = \theta\psi\theta^{-1}(\theta(s)) = \theta(\alpha s)$, for all $s \in S$.

Conversely, from (i) we have that $S = \frac{R[X]}{I(\nu)}$ is a separable R-algebra and from (iii) E is a free S-module of rank one. So $E = Su_o$ for some $u_o \in E$ free over S. From Lemma 1.2(i), $I(\nu) = (f(X))$ for some monic polynomial $f(X) \in R[X]$. So, E is a free R-module and by Lemma 1.2(iii) $f(X)$ is the characteristic polynomial of ν.

We need to ensure the existence of a unit $\lambda \in S$ such that $\varphi(su_o, s'u_o) = \mathrm{tr}_{S/R}(\lambda ss')$ for all $s, s' \in S$. On the other hand, the units of S are in one-to-one correspondence with the nonsingular symmetric S-bilinear forms $b : E \times E \to S$. Hence we have to determine a nonsingular symmetric S-bilinear form $b : E \times E \to S$ such that $\varphi(u, v) = \mathrm{tr}_{S/R}(b(u, v))$ for all $u, v \in E$.

In order to obtain b we observe that every pair $(u, v) \in E \times E$ determines a unique element $f_{(u,v)} \in \mathrm{Hom}_R(S, R)$ such that $f_{(u,v)}(s) = \varphi(su, v)$ for all $s \in S$. On the other hand, by the separability of S over R there exists a unique $\lambda_{(u,v)} \in S$ such that $\mathrm{tr}_{S/R}(\lambda_{(u,v)}s) = f_{(u,v)}(s)$ for all $s \in S$. Define $b : E \times E \to S$ by $b(u, v) = \lambda_{(u,v)}$. Since $\mathrm{tr}_{S/R}$ is nonsingular and ν is self-adjoint, it easily follows that b is symmetric and S-bilinear.

It remains to show that b is nonsingular and it is enough to check that $\lambda = b(u_o, u_o)$ is a unit of S. Suppose that $\lambda \in \mathfrak{q}$, for some maximal ideal $\mathfrak{q}$ of S. ¿From the separability of S over R it follows that $\frac{S}{\mathfrak{p}S}$ is a finite direct sum of finite separable field extensions of $\frac{R}{\mathfrak{p}}$, where $\mathfrak{p} = \mathfrak{q} \cap R$. So $\lambda \in \mathfrak{q}$ implies that there exists $s \in S \setminus \mathfrak{q}$ such that $s\lambda = 0 \pmod{\mathfrak{p}S}$ and consequently $\varphi(su_o, su_o) = \mathrm{tr}_{S/R}(b(su_o, su_o)) = \mathrm{tr}_{S/R}(s^2\lambda) = 0 \pmod{\mathfrak{p}}$. Since φ is nonsingular, $su_o = 0 \pmod{\mathfrak{p}E}$, which is a contradiction. The proof is complete. □

We say that a bilinear space (E, φ) is *proper* if the ideal of R generated by $\varphi(v, v)$, $v \in E$, is equal to R.

Proposition 1.5 *Let (E, φ) a bilinear space of rank n over R. Assume that R is a ring with many units and $|\frac{R}{\mathfrak{p}}| > n$, for every maximal ideal $\mathfrak{p}$ of R. If (E, φ) is proper then (E, φ) is isomorphic to a scaled trace space.*

Proof We start pointing out that R is under the assumptions of Lemma 1.4 [10, Theorem 2.4]. So, it is enough to find $\nu \in \mathrm{End}_R(E)$ satisfying the conditions (i)-(iii) of this lemma.

By [5, Theorem 7.3(ii)] there exist units $d_1, \ldots, d_n \in R$ such that $\varphi = \langle d_1, \ldots, d_n \rangle$ with respect to some orthogonal basis B of E over R. Consider the polynomial in the variables $X_{ij} = X_{ji}$, $1 \leq i, j \leq n$,

$$f(X_{ij}, X) = \det(D^{-1}X - (X_{ij})) \in K[X_{ij}][X]$$

where $D = \mathrm{diag}(d_1, \ldots, d_n)$. Denote by $g(X_{ij}) \in R[X_{ij}]$ the discriminant of $f(X_{ij}, X)$. We claim that there exists a symmetric matrix $(\lambda_{ij}) \in M_n(R)$ such that $g(\lambda_{ij})$ is a unit in R. Since R is a ring with many units, it is enough to show that this is true modulo each maximal ideal $\mathfrak{p}$ of R.

Putting $X_{ij} = 0$ for all $i \neq j$ we have $f(X_{ii}, X) = \prod_{i=1}^{n}(d_i^{-1}X - X_{ii})$, whose discriminant is $g(X_{ii}) = \prod_{i \neq j}(d_i X_{ii} - d_j X_{jj})$. Since $|\frac{R}{\mathfrak{p}}| > n$ we can find $\lambda_1, \ldots, \lambda_n \in R$ such that $g(\lambda_1, \ldots, \lambda_n) \neq 0 \pmod{\mathfrak{p}}$, for each maximal ideal $\mathfrak{p}$ of R. Thus, there exists $A = (\lambda_{ij}) \in M_n(R)$ symmetric and such that $f(\lambda_{ij}, X)$ is separable over R.

Now, consider $\nu \in \mathrm{End}_R(E)$ given by the matrix $A' = AD$ with respect to the orthogonal basis B. By construction, ν is separable. Indeed, by Lemma 1.2 the ideal $I(\nu)$ is generated by the polynomial $\det(XI_n - A') = (\det D) f(\lambda_{ij}, X) \in R[X]$.

From $(A'u)^t Dv = u^t D^t A^t Dv = u^t D(A'v)$, for all $u, v \in E$, it follows that ν is self-adjoint with respect to φ. Finally, it follows from Corollary 1.3 that ν also satisfies the condition (iii) of Lemma 1.4. □

Proof of Theorem 1.1. Since 2 is a unit in R, every bilinear space over R is proper and the result follows from Proposition 1.5. □

Corollary 1.6 *If R is a ring with many units, whose residue fields are infinite, then every bilinear space over R is Witt-equivalent to a scaled trace space.*

Proof It follows from the fact that, under the assumptions, every element in the Witt ring of R is represented by a proper bilinear space. □

2. The hermitian case

Recall that also in this section R denotes a commutative ring with identity. By a *hermitian scaled trace space* over R we mean a bilinear space $(S, t_{(\tau,\lambda)})$, where S is a strongly separable extension of R, τ is an R-linear involution on S, λ is a τ-invariant unit of S and $t_{(\tau,\lambda)}(s, s') = \mathrm{tr}_{S/R}(\lambda s \tau(s'))$, for all $s, s' \in S$. We observe, in particular, that if S has constant rank over R and, for instance, R is a ring with many units whose residue fields are infinite of characteristic different from 2, then the existence of the involution τ implies that $rank_R S$ is even.

Our purpose in this section is to prove the following theorem.

Theorem 2.1 *Let R be a ring with many units whose residue fields are infinite of characteristic different from 2. Then every bilinear space of even constant rank over R is isomorphic to a hermitian scaled trace space.*

As in Section 1, before proving this theorem we also need some preparation. We start with the following lemma which is crucial for the sequel. It generalizes and extends to the setting of commutative rings an old and well known result due to O.Taussky [12].

We say that a vector column $v = (a_1 \dots a_n)^t$ in $R^{(n)}$ is *unimodular* if the ideal of R generated by $a_1, \dots, a_n$ is equal to R.

Lemma 2.2 *Let $A \in M_n(R)$, $f(X) = det(A - XI_n) \in R[X]$ and $S = \frac{R[X]}{(f(X))} = R[\alpha]$, with $\alpha = X + (f(X))$. Let $v_\alpha = (v_1 \dots v_n)^t \in S^{(n)}$ be such that $Av_\alpha = \alpha v_\alpha$. Assume that $f(X)$ is separable over R and that v_α is unimodular. Then $\{v_1, \dots, v_n\}$ is a basis of S over R. Furthermore, there exists $v'_\alpha = (v'_1 \dots v'_n)^t \in S^{(n)}$ such that v'_α is unimodular, $A^t v'_\alpha = \alpha v'_\alpha$ and $\{v'_1, \dots, v'_n\}$ is the dual basis of $\{v_1, \dots, v_n\}$ with respect to $\mathrm{tr}_{S/R}$.*

Proof Observe that S is a separable R-algebra and a free R-module with $rank_R S = n$. Then there exists a Galois extension T of R, with group G, and a subgroup H of G such that $S = T^H := \{t \in T \mid h(t) = t, \text{ for all } h \in H\}$ (see [13], Section 3). Note that $[G : H] = rank_R S = n$. Let $\{\sigma_1 = 1, \sigma_2, \dots, \sigma_n\} \subseteq G$ be a left transversal of H in G and consider $M = (\sigma_j(v_i))_{1 \le i,j \le n} \in M_n(T)$.

From now on we will proceed by steps.

Claim 1: *M is invertible in $M_n(T)$.*

Let $d = \det(M) \in T$ denote the determinant of M. It is enough to verify that d is a unit modulo $\mathfrak{p}T$ for every maximal ideal $\mathfrak{p}$ of R. Indeed, by localization we can suppose that R is local with maximal ideal $\mathfrak{p}$ and then, in this case, $\mathfrak{p}T$ is the Jacobson radical of T [6, Lemma 1.1].

Considering that $\frac{T}{\mathfrak{p}T} = \frac{R}{\mathfrak{p}} \otimes_R T$ is a Galois extension of $\frac{R}{\mathfrak{p}}$, with group G acting in the second component, we may also assume that R is a field. By [7, Lemma 1.1] there exist primitive idempotents $e_1, \dots, e_m \in T$ such that $T = \bigoplus_{1 \le k \le m} Te_k$. Then for each k we have:

- Te_k is a field,
- $\sigma_i(\alpha)e_k \neq \sigma_j(\alpha)e_k$ for every $1 \le i, j \le n$, $i \neq j$, by [10, Proposition 2.1],
- $\sigma_i(v_\alpha)e_k \neq 0$ for every $1 \le i \le n$, since v_α is unimodular,
- $\sigma_i(v_\alpha)e_k = (\sigma_i(v_1)e_k \dots \sigma_i(v_n)e_k)^t$ is an eigenvector of Ae_k corresponding to $\sigma_i(\alpha)e_k$, for every $1 \le i \le n$,
- $\{\sigma_i(v_\alpha)e_k \mid 1 \le i \le n\}$ is a basis of $(Te_k)^{(n)}$ over Te_k.

Hence Me_k is invertible in $M_n(Te_k)$. Now taking $d_k = \det(Me_k)$ and $c_k = d_k^{-1} \in Te_k$ we obtain $d = \sum_{k=1}^m d_k$ and $d(\sum_{k=1}^m c_k) = \sum_{k=1}^m d_k c_k = \sum_{k=1}^m e_k = 1$.

Claim 2: *There exist* $v'_1, \ldots, v'_n \in S$ *such that* $M^{-1} = (\sigma_i(v'_j))_{1 \leq i,j \leq n}$.

It is straightforward that $M^{-1} = (\sigma_i(v'_j))_{1 \leq i,j \leq n}$ with $v'_1, \ldots, v'_n \in T$. So it remains to verify that $v'_i \in S$, for every $1 \leq i \leq n$. Since $S = T^H$ it is enough to check that $h(v'_i) = v'_i$, for all $h \in H$. It follows from $G = \bigcup_{i=1}^n \sigma_i H$ that for each $h \in H$ and $1 \leq i \leq n$ there exist $h_i \in H$ and $1 \leq i(h) \leq n$ such that $h\sigma_i = \sigma_{i(h)} h_i$. Then we have $h(M)h(M^{-1}) = I_n$, where $h(M) = (\sigma_{j(h)}(v_i))_{1 \leq i,j \leq n}$ and $h(M^{-1}) = (\sigma_{i(h)} h_i(v'_j))_{1 \leq i,j \leq n}$. Consequently $h(M^{-1}) = h(M)^{-1}$. On the other hand, it is also straightforward that $h(M)^{-1} = (\sigma_{i(h)}(v'_j))_{1 \leq i,j \leq n}$. Note in particular that the first row of $h(M^{-1})$ (resp. $h(M)^{-1}$) is $(h(v'_1), \ldots, h(v'_n))$ (resp. $(v'_1, \ldots, v'_n)$). So the required follows.

Claim 3: $\{v_1, \ldots, v_n\}$ *is a basis of* S *over* R.

If $\sum_{i=1}^n a_i v_i = 0$, with $a_i \in R$ then $M(a_1 \ldots a_n)^t = 0$ and since M is invertible we have $a_i = 0$, $1 \leq i \leq n$. For any $v \in S$, let $(y_1 \ldots y_n) = (\sigma_1(v) \ldots \sigma_n(v))M^{-1}$. Then $y_i = \sum_{j=1}^n \sigma_j(vv'_i) = \mathrm{tr}_{S/R}(vv'_i) \in R$, $1 \leq i \leq n$, and from $(\sigma_1(v) \ldots \sigma_n(v)) = (y_1 \ldots y_n)M$ we have $v = \sigma_1(v) = \sum_{i=1}^n y_i v_i$.

Claim 4: $\{v'_1, \ldots, v'_n\}$ *is the dual basis of* $\{v_1, \ldots, v_n\}$ *with respect to* $\mathrm{tr}_{S/R}$, $v'_\alpha = (v'_1 \ldots v'_n)^t$ *is unimodular and* $A^t v'_\alpha = \alpha v'_\alpha$.

By the same arguments used in Claim 3 we see that $\{v'_1, \ldots, v'_n\}$ is a basis of $S^{(n)}$. From Claim 2 it follows easily that it is the dual of $\{v_1, \ldots, v_n\}$ with respect to $\mathrm{tr}_{S/R}$ as well as v'_α is unimodular. Thus, it remains to verify that $A^t v'_\alpha = \alpha v'_\alpha$. Since M is invertible it follows that $C_\alpha = \{\sigma_j(v_\alpha) \mid 1 \leq j \leq n\}$ and $C'_\alpha == \{\sigma_i(v'_\alpha) \mid 1 \leq i \leq n\}$ are basis of $T^{(n)}$ over T. If we denote by C the canonical basis of $T^{(n)}$ over T, then M (resp. $(M^{-1})^t$) is the matrix of the identity map on $T^{(n)}$ with respect to C_α (resp. C'_α) and C. Finally denoting by $[T_A]_{C_\alpha}$ (resp. $[T_{A^t}]_{C'_\alpha}$) the matrix of the T-linear map defined by A (resp. A^t) on $T^{(n)}$, with respect to C_α (resp. C'_α), we have

$$\begin{aligned} \mathrm{diag}(\sigma_1(\alpha), \ldots, \sigma_n(\alpha)) &= (\mathrm{diag}(\sigma_1(\alpha), \ldots, \sigma_n(\alpha)))^t = [T_A]^t_{C_\alpha} \\ &= (M^{-1}AM)^t = M^t A^t (M^{-1})^t = [T_{A^t}]_{C'_\alpha}. \end{aligned}$$

This completes the Proof □

For the next proposition we will consider matrices of the type

$$B_{2n}(t_4, t_6, \ldots, t_{2n}) = \begin{pmatrix} 0 & t_{2n} & & & & & & & \\ t_{2n} & 0 & 1 & & & & & & \\ & 1 & 0 & t_{2n-2} & & & & & \\ & & t_{2n-2} & 0 & 1 & & & & \\ & & & 1 & 0 & \ddots & & & \\ & & & & \ddots & \ddots & t_4 & & \\ & & & & & t_4 & 0 & 1 & \\ & & & & & & 1 & 0 & 1 \\ & & & & & & & 1 & 0 \end{pmatrix}$$

These matrices are due to G. Berhuy and have been appeared in the literature in [2].

Proposition 2.3 *Let $B, D \in M_{2n}(R)$ be such that $B = B_{2n}(t_4, \ldots, t_{2n})$ and $D = \mathrm{diag}(s_{2n}, \ldots, s_1)$, with s_i, t_j units in R. Assume that $f(X) = \det(DB - XI_{2n}) \in R[X]$ is separable and let $S = \frac{R[X]}{(f(X))} = R[\alpha]$, with $\alpha = X + (f(X))$. Then there exist a unit $\lambda \in R[\alpha^2]$ and a basis $\{v_1, \ldots, v_{2n}\}$ of S over R such that $D = (\mathrm{tr}_{S/R}(\lambda v_i v_j))_{1 \leq i,j \leq 2n}$.*

Proof Let $A = DB$ and $v_{ij} = (-1)^{i+j}\Delta_{ij}(A - \alpha I_{2n})$ where $\Delta_{ij}(A - \alpha I_{2n})$ denotes the determinant of the matrix obtained by cancellation of the i^{th}-row and the j^{th}-column of $A - \alpha I_{2n}$. It follows from $(A - \alpha I_{2n})(v_{ij})^t = \det(A - \alpha I_{2n})I_{2n} = 0$ that $A(v_{i1} \ldots v_{i2n})^t = \alpha(v_{i1} \ldots v_{i2n})^t$. Set $v_j = v_{1j}$ and $v_\alpha = (v_1 \ldots v_{2n})^t$. It is easy to verify that $v_{2n} = -s_1 \ldots s_{2n-1}t_4 \ldots t_{2n}$. So v_{2n} is a unit of R and v_α is unimodular. By Lemma 2.2 $\{v_1, \ldots, v_{2n}\}$ is a basis of S over R and there exists a unimodular element $v'_\alpha = (v'_1 \ldots v'_{2n})^t \in S^{(2n)}$ such that $\{v'_1, \ldots, v'_{2n}\}$ is its dual basis and $A^t v'_\alpha = \alpha v'_\alpha$.

Furthermore, $Sv_\alpha = V_\alpha := \{v \in S^{(2n)} \mid Av = \alpha v\}$. In fact, it is enough to verify this locally, so assume that R is local with maximal ideal $\mathfrak{p}$. Clearly $Sv_\alpha \subset V_\alpha$. Take $v \in V_\alpha$ and consider the S-module $W_v = Sv_\alpha + Sv$. Since v_α is unimodular and $f(X)$ is separable we have $W_v = Sv_\alpha \pmod{W_v}$ or $W_v = Sv_\alpha + \mathfrak{p}W_v$. By Nakayama's Lemma $W_v = Sv_\alpha$ and the assertion follows.

It follows from $\alpha v'_\alpha = A^t v'_\alpha = D^{-1}ADv'_\alpha$ that $Dv'_\alpha \in V_\alpha = Sv_\alpha$. Thus there exists a unit $\lambda \in S$ such that $Dv'_\alpha = \lambda v_\alpha$ and consequently $\lambda v_j = s_{2n-j+1}v'_j$, for all $1 \leq j \leq 2n$. Hence $\mathrm{tr}_{S/R}(\lambda v_i v_j) = \mathrm{tr}_{S/R}(s_{2n-j+1}v_i v'_j) = \delta_{ij}s_{2n-j+1}$, that is, $D = (\mathrm{tr}_{S/R}(\lambda v_i v_j))_{1 \leq i,j \leq 2n}$.

In order to prove that $\lambda \in R[\alpha^2]$ we will proceed again by localization. Set $\Lambda = R[\alpha^2] + R\lambda$ and assume that R is local with maximal ideal $\mathfrak{p}$. By Nakayama's Lemma it is enough to prove that $\Lambda = R[\alpha^2] \pmod{\mathfrak{p}\Lambda}$. So, for the rest of the proof we will suppose that R is a field. As in the proof of Lemma 2.2, take T a Galois extension of R with group G, H a subgroup of G such that $S = T^H$ and $\{\sigma_1 = 1, \sigma_2, \ldots, \sigma_{2n}\}$ a left transversal of H in G.

It is easy to verify that $f(X) = f(-X)$ (see, for instance, the proof of Proposition 1 of [1]), so the R-linear map $\tau : S \to S$, given by $\tau(\alpha^i) = (-\alpha)^i$, is a well defined involution. Also, $S^{[\tau]} = R[\alpha^2]$.

On the other hand, by [7, Lemma 1.1] there exist primitive idempotents $e_1, \ldots, e_m \in T$ such that $T = \bigoplus_{1 \leq k \leq m} Te_k$. Each Te_k is a field Galois extension of $Re_k \simeq R$ containing Se_k as subfield. Moreover, it follows from [4, Lemma 3.2.7] that for each $1 \leq i \leq 2n$ there exists $1 \leq j \leq 2n$, $j \neq i$ such that $e_k\sigma_i\tau(s) = e_k\sigma_j(s)$, for all $s \in S$. Now, by the same arguments used in the proof of Proposition of [2] we get $\tau(\lambda)e_k = \lambda e_k$, for every $1 \leq k \leq m$. Therefore $\tau(\lambda) = \sum_{k=1}^{m} \tau(\lambda)e_k = \sum_{k=1}^{m} \lambda e_k = \lambda$, which completes the Proof □

Now consider the diagonal matrix $D = \mathrm{diag}(s_{2n}, \ldots, s_1)$, with s_i units of R, and independent variables $T_4, \ldots, T_{2n}, X$ on R. Take the polynomial

$$f(T_4, \ldots, T_{2n}, X) = \det(B_{2n}(T_4, \ldots, T_{2n}) - XD^{-1}) \in R[T_4, \ldots, T_{2n}, X].$$

Set $F_n(X) = f(T_4, \ldots, T_{2n}, X)$ and let $G_n(X) = \frac{\partial F_n(X)}{\partial X}$ be the derivative of $F_n(X)$ with respect to X. We will denote by $d_n(X)$ the discriminant of $F_n(X)$. Clearly $F_n(X) = \det(D)^{-1}X^{2n} +$ (terms of lower degree), so $F_n(X)$ is a nonzero polynomial modulo $\mathfrak{p}R[T_4, \ldots, T_{2n}][X]$, for every maximal ideal $\mathfrak{p}$ of R. It follows from the next lemma that the same statement holds for $G_n(X)$ and $d_n(X)$, provided that 2 is a unit in R.

Lemma 2.4 *Assume that R is a field of characteristic different from 2. Then, $G_n(X)$ and $d_n(X)$ are nonzero polynomials in $R[T_4, \ldots, T_{2n}][X]$.*

Proof We will proceed by induction on n. For $n = 1$ we have

$$G_1(X) = 2s_1^{-1}s_2^{-1}X \neq 0 \qquad \text{and}$$

$$d_1(X) = \mathrm{disc}(F_1(X)) = \det \begin{pmatrix} s_1^{-1}s_2^{-1} & 0 & -1 \\ 2s_1^{-1}s_2^{-1} & 0 & 0 \\ 0 & 2s_1^{-1}s_2^{-1} & 0 \end{pmatrix} = -4s_1^{-2}s_2^{-2} \neq 0.$$

For $n > 1$ assume that $G_{n-1}(X) \neq 0$ and $d_{n-1}(X)) \neq 0$. Note that

$$F_n(X) = U_n(X) - F_{n-1}(X)T_{2n}^2 \quad \text{and} \quad G_n(X) = V_n(X) - G_{n-1}(X)T_{2n}^2$$

where $U_n(X) = -s_{2n}^{-1}XP_n(X)$, $V_n(X) = \frac{\partial U_n(X)}{\partial X}$ and $P_n(X)$ is the determinant of the matrix obtained by cancellation of the first row and the first column of $B_{2n}(T_4, \ldots, T_{2n}) - XD^{-1}$. Since $U_n(X)$ does not depend on T_{2n}, it easily follows that $G_n(X) \neq 0$.

Now suppose that $d_n(X) = 0$. Then, as it is well known, there exist nonzero polynomials $h_n(X), l_n(X) \in R[T_4, \ldots, T_{2n}][X]$ such that

$$h_n(X)G_n(X) + l_n(X)F_n(X) = 0. \qquad (\star)$$

From $(\star)$ it easily follows that $h_n(X)$ and $l_n(X)$ have the same degree as polynomials in the variable T_{2n}. Thus $h_n(X) = \sum_{i=0}^{r} a_i(X)T_{2n}^i$ and $l_n(X) = \sum_{i=0}^{r} b_i(X)T_{2n}^i$ with $a_i(X), b_i(X) \in R[T_4, \ldots, T_{2n-2}, X]$, $1 \leq i \leq r$, $a_r(X) \neq 0$ and $b_r(X) \neq 0$. We will show in the sequel that we can restrict our discussion to the cases $r = 0$ and $r = 1$. Firstly, in order to simplify notation put $F_m = F_m(X)$, $G_m = G_m(X)$, $U_m = U_m(X)$, $V_m = V_m(X)$, $d_m = d_m(X)$, $a_i = a_i(X)$ and $b_i = b_i(X)$, for every $1 \leq m \leq n$ and $1 \leq i \leq r$.

Claim: *For every* $1 \leq k \leq [\frac{r}{2}]$ *there exist polynomials* $f_{2k}(X), f_{2k-2}(X) \in R[T_4 \ldots, T_{2n-2}][X]$*, with degrees equal to* $2k$ *and* $2k-2$ *respectively, such that*

$$a_{r-2k} = f_{2k}(X)F_{n-1} - f_{2k-2}(X)U_n$$

and

$$b_{r-2k} = -(f_{2k}(X)G_{n-1} - f_{2k-2}(X)V_n).$$

In fact, we will proceed again by induction on k. Assume that $k = 1$. So $r \geq 2$ and it follows from $(\star)$ that

$$a_r G_{n-1} + b_r F_{n-1} = 0 \tag{1}$$

$$a_r V_n + b_r U_n - (a_{r-2}G_{n-1} + b_{r-2}F_{n-1}) = 0. \tag{2}$$

Note that $R[T_4, \ldots, T_{2n}, X]$ is a factorial domain. So we can assume that a_r and b_r are relatively prime. Since by assumption $d_{n-1} \neq 0$ then F_{n-1} and G_{n-1} are also relatively prime. Therefore, it follows from (1) that there exists a nonzero constant $f_0 = f_0(X) \in R[T_4, \ldots, T_{2n-2}][X]$ such that $a_r = f_0(X)F_{n-1}$ and $b_r = -f_0(X)G_{n-1}$. Thus we get from (2) that

$$(f_0(X)V_n - b_{r-2})F_{n-1} = (f_0(X)U_n + a_{r-2})G_{n-1}, \tag{3}$$

which implies that F_{n-1} divides $f_0(X)U_n + a_{r-2}$. Observe that $f_0(X)U_n + a_{r-2} \neq 0$ since $\deg(f_0(X)U_n + a_{r-2}) = \deg(U_n) = 2n$. Hence there exists a nonzero polynomial $f_2(X) \in R[T_4, \ldots, T_{2n-2}][X]$ such that $f_0(X)U_n + a_{r-2} = f_2(X)F_{n-1}$. Clearly $\deg(f_2(X)) = 2$ and it follows from (3) that

$$a_{r-2} = f_2(X)F_{n-1} - f_0(X)U_n$$

and

$$b_{r-2} = -(f_2(X)G_{n-1} - f_0(X)V_n).$$

Now assume that $k \geq 2$ and that the claim holds for $l = k - 1$. Replacing a_{r-2l} and b_{r-2l} by their respective formulas in the coefficient of T_{2n}^{r-2l} in $(\star)$, we obtain

$$(f_{2l}(X)V_n - b_{r-2k})F_{n-1} = (f_{2l}(X)U_n + a_{r-2k})G_{n-1}. \tag{4}$$

And using the same arguments as above we obtain from (4) the assertion required.

Finally, if $r = 2k$, replacing a_0 and b_0 by their respective formulas in the coefficient of T_{2n}^0 in $(\star)$ we get

$$\begin{aligned} 0 &= a_0V_n + b_0U_n \\ &= (f_{2k}(X)F_{n-1} - f_{2k-2}(X)U_n)V_n - (f_{2k}(X)G_{n-1} - f_{2k-2}(X)V_n)U_n \\ &= f_{2k}(X)(F_{n-1}V_n - G_{n-1}U_n) \end{aligned}$$

and, consequently $F_{n-1}V_n = G_{n-1}U_n$. Thus F_{n-1} divides U_n and there exists a nonzero polynomial $h(X) \in R[T_4 \ldots, T_{2n-2}][X]$ such that $U_n = h(X)F_{n-1}$, as well as $V_n = h(X)G_{n-1}$. Therefore,

$$h(X)G_{n-1} = V_n = \frac{\partial U_n}{\partial X} = \frac{\partial h(X)}{\partial X}F_{n-1} + h(X)G_{n-1}$$

and so $\frac{\partial h(X)}{\partial X}F_{n-1} = 0$. Since clearly $\deg(h(X)) = 2$, we have a contradiction.

If $r = 2k + 1$ we proceed in a similar way, replacing a_1 and b_1 by their respective formulas in the coefficient of T_{2n} in $(\star)$, in order to get a similar contradiction. The proof is complete. □

Corollary 2.5 *Assume that R is a ring with many units whose residue fields are infinite of characteristic different from 2, and let $s_1, \ldots, s_{2n}$ be units in R. Then there exist units $t_4, t_6, \ldots, t_{2n}$ in R such that the polynomial $f(X) = \det(BD - XI_{2n})$ is separable over R, where $D = \operatorname{diag}(s_{2n}, \ldots, s_1)$ and $B = B_{2n}(t_4, t_6, \ldots, t_{2n})$.*

Proof Consider the polynomial

$$f(T_4, \ldots, T_{2n}, X) = \det(B_{2n}(T_4, \ldots, T_{2n}) - XD^{-1}) \in R[T_4, \ldots, T_{2n}, X].$$

Set $g(T_4, \ldots, T_{2n}) = T_4 \ldots T_{2n}d_n(X) \in R[T_4, \ldots, T_{2n}]$, where $d_n(X)$ denotes the discriminant of $f(T_4, \ldots, T_{2n}, X)$. We have to prove that $g(T_4, \ldots, T_{2n})$ represents a unit over R. Since R is a ring with many units, it is enough to show this in the case that R is a field. Under this assumption, since R is infinite, it remains only to ensure that $g(T_4, \ldots, T_{2n})$ is not zero. The assertion follows now from Lemma 2.4. □

Proof of Theorem 2.1. Let (E, φ) be a bilinear space of rank $2n$ over R. Since 2 is a unit in R, we have that (E, φ) is proper and by [5, Theorem 7.3(ii)] there exist units $s_1, \ldots, s_{2n} \in R$ such that $\varphi = \langle s_{2n}, \ldots, s_1 \rangle$ with respect to some orthogonal basis of E over R. Let $D = \operatorname{diag}(s_{2n}, \ldots, s_1)$. By Corollary 2.5 there exist units $t_4, t_6, \ldots, t_{2n}$ in R such that the polynomial $f(X) = \det(BD - XI_{2n})$ is separable over R, where $B = B_{2n}(t_4, t_6, \ldots, t_{2n})$. Set $S = \frac{R[X]}{(f(X))} = R[\alpha]$, with $\alpha = X + (f(X))$. By Proposition 2.3 there exists a unit $\lambda \in L = R[\alpha^2]$ such that (E, φ) is isomorphic to the scaled trace space (S, t_λ).

Furthermore, there exists a R-linear involution $\tau : S \to S$ such that $\tau(\alpha) = -\alpha$, $R[\alpha^2] = S^{[\tau]}$ and $S = L[\alpha] \simeq \frac{L[X]}{(X^2-\alpha^2)}$ is a strongly separable extension of L. Putting $S' = \frac{L[X]}{(X^2+\alpha^2)}$ we have that S' is also a strongly separable extension of L and

$$\mathrm{tr}_{S/R}(\langle\lambda\rangle) \simeq \mathrm{tr}_{L/R}(\langle 2\lambda\rangle) \perp \mathrm{tr}_{L/R}(\langle 2\lambda\alpha^2\rangle) \simeq \mathrm{tr}_{S'/R}(\langle\lambda\rangle_\tau),$$

where $\mathrm{tr}_{S'/R}(\langle\lambda\rangle_\tau)(s, s') = \mathrm{tr}_{S'/R}(\lambda s\tau(s'))$ for all $s, s' \in S'$. □

Remark 2.6 We end this paper giving some examples, taken from the literature (see for instance [5, 8]), of rings with many units, others than fields, which satisfy the conditions of the main Theorems 1.1 and 2.1. (in these examples K will always denote an infinite field of characteristic different from 2):

a) the ring of formal power series $K[[X]]$ (its unique residue field is K),

b) the ring of fractions $S^{-1}A[Y]$, where $A = K[X]$ and S is the multiplicative set of all polynomials in A such that the ideal generated by its coefficients equals A (its residue fields are all finite field extensions of K),

c) any integral extension and any homomorphic image of a ring of the type given in a) or b),

d) any direct product and any direct limit of rings of the type given in a), b) or c).

References

[1] G. Berhuy, *On hermitian trace forms over hilbertian fields*, Math. Z. **237**n.3, (2001), 561-570.

[2] G. Berhuy, *Réalisation de formes $\mathbb{Z}$-bilinéaires symétriques comme formes traces hermitiennes amplifiées*, J. Th. Nombres Bordeaux **12** (2000), 25-36.

[3] S. U. Chase, D. K. Harrison and A. Rosenberg, *Galois theory and Galois cohomology of commutative rings*, Mem. Am. Math. Soc.**52** (1965), 15-33.

[4] F. De Meyer and E. Ingraham, "Separable algebras over commutative rings", L.N.in Math **181**, Springer Verlag, 1971.

[5] D. R. Estes and R.M. Guralnick, *Module equivalences: local to global when primitive polynomials represent units*, J. of Algebra **77** (1982), 138-157.

[6] E. C. Ingraham, *Inertial subalgebras of algebras over commutative rings*, Trans. Amer. Math. Soc. **124** (1966), 77-93.

[7] I. Kikumasa,T. Nagahara and K. Kishimoto, *On primitive elements of Galois extensions of commutative semilocal rings*, Math. J. Okayama Univ. **31** (1989), 31-55.

[8] B. R. McDonald, *Linear algebra over commutative rings*, Pure and Aplied Math. **87**, Marcel Dekker Inc, 1984.

[9] B. R. McDonald and W. C. Waterhouse, *Projective modules over rings with many units*, Proc. Am. Math. Soc. **83** (1981), 455-458.

[10] A. Paques, *On primitive and normal basis theorem*, Comm. in Algebra **16** (1988),443-455.

[11] W. Sharlau, *On trace forms of algebraic number fields*, Math. Z. **196** (1987), 125-127.

[12] O. Taussky, *On matrix classes corresponding to an ideal and its inverse*, Illinois Math. J.**1** (1957), 108-113.

[13] O. V. Villamayor, *Separable algebras and Galois extensions*, Osaka J. Math **4** (1967), 161-171.

[14] W. C. Waterhouse, *Scaled trace forms over number fields*, Arch. Math. **47** (1986), 229-231.