CADERNOS DE MATEMÁTICA **03**, 61–75 May (2002)
ARTIGO NÚMERO SMA#136

Split firs

P. M. Cohn

Department of Mathematics, University College London, Gower Street, London WC1E 6BT, UK
E-mail: pmc@math.ucl.ac.uk

V. O. Ferreira

Departamento de Matemática, Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo - Campus de São Carlos, Caixa Postal 668, 13560-970 São Carlos SP, Brazil
E-mail: vitor@icmc.sc.usp.br

A study is made of firs under ground field extension. We consider a generalization: power-free ideal rings (pfirs) and show that for any fir R there is a finite localization T such that for any Galois extension E of the centre T_E is a pfir. Cases are examined where the resulting ring is a fir and where no localization is necessary. May, 2002 ICMC-USP

INTRODUCTION

Let D be a skew field with centre k. For any finite field extension E of k, the extended algebra $D_E = D \otimes_k E$ is a total matrix ring over a skew field, as is well known (see e.g. [5], Chapter 7). For a subring R of D which is a k-algebra and which generates D as a skew field, it is no longer true that R_E is necessarily a full matrix ring, but this can be achieved if we enlarge R by adjoining the inverses of a finite set of elements. In the case where R_E is a full matrix ring of the same order as the ring D_E, R is said to be *split* by E. Here it is of some interest to find out what properties of R are preserved by extension. We shall be particularly concerned with free ideal rings, briefly firs; it seems plausible that for a fir R a split fir can be obtained by adjoining inverses of a finite set, this has been proved in the particular case of tensor rings in [8]. For general firs we are not quite able to prove this, but we shall find in §1 that the extended ring is hereditary and power-free, i.e. every finitely generated projective module has a power which is free of unique rank. This leads to the notion of a power-free ideal ring (pfir), which is discussed in §2. In §3 we study the effect on skew fields of extending the centre, and in §4 we look at some special cases where the extended ring is a matrix ring over a fir. This already yields some interesting constructions; in particular, we shall need the matrix reduction functor (§5) as well as some of the results on division algebras which remain true for skew fields finite-dimensional over their centres (§6).

Publicado pelo ICMC-USP
Sob a supervisão CPq/ICMC

Sometimes the prefix "skew" is omitted from skew field; it is usually clear from the context whether fields are commutative or not.

1. GENERALITIES ON EXTENSIONS

Let R be a ring and Σ a set of matrices over R. If we adjoin a formal inverse to each matrix in Σ we obtain a ring R_Σ, called the *localization* of R by Σ, with a homomorphism $R \longrightarrow R_\Sigma$. If Σ is a finite set of matrices over R, then R_Σ will be called a *finite localization* of R. Since we are mainly interested in fields of fractions, we shall assume that Σ consists of full matrices, where a matrix A is *full* if it is square, say $n \times n$, and for any factorization into an $n \times r$ by an $r \times n$ matrix of A we have $r \geq n$ (see [3] or [6]). When R is a fir, semifir, or more generally, a Sylvester domain, the mapping $R \longrightarrow R_\Sigma$ is injective for any set Σ of full matrices, and there exists a universal (skew) field of fractions U, obtained by localizing at the set of all full matrices over R.

Suppose further that R is a k-algebra, where k is a commutative field, and let E be a finite commutative field extension of k. We write $R_E = R \otimes_k E$ and similarly for the universal field of fractions U. Our object will be to compare R with R_E, for any fir R, given information about the relation between U and U_E. The centre C of U is a commutative extension field of k and if we localize a fir R at $C^\times$ we again obtain a fir, by [3], Proposition 1.5.4; a similar result (with a similar proof) holds for semifirs or Sylvester domains. Henceforth we shall assume that R, U, k are as before and in addition k is the centre of R and of U. As we know from Corollary 6.3.4 of [3], this is so for any non-Ore fir.

Our first result concerns the effect of extending the ground field.

PROPOSITION 1.1. *Let R be an algebra over a commutative field k and E/k be a commutative field extension. Then for any set Σ of matrices over R we have*

$$(R_\Sigma)_E \cong (R_E)_\Sigma \tag{1}$$

Proof. The natural homomorphism $R \longrightarrow R_\Sigma$ arises by inverting Σ; hence we have a homomorphism $R_E \longrightarrow (R_\Sigma)_E$ in which Σ is inverted. This gives rise to a homomorphism $(R_E)_\Sigma \longrightarrow (R_\Sigma)_E$; to show that it is an isomorphism, we construct its inverse. The homomorphism $R \longrightarrow R_E$ extends to a homomorphism $R_\Sigma \longrightarrow (R_E)_\Sigma$, and hence to a map $(R_\Sigma)_E \longrightarrow (R_E)_\Sigma$, which is seen to be the inverse, and it establishes the isomorphism (1). □

In the particular case where R is a semifir and Σ the set of all full matrices over R, this (with the remark before Proposition 1.1) proves

COROLLARY 1.1. *Let R be a semifir with universal field of fractions U, and suppose that R is a k-algebra, where k is the centre of U (hence also of R). Let E/k be a commutative field extension and denote by Φ the set of all full matrices over R. Then*

$$U_E \cong (R_E)_\Phi. \square$$

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

Next we note that coproducts are preserved by field extensions.

THEOREM 1.1. *Let k be a commutative field and R, S any k-algebras with a common subfield F which is a k-algebra. If E/k is any commutative field extension, then we have a natural isomorphism*

$$(R *_F S)_E \cong R_E * S_E, \tag{2}$$

where the coproduct on the right is taken over F_E.

Proof. We have a bilinear map $(R*S)\times E \longrightarrow R_E*S_E$ which extends to a homomorphism

$$(R * S) \otimes_k E = (R * S)_E \longrightarrow R_E * S_E. \tag{3}$$

In the other direction we have embeddings $R_E \longrightarrow (R * S)_E$, $S_E \longrightarrow (R * S)_E$, and hence a homomorphism from right to left in (2) which is inverse to the map (3), hence the latter is an isomorphism. ∎

We also note that for a coproduct of firs, we can find the universal field of fractions of the coproduct by taking the firs or their universal fields of fractions. A homomorphism is called *honest* if it keeps all full matrices full.

THEOREM 1.2. *Let R_i $(i = 1, 2)$ be a fir with centre k and universal field of fractions U_i and put $R = R_1 *_k R_2$, with universal field of fractions U. Then U is also the universal field of fractions of $U_1 *_k U_2$.*

Proof. The coproduct $U_1 * U_2$ is a fir and so has a universal field of fractions V, say, and we have to show that $U \cong V$. Consider the inclusion map $R_1 \longrightarrow R_1 * R_2$. It is honest, for if we combine it with the natural map $R_1 * R_2 \longrightarrow U_1 * U_2$, it maps all full matrices over R_1 to invertible matrices, so these matrices must be full over $R_1 * R_2$. It follows that the natural map $R_1 * R_2 \longrightarrow U$ inverts all full matrices over R_1 and likewise all full matrices over R_2, so we have a map $U_1 * U_2 \longrightarrow U$. Now any full matrix over $R_1 * R_2$ is inverted over U (by definition of the latter) and so is full over $U_1 * U_2$; therefore it is inverted over V and so we have a map $U \longrightarrow V$ which restricts to the identity on $R_1 * R_2$. But the map $U_1 * U_2 \longrightarrow V$ is an epimorphism, hence the map $U \longrightarrow V$ is an isomorphism, as claimed. ∎

Auslander-Reiten-Smalø have given conditions for a ring extension to preserve the global dimension (cf. III.4, p. 89ff. of [2]), which can be put as follows in a more general context.

All rings are K-algebras, where K is a commutative ring. We shall be concerned with a ring extension $A \subseteq B$, and look for conditions under which the global dimension is unchanged.

PROPOSITION 1.2. *Let A, B be rings, where $A \subseteq B$ with a split exact sequence of A-bimodules*

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0,$$

where C_A is projective. Then $\text{r.gl.dim}(A) \leq \text{r.gl.dim}(B)$.

Proof. By hypothesis $B = A \oplus C$, hence we have, for any right A-module M, $M \otimes B = M \oplus (M \otimes C)$, and so

$$\mathrm{pd}_A(M) \leq \mathrm{pd}_A(M \otimes B). \tag{4}$$

Now take a minimal projective B-resolution of $M \otimes B$:

$$\ldots \longrightarrow P_1 \longrightarrow P_0 \longrightarrow M \otimes B \longrightarrow 0.$$

Since $B_A = A \oplus C$ is projective, this is a projective resolution of $M \otimes B$ as A-module, so $\mathrm{pd}_A(M \otimes B) \leq \mathrm{pd}_B(M \otimes B)$, and with (4) this shows that

$$\mathrm{pd}_A(M) \leq \mathrm{pd}_B(M \otimes B) \leq \mathrm{r.gl.dim}(B).$$

Taking the supremum over all M_A, we get the asserted inequality. □

For an inequality in the other direction we need a stronger condition. We recall that, regarding B as an A-ring, we have an exact sequence of B-bimodules

$$0 \longrightarrow \Omega \longrightarrow B \otimes_A B \longrightarrow B \longrightarrow 0,$$

where the second homomorphism is the multiplication map (and Ω is the universal derivation module, cf. [5] 2.2, p. 48). If the sequence splits, as B-bimodule sequence, B is said to be *separable* over A. As is well known, this is equivalent to the existence of a separability idempotent $e = \sum a_i \otimes b_i$, i.e. an idempotent e in $B \otimes B$ mapping to 1 in B and such that $ea = ae$ for all $a \in A$ ([5], Proposition 6.7.1, p. 249).

PROPOSITION 1.3. *Let A, B be rings such that B is separable as A-ring and projective as left A-module. Then* $\mathrm{r.gl.dim}(B) \leq \mathrm{r.gl.dim}(A)$.

Proof. For any right B-module N we have $N \otimes_A B = N \otimes_B (B \otimes_A B) = N \oplus (N \otimes_B \Omega)$, hence

$$\mathrm{pd}_B(N) \leq \mathrm{pd}_B(N \otimes B). \tag{5}$$

Now take a minimal projective A-resolution of N:

$$\ldots \longrightarrow P_1 \longrightarrow P_0 \longrightarrow N \longrightarrow 0$$

and tensor with B over A. Since ${}_AB$ is projective, we get an exact sequence

$$\ldots \longrightarrow P_1 \otimes B \longrightarrow P_0 \otimes B \longrightarrow N \otimes B \longrightarrow 0. \tag{6}$$

Now for any projective right A-module P and right B-module N,

$$\mathrm{Hom}_B(P \otimes B, N) \cong \mathrm{Hom}_A(P, \mathrm{Hom}_B(B, N)) \cong \mathrm{Hom}_A(P, N);$$

since P_A is projective, this is exact in N, so $P \otimes B$ is B-projective and (6) is a projective B-resolution of $N \otimes B$. It follows that

$$\mathrm{pd}_B(N \otimes B) \leq \mathrm{pd}_A(N). \tag{7}$$

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

Combining (5) and (7) we find that $\mathrm{pd}_B(N) \leq \mathrm{pd}_A(N)$ for all B-modules N, hence the result. □

To apply these results to group rings we note that for any ring A and any finite group G whose order is a unit in A, the group ring GA of G over A, more generally any skew group ring of G over A is separable over A, for we have the separability idempotent $e = |G|^{-1} \sum g^{-1} \otimes g$, where the summation is over all $g \in G$. Clearly e maps to 1 and for any $h \in G$, $\sum g^{-1} \otimes gh = h \sum (gh)^{-1} \otimes gh$, hence $eh = he$, while for $a \in A$, $\sum g^{-1} \otimes ga = \sum g^{-1} \otimes a^g g = \sum g^{-1} a^g \otimes g = a \sum g^{-1} \otimes g$, so $ea = ae$. Thus we have

Theorem 1.3. *Let A be any ring and G a finite group with an action on A and such that $|G|$ is a unit in A. Then the skew group ring B of G over A has the same (left or right) global dimension as A.* □

Suppose that E/k is any commutative field extension which is separable. Then the multiplication map $E \otimes_k E \longrightarrow E$ is split by a separability idempotent, and for any k-algebra A we have

$$A_E \otimes_A A_E = (A \otimes_k E) \otimes_A (A \otimes_k E) = A \otimes_k E \otimes_k E,$$

and now the separability idempotent for E can be used to show that A_E is separable over A. Thus we obtain

Proposition 1.4. *Let A be any k-algebra, where k is a commutative field and let E/k be a finite separable field extension. Then A_E is separable over A and so these two rings have the same global dimension.* □

We recall from [3] that any fir is (left and right) hereditary; in fact it may be defined as a ring which is (left and right) hereditary and projective-free (i.e. finitely generated projective modules are free, of unique rank). Hence the above result shows in particular that a fir under a separable field extension of the centre remains a hereditary ring. Whether it remains a fir depends on the behaviour of the monoid of projectives. Our next result gives some information in the case of a Galois extension. A ring R will be called *powerprojective-free*, or briefly *power-free*, if it has IBN (invariant basis number) and for each finitely generated projective R-module P there is a positive integer n such that P^n is free. If the integer n can be chosen independently of P, R is said to be power-free of *index* n, or generally of *bounded index*. It is clear that any power-free ring has a unique projective rank function.

For the next proof we shall need a result on Galois descent (see [7], Chapter 11). If E/k is a finite Galois extension with group G and V is a vector space over E with an action of G by semilinear transformations, then V can be obtained from a k-space by extension of scalars and the same holds for any subspace admitting the G-action (Theorem 11.9.1).

Theorem 1.4. *Let R be a fir with centre k, where k is a field, and let E/k be a (commutative) Galois extension of finite degree n. Then there is a finite localization T of R such that $T_E = T \otimes_k E$ is power-free of index at most n.*

Proof. Denote the Galois group of E/k by G, write $S = R_E = R \otimes_k E$ and let P be any (finitely generated) projective S-module. If P is a direct summand of S^r, write $P_1 = P, P_2, \dots, P_n$ for the submodules of S^r obtained by applying the n elements of G to P, form $Q = P_1 \oplus \cdots \oplus P_n$ and define a homomorphism $\phi : Q \longrightarrow S^r$ by the rule $(x_i) \longmapsto \sum x_i$. The image I is invariant under G and hence is obtained by extension from a submodule of a free R-module, which is itself free because R is a fir. It follows that the image is free, say $I \cong S^s$. The kernel K consists of all elements $u \in Q$ such that u maps to 0 in S^r, but if u maps to 0, then so does u^σ, for any $\sigma \in G$, so K is again obtained by extension from a free module and so is itself a free S-module, say $K \cong S^t$. Thus we have an exact sequence

$$0 \longrightarrow K \longrightarrow Q \xrightarrow{\phi} I \longrightarrow 0.$$

The sequence is clearly split, and we conclude that $Q \cong S^{t+s}$. Now let U be the universal field of fractions of R; then U_E is a $d \times d$ matrix ring, where $d \mid n$, so over U_E the modules P_i are all isomorphic: if $P_i = S^r e_i$, then $e_i = e_1 u_i$ for a unit u_i in U_E. Let Σ be the set of denominators of the u_i in R and set $T = R_\Sigma$; then over T_E all the P_i become isomorphic and so $Q \cong P^n \cong T_E^{t+s}$, which is what we had to prove. □

It seems likely that under the given hypothesis T_E is actually a full matrix ring over a fir, but so far there is no proof.

Let U be any skew field with centre k. Then for any finite field extension E of k, the extended ring U_E is a $d \times d$ matrix ring over a skew field, where $d \mid [E : k]$. If R is a k-subalgebra of U such that R_E is a $d \times d$ matrix ring, we shall say that R is *split* by E. If in particular R is split by the algebraic closure of k, R is said to be *absolutely split*. It is easy to see that any algebra generating a skew field can be extended to a split ring by adjoining a finite set of inverses of elements. We need only form U_E and adjoin the inverses occurring in the matrix units e_{ij}. Thus we obtain

PROPOSITION 1.5. *Let U be a skew field with centre k and let R be a k-subalgebra generating U as a skew field. Then there is a finite localization of R which is absolutely split.* □

2. POWER-FREE IDEAL RINGS

The results of §1 suggest the following slight extension of the notion of a fir.

DEFINITION 2.1. A ring R is called a *left power-free ideal ring*, *left pfir* for short, if there exists an integer $n \geq 1$ such that for every left ideal I of R the left R-module I^n is free of unique rank. *Right pfirs* are defined similarly and a *pfir* is a left and right pfir.

We note that in contrast to firs, pfirs may have zero-divisors; for example, any full matrix over a fir is a pfir, as is easily verified. The converse does not hold, as Theorem 2.1 below shows.

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

In analogy with the case of firs we have

PROPOSITION 2.1. *A ring is a left pfir if and only if it is left hereditary and power-free of bounded index.*

Proof. Under either hypothesis R has IBN. Now let R be a left pfir of index n. For any left ideal I of R, I^n is free, hence projective, so R is hereditary. Further, any finitely generated projective left R-module P is a direct sum of left ideals and it follows that P^n is free, so R is power-free of index n. Conversely, assume that R is left hereditary and power-free of index n. Then any left ideal I is projective, and in fact isomorphic to a direct sum of finitely generated projective modules. It follows that I^n is free, and so R is a left pfir. □

As an example of a pfir we have the coproduct of skew fields under field extension.

THEOREM 2.1. *Let C, D be skew fields with a common centre k and let $R = C *_k D$. Then, for any finite commutative field extension E of k, R_E is a pfir.*

Proof. We know that $R_E \cong C_E *_E D_E$, by Theorem 1.1, and that $C_E \cong \mathfrak{M}_r(K), D_E \cong \mathfrak{M}_s(L)$, where both r and s divide $[E : k]$ and K and L are skew fields with centre E. Therefore R_E is hereditary. Moreover, the monoid of projectives of R_E is isomorphic to $\frac{1}{r}\mathbf{N} \coprod_{\mathbf{N}} \frac{1}{s}\mathbf{N}$ and hence R_E is power-free of index at most $[E : k]$. □

It is clear that if in this theorem we choose C, D and E so that neither r nor s is 1, we obtain a pfir which is not a full matrix ring over a fir.

More generally, we obtain from Proposition 1.4 and Theorem 1.4,

THEOREM 2.2. *Let R be a fir with centre k. Then for any Galois field extension E of k, there exists a finite localization T of R such that T_E is a pfir of index at most $[E : k]$.* □

3. SKEW FIELDS UNDER EXTENSION OF THE CENTRE

Let R be a semifir with centre k, a field, and suppose that the universal field of fractions U of R also has the precise centre k. Given a finite algebraic extension field E of k of degree n, form $R_E = R \otimes_k E$; this is contained as a subring in $U_E = U \otimes_k E$. By Theorem 7.1.3 of [5], U_E is a central simple E-algebra, left Artinian, because $[U_E : U] = [E : k] = n$ and so we have

$$U_E \cong D \otimes_E E_r,$$

for some integer r and skew field D. Secondly, since E is embedded in k_n, U_E is embedded in U_n. But $U_n \cong U \otimes k_n$ contains U_E and hence k_r. If the centralizer of k_r in U_n is denoted by B, then $B \cong C_s \cong C \otimes k_s$ for some skew field C, and so, by Proposition 7.1.5 of [5],

$$U \otimes k_n = k_r \otimes B \cong k_r \otimes C \otimes k_s,$$

in fact, $C \cong U$ by uniqueness, and now a comparison gives $n = rs$. Thus we have

Proposition 3.1. *Let U be any skew field with centre k, and E a finite extension of k of degree n. Then $U_E = D_r$, for a skew field D, where $r \mid n$. More precisely, if $E = k(\alpha)$, where α has the minimal polynomial f of degree n over k, then f splits into r factors over D; thus D_E is a skew field if and only if f remains irreducible over D.*

Proof. We have seen that $U_E = D_r$. Now assume that E/k is a simple extension, say $E = k(\alpha)$, and let f be the minimal polynomial of α over k, $\deg f = [E : k] = n$. Since f is irreducible over the centre k of D, f is an I-atom in $D[t]$ (that is, f is an invariant non-unit which is not a product of invariant non-units) and over D we have the factorization $f = p_1 \dots p_r$, where the polynomials p_i all have the same degree $t = n/r$, and by tensoring the exact sequence

$$0 \longrightarrow (f) \longrightarrow k[t] \longrightarrow E \longrightarrow 0$$

with D we obtain

$$0 \longrightarrow (f) \longrightarrow D[t] \longrightarrow D_E \longrightarrow 0,$$

hence $D_E = D_r$, where D is the endomorphism ring of the (unique) simple module of D_E (see [3] Theorem 6.4.3, p. 314, [6] Theorem 1.5.4, p. 29). □

The next lemma generalizes Theorem 7.2.6 of [5] (which was limited to finite-dimensional algebras). We shall write $A \oplus B$ for the diagonal sum of matrices A, B.

Lemma 3.1. *Let D be a skew field with centre k, let E/k be a finite field extension of degree r and let n be the least integer such that E is embedded in D_n. Then $n \leq r$, the centralizer E' of E in D_n is a skew field and $D \otimes_k E \cong (E')_d$, where $r = nd$.*

Proof. Since $E \subseteq k_r \subseteq D_r$, it follows that n exists and satisfies $n \leq r$. Take the least such n and denote by E' the centralizer of E in D_n. By Theorem 7.1.9 of [5], E' is simple with centre E; if E' consists entirely of non-singular elements it is a field. Otherwise take $A \in E'$ singular but not zero. By similarity transformation we have $A = B \oplus 0$, where B is non-singular. Any matrix commuting with A has the form $P \oplus Q$, where $PB = BP$. Thus all the matrices in E have this form, and if $P(a) \oplus Q(a)$ is the matrix corresponding to $a \in E$, then the map $a \longmapsto P(a)$ is a homomorphism $E \longrightarrow D_m$, where $m < n$ and this contradicts the definition of n. Thus E' is a field; by Theorem 7.1.9 of [5], we have $D_n \otimes E \cong E' \otimes k_r$, hence $n \mid r$, say $r = dn$, and so $D \otimes E \cong (E')_d$. □

Given a fir R with centre k, if R contains a commutative field F (containing k) and $E \cong F$, then R_E has zero-divisors and so is not a fir; to study it, we shall need to examine $F \otimes E$; this is a direct product of commutative fields, which are all isomorphic when F/k is Galois (5.7 of [4]). To find its structure it will be helpful to have idempotents in $F \otimes E$:

Proposition 3.2. *Let f be a separable polynomial over k and define $\varphi(x, y)$ by the equation*

$$\varphi(x, y) = \frac{f(x) - f(y)}{(x - y)}. \tag{8}$$

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

If F, E are extension fields of k generated by zeros α, β of f respectively, then in $F \otimes E$ the element $p = \varphi(\alpha, \beta)$ satisfies $p\alpha = p\beta$ and $p^2 = f'(\beta)p$, where f' is the derivative of f; so $p/f'(\beta)$ is an idempotent in $F \otimes E$.

Proof. By definition we have $\varphi(x, y)(x - y) = f(x) - f(y)$, hence $\varphi(\alpha, \beta)(\alpha - \beta) = f(\alpha) - f(\beta) = 0$, and it follows that $p\alpha = p\beta$. Now the Taylor expansion shows that $\varphi(x, \beta) = f'(\beta) + (x - \beta)h(x)$, hence $p - f'(\beta) = (\alpha - \beta)h(\alpha)$, and so $(p - f'(\beta))p = 0$, as we had to show. ∎

Let R be a fir with centre k and let F be a subfield of R containing k such that F/k is a Galois extension of finite degree n, say $F = k(\alpha)$, where $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_n$ are the conjugates of α. Given a field E isomorphic to F, with $\alpha \longleftrightarrow \beta$ say, consider the extension R_E. Let f be the minimal polynomial of α over k and define $\varphi(x, y)$ as in (8). We note that $\varphi(y, x) = \varphi(x, y), \varphi(x, x) = f'(x)$. In $F \otimes E$ we have $\varphi(\alpha, \beta)(\alpha - \beta) = f(\alpha) - f(\beta) = 0$, hence $\varphi(\alpha, \beta)\alpha = \varphi(\alpha, \beta)\beta$ and so $\varphi(\alpha, \beta)f'(\alpha) = \varphi(\alpha, \beta)f'(\beta)$. Let us define

$$e_i = \frac{\varphi(\alpha_i, \beta)}{f'(\alpha_i)} = \frac{\varphi(\alpha_i, \beta)}{f'(\beta)},$$

so that e_i is an idempotent, by Proposition 3.2. For any $b_1, \ldots, b_n$ the polynomial $F(x) = \sum b_i\varphi(x, \alpha_i)/f'(\alpha_i)$ is of degree at most $n - 1$ and for $x = \alpha_j$ it reduces to b_j, because $\varphi(\alpha_j, \alpha_i)/f'(\alpha_i) = \delta_{ij}$. Thus F is constant, equal to 1, and so $\sum e_i = 1$; further for $i \neq j$ we have $\varphi(\alpha_i, \beta)\varphi(\alpha_j, \beta)\alpha_i = \varphi(\alpha_i, \beta)\varphi(\alpha_j, \beta)\beta = \varphi(\alpha_i, \beta)\varphi(\alpha_j, \beta)\alpha_j$, hence $e_ie_j = 0$; so it only remains to show that all the e_i are conjugate.

Let $L(c), R(c)$ denote left and right multiplication by c, respectively, for any $c \in R$. Since $L(a), R(b)$ commute, for any a, b, by associativity, we have $\varphi(L(\alpha), R(\alpha_i))(L(\alpha) - R(\alpha_i)) = f(L(\alpha)) - f(R(\alpha_i)) = 0$. Now choose $x \in R$ such that $x\alpha \neq \alpha x$; this is possible, because α is not in the centre k of R. We put $c_i = x\varphi(L(\alpha), R(\alpha_i))$; then $\alpha c_i - c_i\alpha_i = c_i(L(\alpha) - R(\alpha_i)) = 0$, so $c_i^{-1}\alpha c_i = \alpha_i$ and more generally, $c_i^{-1}e_1c_i = e_i$. Thus all the e_i are conjugate, once the inverses of the c_i have been adjoined.

Let U be the universal field of fractions of R; then $R_E \subseteq U_E$, while $U_E \cong D_n$ for some field D. Now $e_iU_E \cong D^n$, a simple D_n-module; it follows that e_iR_E is indecomposable, and every projective R_E-module is a power of e_iR_E. Hence R_E is an $n \times n$ matrix ring over a fir.

We sum up the result as

Theorem 3.1. *Let R be a fir with centre k and let F be a subfield of R containing k such that F/k is a Galois extension of degree n. Then there is a finite localization T of R such that for any field E isomorphic to F, T_E is a full $n \times n$ matrix ring over a fir.* ∎

4. EXAMPLES

Let us look again at the examples at the end of §3, of a fir which is split by a field extension. Our ground field k is assumed to have characteristic not 2 and to contain an

Publicado pelo ICMC-USP
Sob a supervisão CPq/ICMC

element a, say, which is not a square. We put $F = k(\alpha)$, where $\alpha^2 = a$, and consider the tensor ring $R = F_k\langle x\rangle$. Clearly this is a fir, we denote its universal field of fractions by U. Next take a field E isomorphic to F, say $E = k(\beta)$, where $\beta^2 = a$, and consider $R_E = R \otimes_k E$. We have $U_E = D_2$, where D is a skew field, and we ask what elements need to be adjoined to R to ensure that an extension of the ground field k to E produces a 2×2 matrix ring. Clearly what is needed is a complete set of matrix units, so we need to take the matrix units in U_E and adjoin inverses of their denominators, elements of R, to R. They can be obtained as follows. In $F \otimes E$ we have an idempotent $e = 1/2(1 + \alpha/\beta)$; we put $e_{11} = e, e_{22} = 1 - e$, and further define $u = \alpha x + x\alpha, v = \alpha x - x\alpha$. Then $\alpha u = \alpha x\alpha + ax = u\alpha, \alpha v = ax - \alpha x\alpha = -v\alpha$, hence $\alpha v^2 = v^2\alpha$. The set $\Sigma = \{v\}$ regarded as a matrix system is *factor-complete*, i.e. if $AB \in \Sigma$, where A is $r \times n$ and B is $n \times r$, then $r \leq n$ and in the localization R_Σ there exists an $n \times (n - r)$ matrix B' such that (B, B') is invertible. It follows that the multiplicative system Σ' generated by Σ is also factor-complete. Let us put $S = R_{\Sigma'}$; by Theorem 7.10.7 of [3], S is again a fir and in S we have $e_{11}v = ve_{22}$; we now put $e_{12} = e_{11}v, e_{21} = v^{-1}e_{11}$; then $e_{12} = e_{22}v, e_{21} = e_{22}v^{-1}$, and it is easily verified that the e_{ij} form a set of matrix units. Thus we have

$$S_E \cong T_2, \tag{9}$$

where T is a subring of D, because $S_E \subseteq U_E$. Since S_E is hereditary, by Proposition 1.4 above, so is T (by Morita equivalence). We also note that R has centre k, as does S, so S_E has centre E and hence T also has centre E.

Now T is the centralizer of the e_{ij} and it follows that T contains v^2 as well as p, q, where $p = e_{11}u + e_{22}v^{-1}uv, q = e_{22}u + e_{11}vuv^{-1}$. To realize the isomorphism (9) we need to map $s \in S_E$ to (s_{ij}), where $s_{ij} = \sum_\nu e_{\nu i}se_{j\nu}$. Writing $[s]$ for the matrix (s_{ij}), we find

$$\begin{aligned} [u] &= \begin{pmatrix} p & 0 \\ 0 & q \end{pmatrix}, \qquad [v] = \begin{pmatrix} 0 & 1 \\ v^2 & 0 \end{pmatrix}, \\ [\alpha] &= \begin{pmatrix} \beta & 0 \\ 0 & -\beta \end{pmatrix}, \quad [x] = \Big[\frac{\alpha}{2a}(u+v)\Big] = \frac{\beta}{2a}\begin{pmatrix} p & 1 \\ -v^2 & -q \end{pmatrix}. \end{aligned} \tag{10}$$

Let $A = E\langle p, q, r\rangle$, the free E-algebra on p, q, r. This is a fir, and if we adjoin r^{-1}, we again get a fir, B say. We claim that $B \cong T$; to prove this it will be enough to show that $B_2 \cong T_2$. We define a map from S_E to B_2 as follows:

$$x \longmapsto \frac{\beta}{2a}\begin{pmatrix} p & 1 \\ -r & -q \end{pmatrix}, \quad \alpha \longmapsto \begin{pmatrix} \beta & 0 \\ 0 & -\beta \end{pmatrix}.$$

Then $\alpha x + x\alpha = u, \alpha x - x\alpha = v$, where u, v are as in (10) (with v^2 replaced by r). Thus we have a homomorphism from S_E to B_2, which is surjective, since the image includes a generating set, and the restriction to T is injective, because its image B is free. This shows that $B \cong T$, so T is a fir, as claimed.

More generally, suppose that F/k is a cyclic extension of degree n (prime to char k), say $F = k(\alpha)$, where $\alpha^n = a \in k$, and $E = k(\beta)$ with $\beta^n = a$, assume further that k contains a primitive nth root of 1, say ω, and put $v = \alpha^{n-1}x + \omega\alpha^{n-2}x\alpha + \cdots + \omega^{n-1}x\alpha^{n-1}$. Then we have $\alpha v = v\omega\alpha$, thus the automorphism $\alpha \longmapsto \omega\alpha$ of F is realized within $F_k\langle x\rangle$ by conjugation with v. From this it is easy to construct a set of matrix units in S_E as before.

As another example let us take a field k of characteristic 2, with an element a which is not a square in k. Define $F = k(\alpha)$, where α is a root of $x^2 = a$, and form the tensor ring $F_k\langle x\rangle$ with a single indeterminate x and its universal field of fractions U. Let E be a field isomorphic to F over k, say $E = k(\beta)$, where $\beta^2 = a$, and consider $U_E = U \otimes_k E$. As a skew field under extension, U_E is central simple and Artinian, but it is not a field because it has zero divisors, e.g. $1 + \alpha^{-1}\beta$; hence it is a matrix ring over a field. Let us find an explicit form for the matrix units. We put $t = x(x\alpha + \alpha x)^{-1}$; then $\alpha t + t\alpha = 1$ and if we put $u = t\alpha$, then $\alpha t = u + 1$ and $u(u+1) = t^2 a$. Now consider $u + \beta t = t(\alpha + \beta)$ in U_E; we have $(u + \beta t)^2 = u^2 + \beta(ut + tu) + at^2 = u + \beta t$, because $ut + tu = t\alpha t + t^2\alpha = t$. Thus we have found an idempotent $e = t(\alpha + \beta)$ different from 0 and 1 in U_E. Further, we have $t^{-1}et = (\alpha + \beta)t = t(\alpha + \beta) + 1 = 1 - e$. Now put $p = t(\alpha + \beta)t, q = \alpha + \beta$, so that $p^2 = q^2 = 0$. Then $pe = 0, ep = p, qe = q, eq = 0$ with similar equations for $1 - e$ in place of e, so that $e, p, q, 1 - e$ form a set of matrix units for U_E.

More generally consider the case of a p-radical (purely inseparable) extension in characteristic p. We shall need the following elementary fact:

LEMMA 4.1. *Let k be a field of prime characteristic p and let x, y be two indeterminates satisfying the relation*

$$xy - yx = 1. \tag{11}$$

Then for any positive integer r,

$$x^r y - yx^r = rx^{r-1}, \tag{12}$$

$$(xy)^p = x^p y^p + xy, \tag{13}$$

$$(yx)^{p-1} = x^{p-1}y^{p-1} + 1. \tag{14}$$

Proof. The formula (12) (which is well known) follows by an easy induction left to the reader. To prove (13), let us put $z = xy$; then (11) becomes $xz = zx + x = (z+1)x$, hence $zx^{-1} = x^{-1}(z+1)$. Now we have $y^p = (x^{-1}z)^p = x^{-p}(z+p-1)(z+p-2)\ldots(z+1)z = x^{-p}(z^p - z)$, hence $z^p - z = x^p y^p$, i.e. (13), and (14) follows on dividing by x on the left and y on the right. □

Now, as before, let $F = k(\alpha)$, where α is a root of $x^p = a$, and $\operatorname{char} k = p$, form the tensor ring $F_k\langle x\rangle$ with a single indeterminate x and denote its universal field of fractions by U. Further, let $E = k(\beta)$, where $\beta^p = a$, and consider U_E. As before this is a full matrix ring over a field and our task is to find a set of matrix units in U_E. We shall use the characterization of matrix rings given in [1]: a given ring R is an $n \times n$ matrix ring if and only if R contains elements c, f, g such that $f^n = 0$ and $cf^{n-1} + fg = 1$. In that case $R = S_n$, where S is the centralizer of c, f, g in R.

Let δ be the inner derivation $u \longmapsto u\alpha - \alpha u$ on U. Clearly $\delta^p = 0$, so if we put $t = x\delta^{p-2}(x\delta^{p-1})^{-1}$, then $t\delta = 1$, i.e. $t\alpha - \alpha t = 1$, and it follows that on writing $d = \alpha - \beta$

we have $td - dt = 1$. Further, we have $d^p = (\alpha - \beta)^p = \alpha^p - \beta^p = a - a = 0$, and, by (14), $(dt)^{p-1} = t^{p-1}d^{p-1} + 1$. Let us put $f = d, c = t^{p-1}dt, g = t(dt)^{p-2}$. We have $f^p = 0, cf^{p-1} + fg = t^{p-1}dtd^{p-1} + (dt)^{p-1} = t^{p-1}(td-1)d^{p-1} + (dt)^{p-1} = t^pd^p - t^{p-1}d^{p-1} + (dt)^{p-1} = 1$, by (14), bearing in mind that $d^p = 0$. Thus the conditions for a matrix ring are satisfied and we have $U_E = V_p$, where V is the centralizer in U_E of c, f, g, i.e. of $d, t^{p-1}dt$ and $t(dt)^{p-2}$.

In this connexion it may be of interest to note Theorem 3.2 of [8], which deals with a purely inseparable field extension F/k of degree p: given a tensor ring $R = F_k\langle x\rangle$, there is an element of R such that by adjoining its inverse we obtain a ring S with the property that $S_F = A_p$, where A is a fir.

5. MATRIX REDUCTION

We recall the matrix reduction functor from [3], 2.11 and [6], 1.7 in a slightly generalized form. Let K be any ring and consider the category Rg_K of K-rings. For each $n \geq 1$, the *matrix reduction functor* $\mathfrak{W}_n$ is defined as the left adjoint of the $n \times n$ matrix functor $\mathfrak{M}_n(R) = R_n$:

$$\mathrm{Rg}_K(R, \mathfrak{M}_n(S)) \cong \mathrm{Rg}_K(\mathfrak{W}_n(R), S).$$

The explicit definition of $\mathfrak{W}_n$ runs as follows. Put $\mathfrak{F}_n(R) = R *_K K_n$; since $\mathfrak{F}_n(R)$ contains a set of $n \times n$ matrix units (e_{ij}), it is itself a matrix ring: $\mathfrak{F}_n(R) = S_n$ (cf. Proposition 0.1.1 of [3] or Proposition 4.3.3 of [4]). We put $S = \mathfrak{W}_n(R)$, thus

$$R *_K K_n \cong \mathfrak{M}_n(\mathfrak{W}_n(R)).$$

Sometimes we shall write $\mathfrak{W}_n(R; K)$ to emphasize the rôle of K. Another description which is sometimes useful (and is easily seen to be equivalent to the one just given) is as follows: interpret the elements of R as $n \times n$ matrices, with the elements of K as scalar matrices. To obtain the elements of $\mathfrak{W}_n(R)$ we take the centralizer of the e_{ij}. For each $a \in R$ this gives n^2 elements $a_{ij} = \sum_\nu e_{i\nu}ae_{j\nu}$; when $a \in K$, then since a commutes with the e_{ij}, this reduces to $a_{ij} = a\delta_{ij}$. Now we have

THEOREM 5.1. *Let K be a field and R a K-ring which is non-trivial. Then for any $n > 1$, $\mathfrak{W}_n(R; K)$ is a K-ring which is an $(n-1)$-fir. If R is a fir and K is a field, then $\mathfrak{W}_n(R; K)$ is again a fir.*

Proof. When K is in the centre of R, then $\mathfrak{W}_n(R; K)$ has a filtration satisfying the $(n-1)$-term weak algorithm, by Theorem 2.11.2 of [3], and the proof clearly still applies in the more general case of a K-ring. The last part follows by Corollary 5.7.7 of [6] when K is a commutative field; the extension to the general case is straightforward. □

We can also obtain pfirs through matrix reduction. We shall need

LEMMA 5.1. *Let R be an algebra over a commutative field k and let E/k be a commutative field extension. Then for any $n \geq 1$ we have an isomorphism of E-algebras*

$$\mathfrak{W}_n(R; k)_E \cong \mathfrak{W}_n(R_E; E).$$

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

Proof. If we tensor $\mathfrak{M}_n(\mathfrak{W}_n(R;k))$ with E over k, we obtain

$$\mathfrak{M}_n(\mathfrak{W}_n(R;k))_E \cong \mathfrak{M}_n(\mathfrak{W}_n(R;k)_E). \tag{15}$$

Next we tensor $R *_k \mathfrak{M}_n(k)$ with E over k and use Theorem 1.1 to obtain

$$(R *_k \mathfrak{M}_n(k))_E \cong R_E *_E \mathfrak{M}_n(E).$$

By definition, $R_E *_E \mathfrak{M}_n(E) \cong \mathfrak{M}_n(\mathfrak{W}_n(R_E;E))$, therefore

$$(R *_k \mathfrak{M}_n(k))_E \cong \mathfrak{M}_n(\mathfrak{W}_n(R_E;E)). \tag{16}$$

We now combine (15) and (16), bearing in mind that all the isomorphisms involved preserve the matrix units; this yields the desired result. $\square$

As a consequence we have

THEOREM 5.2. *Let D be a skew field with centre k and let E/k be a finite commutative field extension. Then, for every $n \geq 1$, $R = \mathfrak{W}_n(D;k)$ is a fir and R_E is a pfir, but not a fir, unless D_E is a skew field.*

Proof. We have seen in Theorem 5.1 that R is a fir and, by Proposition 3.1, $D_E \cong \mathfrak{M}_r(U)$, where $r \mid [E:k]$ and U is a skew field. By Lemma 5.1,

$$\mathfrak{M}_n(R_E) \cong \mathfrak{M}_r(U) *_E \mathfrak{M}_n(E). \tag{17}$$

By (17), $\mathfrak{M}_n(R_E)$ is hereditary, hence so is R_E, and if M denotes its monoid of projectives, the isomorphism (17) gives $\frac{1}{n}M \cong \frac{1}{r}\mathbf{N} \coprod_{\mathbf{N}} \frac{1}{n}\mathbf{N}$. Hence R is power-free of index r. Finally it is clear that $M \cong \mathbf{N}$ if and only if $r = 1$. $\square$

Given a fir R with centre k and universal field of fractions U, let us take an algebraic extension E of k of degree r, say. Then $U_E = U \otimes_k E \cong D_s$, where D is a field and s is a factor of r. We ask: what can be said about R_E? One would hope that R_E has the form T_s, where T is a fir with universal field of fractions D, or at least a well-behaved integral domain, but this need not be so. E.g. let $R = F *_k F$, where F is a field with centre k and with E as commutative subfield. Then $F_E \cong L_s$, for some field L with centre E, and $s > 1$, because $E \otimes_k E$, a subring of F_E, has zero-divisors. It follows that $R_E = (F *_k F)_E = F_E *_E F_E = L_s *_E L_s$ (cf. Theorem 1.1 above), and this is not of the form A_t for any fir A and any integer t. For we have $R_E = \mathfrak{M}_s(\mathfrak{W}_s(L *_E L_s; L)) \cong T_s$, where T is a ring with $(s-1)$-term weak algorithm, but T has non-trivializable s-term relations and so is not an s-fir (cf. [6], Theorem 5.7.6, p. 247).

We also note a characterization of matrix algebras, taken from [9], which is sometimes useful. Let R be a ring which is an $n \times n$ matrix algebra, say $R = \mathfrak{M}_n(A)$; if $e = e_{11}, w = e_{1n} + e_{21} + e_{32} + \cdots + e_{nn-1}$, then we have equations

$$w^n = 1 = \sum_i w^{i-1} e w^{1-i} \quad \text{and} \quad e w^{i-1} e = \delta_{i1} e.$$

Conversely if a ring R contains two elements e, w satisfying these equations, then $R \cong \mathfrak{M}_n(A)$, where A is the centralizer of e and w. To see this we define, for any $b \in R$, n^2 elements b_{ij} by the equations

$$b_{ij} = ew^{1-i}bw^{j-1}e, \quad i, j = 1, \ldots, n.$$

Now it is easily verified that the rule $b \longmapsto (b_{ij})$ defines a homomorphism from R to $\mathfrak{M}_n(A)$, where $A = eRe$, with inverse $(c_{ij}) \longmapsto \sum_{ij} w^{i-1}ec_{ij}ew^{1-j}$.

6. SPECIAL CASES OF EXTENSIONS

Let D be a skew field with centre k and let E/k be a finite commutative field extension, say $[E : k] = r$. Then $D_E \cong G_s$, where $s \mid r$ and G is a skew field with centre E, by Proposition 3.1.

If E has a subfield containing k which can be embedded in D, then D_E clearly cannot be a field, as we see by taking the minimal equation of an element in $E \setminus k$ which has a root in D. To give an example where D_E is a matrix ring even though E and D have no isomorphic subextension over k, take any commutative field F and let $H = F(x, \xi)$ be a rational function field, put $\eta = x(\xi - x)$ and $k = F(\xi, \eta), D = H \circ_k k(y)$ with an indeterminate y, where $\circ$ stands for the field coproduct. Then D is a field with centre k and $f = t^4 + \xi t^2 + \eta$ is irreducible over k, but over D we have $f = (t^2 + x)(t^2 + \xi - x)$, where the factors are irreducible over D. Let E be the field obtained by adjoining to k a zero of f; calling this zero λ, we have $(\lambda^2 + x)(\lambda^2 + \xi - x) = 0$. If D_E were a skew field, it would follow that either $\lambda^2 + x = 0$ or $\lambda^2 + \xi - x = 0$, so x now lies in the centre, but $xy - yx \neq 0$, a contradiction. It follows that $D_E \cong G_2$ for some field G. However, D contains no zero of f, because f splits into two irreducible factors of degree greater than one.

The phenomenon can also occur for finite-dimensional algebras. Let F and $H = F(x, \xi)$ be as before; on H we have an automorphism α of order two fixing $F(\xi)$ and mapping x to $\xi - x$. We form the skew polynomial ring $H[y; \alpha]$ and its rational function field $D = H(y; \alpha)$; clearly D is generated over F by x, y, ξ subject to $xy = y(\xi - x)$, and its centre is $C = F(\xi, y^2, x(\xi - x))$. Since $1, x, y, xy$ span D over C and are linearly independent, we have $[D : C] = 4$. We write $\eta = x(\xi - x)$ and consider the polynomial $f = t^4 - \xi t^2 + \eta$ in $D[t]$; it is irreducible over C, while over D it splits into two irreducible factors: $f = (t^2 - x)(t^2 - \xi + x)$. Let E be the field obtained by adjoining a zero λ of f and consider D_E. If this were a skew field, we find as before that x lies in the centre, but $xy = y(\xi - x)$, so $2x = \xi$, a contradiction.

However, it is not clear whether the stated condition (no isomorphic subfields) is really satisfied, so it may be better to use the example below.

Here is an example of a central division algebra (finite-dimensional) D/k and a finite commutative extension E/k such that D_E is not a skew field, even though E and D have no commutative subfields strictly containing k that are isomorphic. Let D be the rational quaternions, so that $k = \mathbf{Q}$, the rationals, and take E/k to be of degree 4, generated by two square roots β_1, β_2, where $\beta_i^2 = b_i \in k$. We know that D_E is a total matrix ring over a skew field; to show that it is not a skew field, it will be enough to show that it contains a non-zero element whose square is zero. Consider the element $f = \mathbf{i} + \mathbf{j}\beta_1 + \mathbf{k}\beta_2$, where we have omitted the tensor product for simplicity. If $f^2 = 0$, then

$$\begin{aligned} 0 &= (\mathbf{i} + \mathbf{j}\beta_1 + \mathbf{k}\beta_2)^2 \\ &= -1 - b_1 - b_2 + (\mathbf{ij} + \mathbf{ji})\beta_1 + (\mathbf{ik} + \mathbf{ki})\beta_2 + (\mathbf{jk} + \mathbf{kj})\beta_1\beta_2 \\ &= -1 - b_1 - b_2. \end{aligned} \tag{18}$$

It only remains to choose b_1, b_2 so that $\sqrt{-1} \notin E$. Take $b_1 = 2, b_2 = -3$, then (18) is satisfied and $E = \mathbf{Q}(\sqrt{2}, \sqrt{-3})$. Clearly E does not contain $\sqrt{-1}$, so this is the desired construction. We note further that for any commutative subfield F of D, $F \otimes E$ is again a field, by Theorem 5.5.5', p. 188 of [5], because F is a Galois extension of k (so, for that matter, is E/k).

REFERENCES

1. G. Agnarsson, S. A. Amitsur and J. C. Robson, Recognition of matrix rings. II, *Israel J. Math.* **96** (1996), 1–13.
2. M. Auslander, I. Reiten and S. O. Smalø, *Representation Theory of Artin Algebras*, Cambridge University Press, Cambridge, 1995.
3. P. M. Cohn, *Free Rings and Their Relations*, 2nd Ed., London Mathematical Society Monographs, Vol. 19, Academic Press, London, 1985.
4. P. M. Cohn, *Algebra*, 2nd Ed., Vol. 2, John Wiley & Sons, Chichester, 1989.
5. P. M. Cohn, *Algebra*, 2nd Ed., Vol. 3, John Wiley & Sons, Chichester, 1991.
6. P. M. Cohn, *Skew Fields. Theory of General Division Rings*, Encyclopedia of Mathematics and its Aplications, Vol. 57, Cambridge University Press, Cambridge, 1995.
7. P. M. Cohn, *Basic Algebra*, Springer-Verlag, London, to appear.
8. V. O. Ferreira, Tensor rings under field extensions, *J. Algebra* **231** (2000), 342–363.
9. T. W. Palmer, *Banach Algebras and the General Theory of $*$-algebras. Vol. I. Algebras and Banach algebras*, Encyclopedia of Mathematics and its Aplications, Vol. 49, Cambridge University Press, Cambridge, 1994.

Publicado pelo ICMC-USP
Sob a supervisão CPq/ICMC