CADERNOS DE MATEMÁTICA **03**, 45–60 May (2002)
ARTIGO NÚMERO SMA#132

# Free symmetric and unitary pairs in division rings with involution

Vitor 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

Jairo Z. Gonçalves†

*Departamento de Matemática, Instituto de Matemática e Estatística, Universidade de São Paulo, Caixa Postal 66.281, 05315-970 São Paulo SP, Brazil*
E-mail: jzg@ime.usp.br

Arnaldo Mandel‡

*Departamento de Ciência da Computação, Instituto de Matemática e Estatística, Universidade de São Paulo, Caixa Postal 66.281, 05315-970 São Paulo SP, Brazil*
E-mail: am@ime.usp.br

Let $D$ be a division ring with an involution and characteristic different from 2. Then, up to a few exceptions, $D$ contains a free pair of symmetric elements provided that (a) it is finite-dimensional and the center has a finite sufficiently large transcendence degree over the prime field, or (b) the center is uncountable, but not algebraically closed in $D$. Under conditions (a), if the involution is of the first kind, it is also shown that the unitary subgroup of $U(D)$ contains a free subgroup, with one exception. The methods developed are also used to describe free subgroups in the multiplicative group of a finite-dimensional division ring provided the center has a sufficiently large transcendence degree over its prime field. May, 2002 ICMC-USP

## INTRODUCTION

Let $k$ be a field of characteristic different from 2 and let $A$ be a $k$-algebra with an involution $*$. Let $U(A)$ denote the group of units of $A$. We consider the existence of free pairs of symmetric and unitary elements in $U(A)$.

* Partially supported by FAPESP, São Paulo - Brazil (Grant 98/14402–8).
† Partially supported by CNPq, Brasília - Brazil (Grant 302756/82–5) and partially supported by FAPESP, São Paulo - Brazil (Projeto Temático 00/07291-0).
‡ Partially supported by PRONEX/CNPq (Projeto PRONEX 664107/1997–4).



Publicado pelo ICMC-USP
Sob a supervisão CPq/ICMC

In [8], where $A$ is the group algebra $kG$ of a finite group $G$ over $k$, with the involution that sends each element of $G$ to its inverse, we give conditions for the existence of free symmetric pairs; such pairs were also shown for some special division algebras. Conditions for the existence of free unitary pairs in $U(kG)$ were given in [10].

Here we further investigate the problem for division rings. We believe that some general form of Lichtman's Conjecture [14] should be true, namely, with few exceptions, division rings with an involution always contain free symmetric and unitary pairs.

We study involutions of the first and second kind on a division ring $D$ finite-dimensional over its center $k$. We are able to show, except for a few cases, the existence of free symmetric and unitary pairs in $D$ provided that $\mathrm{tr.deg}(k:P) > f(n)$, where $\mathrm{tr.deg}(k:P)$ stands for the transcendence degree of $k$ over its prime field $P$ and $f$ is a function of the index $n$ of $D$. In the case of involutions of the first kind the exceptions are quaternion algebras whose symmetric (or unitary) elements all commute. For involutions of the second kind, the exceptions are a little more cumbersome to describe.

In the case of free symmetric units and involutions of the first kind, we can trade the finite-dimensional hypothesis for the existence of a noncentral algebraic element, provided the center is uncountable.

One of the authors proved in [7] that every finite-dimensional division ring contained a noncommutative free group. In [15] Makar-Limanov expressed his dislike for the essential use of Tits' Alternative in that proof. No significantly different proof has appeared so far, but as a side result of our study we show that Tits' Alternative can be avoided in "almost" all cases. To be more precise, we show that if either $\mathrm{tr.deg}(k:P) > g(n)$, where $g$ is a polynomial function and $n^2$ is the dimension of $D$, or $k$ is algebraic over $P$, then $D$ contains a free pair. Moreover, if $\mathrm{tr.deg}(k:P) > g(n)+1$, then we can explicitly construct such a free pair using a method due to Chiba [4]; these pairs are essentially different from those detected in Tits' proof.

The authors are indebted to Professors D. Passman and A. Giambruno for many useful conversations.

## 1. PRELIMINARIES

If $A$ is a ring, the center of $A$ will be denoted by $Z(A)$ and the group of units of $A$ by $U(A)$. By an *involution* in $A$ one understands an additive map $*: A \longrightarrow A$ such that $(ab)^* = b^*a^*$ and $(a^*)^* = a$ for all $a, b \in A$. An element $a$ of $A$ is called *symmetric* if $a^* = a$, *antisymmetric* if $a^* = -a$, and *unitary* if $aa^* = a^*a = 1$. An involution in a simple ring $A$ is said to be of the *first kind* if every element of $Z(A)$ is symmetric, otherwise it is said to be of the *second kind*.

More generally, in an algebra over a field $k$, a *$k$-involution* is just a $k$-linear involution. A subset of $A$ is called *free* if its elements freely generate a free subgroup of $U(A)$. A free pair of symmetric (resp. unitary) elements will be called a *free symmetric* (resp. *unitary*) *pair*.

An involution $*$ on a ring $A$ induces an involution $*$ on the polynomial ring $A[t]$ such that $t^* = t$. If $A$ is simple and $F$ is a field extension of the center $k$ of $A$, then an involution $*$ of

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

the first kind on $A$ can be extended to an involution $*$ of the same kind on $A_F = A \otimes_k F$ by $(\sum_i a_i \otimes f_i)^* = \sum_i a_i^* \otimes f_i$, where $a_i \in A$ and $f_i \in F$.

If $D$ is a division ring, then $D^+$ will denote the multiplicative group of $D$, that is, $D^+ = D \setminus \{0\}$. The sets $\mathbf{N}, \mathbf{Z}, \mathbf{Q}$ will denote the natural numbers, the integers and the rational numbers, respectively. We shall use the convention that division rings are always noncommutative unless otherwise stated.

Let $D$ be a division ring with center $k$, let $n$ be a positive integer, and let $R = D_n$ be the $n \times n$ full matrix ring over $D$. Consider the polynomial ring $R[t]$. We shall make use of the following lemmas.

LEMMA 1.1 ([1, Lemma 4]). *The ring $R[t]$ has a unique ring of quotients $R(t)$ containing all elements of the form $pq^{-1}$ (and $q^{-1}p$) with $q$ a non-zero divisor of $R[t]$. Furthermore, $q$ can be chosen to be a polynomial in $D[t]$. Finally, $R(t)$ is canonically isomorphic to $D(t)_n$, where $D(t) = \{fg^{-1} : f, g \in D[t], g \neq 0\}$ is the Ore ring of quotients of $D[t]$.*

LEMMA 1.2 ([1, Lemma 5]). *Let $F = k(\alpha)$ be a finite extension of $k$ generated by a single element $\alpha$ and let $\pi_\alpha : R[t] \longrightarrow R_F$ be the homomorphism defined by $\pi_\alpha(p(t)) = p(1 \otimes \alpha)$. Then*

(i) *the set $R_\alpha(t) = \{p(t)q(t)^{-1} : \pi_\alpha(q(t))$ is regular in $R_F\}$ is a subring of the ring of quotients $R(t)$ of $R[t]$;*

(ii) *the homomorphism $\pi_\alpha$ can be extended uniquely to a homomorphism*

$$\pi_\alpha : R_\alpha(t) \longrightarrow R_F$$

*by setting*

$$\pi_\alpha(p(t)q(t)^{-1}) = p(1 \otimes \alpha)q(1 \otimes \alpha)^{-1}.$$

*Furthermore, if $r(t) \in R_\alpha(t)$ is such that $\pi_\alpha(r(t))$ is regular, then $r(t)^{-1} \in R_\alpha(t)$.*

Our aim is to prove a sort of "cancellation" property in Lemma 2.1. We start with the following two lemmas.

LEMMA 1.3. *Let $D$ be a division ring of finite dimension $n^2$ over its center $k$ and let $P$ denote the prime field of $k$. Let $X$ be a finite subset of $D$. Then $X$ is contained in a division subring $D'$ of $D$ of dimension $n^2$ over its center $k'$, a subfield of $k$ that is finitely generated over $P$. Moreover, if the cardinality of $X$ is $r$, then* $\mathrm{tr.deg}(k' : P) \leq n^3 + (r-1)n^2 + n$.

*Proof.* By the Corollary on p. 182 of [12], $D$ has a basis $B = \{\alpha^i \beta^j : i, j = 0, \ldots, n-1\}$, where $\alpha, \beta \in D$ are conjugated elements of degree $n$. Let $f(X) = a_0 + a_1 X + \cdots + a_{n-1} + X^n$ denote the minimal polynomial of $\alpha$ (and, thus, of $\beta$) over $k$. For each $j = 1, \ldots, n-1$, let $b_{jil} \in k$ be such that $\beta^j \alpha = \sum_{il} b_{jil} \alpha^i \beta^l$. Finally, for each $x_q \in X$, write $x_q = \sum_{ij} c_{qij} \alpha^i \beta^j$, with $c_{qij} \in k$. Denote by $k'$ the subfield of $k$ generated by the $a_i, b_{jil}, c_{qij}$ over $P$. It can be easily proved by induction on $i$ that $\beta^j \alpha^i \in k'$ for all $i, j = 0, \ldots, n-1$. Let $D'$ be

the linear span of $B$ over $k'$. By the way $k'$ was defined, $D'$ is a division subring of $D$, containing $X$, and its center contains $k'$. Actually, $k'$ is the center of $D'$, for a central element in $D'$ commutes with all $\alpha^i\beta^j$, hence it is central in $D$ and so its only nonzero coordinate relative to $B$ is at the basis element 1. By definition, $k'$ is finitely generated over $P$ and $\mathrm{tr.deg}(k':P) \leq n + (n-1)n^2 + rn^2 = n^3 + (r-1)n^2 + n$. □

To put things in perspective, here is a construction of a division ring that is finitely-generated over the prime field, and whose center is not finitely generated. Let $F = P(x_i : i \in \mathbf{Z}), K = F(y_i : i \in \mathbf{Z})$, where the $x_i, y_i$ are indeterminates. Let $\sigma_i$ be the $F$-automorphism of $K$ given by $\sigma_i(y_j) = x_{i+j}y_j$; let $\tau$ be the $F$-automorphism given by $\tau(y_i) = y_{i+1}$. Denote by $H$ the group generated by the $\sigma_i$ and let $G = \langle H, \tau\rangle$. It is easy to see that $\sigma_i\tau = \tau\sigma_{i+1}$ and that $G = H \rtimes \langle\tau\rangle$. Since $H$ is isomorphic to the free abelian group in $\{x_i : i \in \mathbf{Z}\}$, it follows that $G$ is orderable. Therefore, the twisted group ring $KG$ can be embedded in a division ring of twisted Malcev series; let $D$ be the division subring of that generated by $\{y_0, \sigma_0, \tau\}$. We claim that $F \subseteq Z(D)$ (it is actually equal). Indeed, it suffices to show that $F \subseteq D$, since $F$ commutes with everything in sight. Since $x_i = y_0^{-1}\sigma_i y_0 \sigma_i^{-1}$ and $\sigma_i = \tau^{-i}\sigma_0\tau^i$, the result follows.

The following is essentially present in the proof of [4, Theorem 2].

LEMMA 1.4. *Let $D$ be a division ring with center $k$ and let $D'$ be a division subring of $D$ with center $k'$. Then any subset of $k$ which is algebraically independent over $k'$ is also algebraically independent over $D'$.*

*Proof.* Let $X = \{x_i : i \in I\}$ be a subset of $k$ which is algebraically independent over $k'$ and suppose that the set $W = \{x_{i_1}^{r_1} \cdots x_{i_n}^{r_n} : n \in \mathbf{N}, i_j \in I, r_j \in \mathbf{N}\}$ is linearly dependent over $D'$. Take a minimal dependence relation holding among the elements of $W$:

$$w_0 + a_1w_1 + \cdots + a_sw_s = 0, \tag{1}$$

where $w_i \in W$ and $a_i \in D'$. Since $X$ is algebraically independent over $k'$, at least one of the $a_i$ lies outside $k'$, say $a_1$. Let $c \in D'$ be such that $a_1c - ca_1 \neq 0$. Then, taking commutators determined by $c$, the equation above gives rise to

$$(a_1c - ca_1)w_1 + \cdots + (a_sc - ca_s)w_s = 0,$$

which contradicts the minimality of (1). □

In the particular case of a singleton the lemma above guarantees that if $\lambda \in k$ is transcendental over $k'$, then it is transcendental over $D'$.

In our study of involutions, the special case of quaternion division rings must be treated separately.

Given a field $k$ of characteristic different from 2, a *quaternion algebra* is a $k$-algebra generated by two elements $\mathbf{i}, \mathbf{j}$ (called *quaternion generators*) which satisfy $\mathbf{i}^2, \mathbf{j}^2 \in k^+, \mathbf{ij} = -\mathbf{ji}$. A quaternion algebra is a central simple $k$-algebra with basis $\{1, \mathbf{i}, \mathbf{j}, \mathbf{ij}\}$.

An involution $*$ in a quaternion algebra is said to be of *type I* if any pair of quaternion generators is antisymmetric. Otherwise, it is said to be of *type II*.

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

LEMMA 1.5. *A quaternion algebra of type II contains a pair of symmetric quaternion generators.*

*Proof.* Let $H$ be a quaternion algebra over a field $k$ with an involution $*$. Let $S$ denote the set of symmetric elements in $H$. Suppose that $S \subseteq k$ and let $\mathbf{i}, \mathbf{j}$ be a pair of quaternion generators for $H$ over $k$. The following identity holds in $H$:

$$\mathbf{i}^2 - (\mathbf{i} + \mathbf{i}^*)\mathbf{i} + (\mathbf{i}^*\mathbf{i}) = 0.$$

Since $\mathbf{i}^2 \in k$ and $\mathbf{i} + \mathbf{i}^*, \mathbf{i}^*\mathbf{i} \in S \subseteq k$, it follows that $\mathbf{i}^* = -\mathbf{i}$, because $\{1, \mathbf{i}\}$ is linearly independent over $k$. The same reasoning holds for $\mathbf{j}$ and, thus, $H$ would be of type I. So there exists $u \in S \setminus k$. Let $F = k(u)$. We have $[H : F][F : k] = [H : k] = 4$. Since $F \neq k$ and $F \neq H$, it follows that $[F : k] = 2$. We can suppose that $u^2 \in S \cap k$, for if $t^2 + at + b \in k[t]$ is the minimal polynomial of $u$ over $k$, then $u$ also satisfies $t^2 + a^*t + b^*$, which is a polynomial over $k^* = k$. Therefore, $a, b \in S \cap k$. Now the element $u' = u + \frac{a}{2}$ is such that $u'^* = u'$, $k(u) = k(u')$ and $u'^2 \in S \cap k$. The mapping $u \longmapsto -u$ induces an automorphism of $F$ over $k$, so $-u = vuv^{-1}$ for some $v \in H$. Since $v \notin F$, it follows that $\{1, u, v, uv\}$ is a basis for $H$ over $k$ and hence $v^2 \in k$. If $v^* = -v$, then $\{u, uv\}$ is a pair of symmetric generators. Otherwise, $\{u, v + v^*\}$ is a pair of symmetric generators. Hence, $H$ is of type II. □

The next result gives a characterization of quaternion division rings containing free symmetric and unitary pairs.

LEMMA 1.6. *Let $H$ be a quaternion division ring over a field $k$ of characteristic different from 2 and let $*$ be an involution in $H$.*

(i) *If $H$ is of type I and $*$ is of the first kind, then it contains a free unitary pair, but does not contain free symmetric pairs.*

(ii) *If $H$ is of type II and $*$ is of the first kind, then $H$ contains a free symmetric pair, but does not contain free unitary pairs.*

(iii) *If $*$ is of the second kind, then $H$ contains both free symmetric and unitary pairs.*

*Proof.* Suppose that $H$ is of type I and that $*$ is of the first kind. Given $x \in H$, let $N(x) = xx^*$. Then $N(x) \in k$, $N(x) = 0$ if and only if $x = 0$, and $N(xy) = N(x)N(y)$ for all $x, y \in H$. Therefore, $N : H^+ \longrightarrow k^+$ is a group homomorphism. Let $H' = \ker(N)$. By [7], any noncentral normal subgroup of $H^+$ contains a free subgroup. Since $H'$ is formed by unitary elements, part (i) is proved.

Now suppose that $H$ is of type II and that $*$ is of the first kind. By Lemma 1.5, $H$ contains a pair $\mathbf{i}, \mathbf{j}$ of quaternion generators such that $\mathbf{i}^* = \mathbf{i}$ and $\mathbf{j}^* = \mathbf{j}$. In this case, it is not difficult to see that unitary elements commute, so there are no free unitary pairs in $H^+$. Let $F$ be the subfield of $k$ generated by $\mathbf{i}^2$ and $\mathbf{j}^2$ over the prime field of $k$. Observe that $F$ can be regarded as the field of fractions of a Dedekind domain $A \neq F$. Set $L = F(\mathbf{i})$ and let $\sigma$ be the $F$-automorphism of $L$ induced by the map $\mathbf{i} \longmapsto -\mathbf{i}$. The quaternion algebra $Q$ over $F$ with quaternion generators $\mathbf{i}, \mathbf{j}$ can be regarded as a crossed product with basis $\{1, \mathbf{j}\}$, coefficients in $L$ and group of automorphisms $\langle\sigma\rangle$ acting on $L$. Also, $L^* = L$ and $Q$

is not of "quaternion type" as defined in [8]. By [8, Theorem 4], $Q^+ \subseteq H^+$ contains a free symmetric pair. This proves part (ii).

Finally, if $*$ is of the second kind, then $H$ must be of type II, for there exists $\theta \in k$ such that $\theta^* = -\theta$ and if $H$ were of type I we would have $(\theta\mathbf{i})^* = \mathbf{i}^*\theta^* = \theta\mathbf{i}$ for any element $\mathbf{i}$ of a pair of quaternion generators. This would imply that $\theta\mathbf{i} \in k$, which is an absurd, for $\mathbf{i} \notin k$. So let $\mathbf{i}, \mathbf{j}$ be a pair of symmetric quaternion generators for $H$ and consider the quaternion algebra $Q_1$ over the subfield $F$ of $k$ left fixed by $*$ generated by $\mathbf{i}, \mathbf{j}$. By part (ii), $Q_1^+ \subseteq H^+$ contains free symmetric pairs. Let $Q_2$ be the quaternion algebra over $F$ generated by $\theta\mathbf{i}, \theta\mathbf{j}$. By part (i), $Q_2^+ \subseteq H^+$ contains free unitary pairs. □

## 2. INVOLUTIONS OF THE FIRST KIND

In this section, we treat the case of involutions of the first kind.

The following result was inspired by [17, Proposition 3].

LEMMA 2.1. *Let $D$ be a division ring of finite dimension $s^2$ over its center $k$, and let $P$ denote the prime field of $k$. Let $n$ be a positive integer and let $R = D_n$. Suppose that $R(t)$ contains a free pair $\{u(t), v(t)\}$. Then there exists a positive integer $N = N(s, n, u, v)$ such that if $\mathrm{tr.deg}(k : P) > N$, then $R$ contains a free pair of the form $\{u(\lambda), v(\lambda)\}$, for some $\lambda \in k$. Moreover, if $R$ has an involution and the free pair in $R(t)$ is formed by symmetric (resp. unitary) elements under the induced involution, then the free pair in $R$ is also symmetric (resp. unitary).*

*Proof.* Suppose that $u(t) = G(t)h(t)^{-1}$, $v(t) = L(t)m(t)^{-1}$, with $G(t)$, $L(t) \in R[t]$ and $h(t), m(t) \in D[t]$, $h(t) \neq 0$, $m(t) \neq 0$, and that $r$ is the highest degree occurring among the polynomials $h(t), m(t)$ and the entries of $G(t)$ and of $H(t)$. Let $X$ be the set formed by the coefficients of $h(t), m(t)$ and the coefficients of the entries of $G(t)$ and of $L(t)$. By assumption, $X$ contains at most $(2n^2+2)(r+1)$ elements. By Lemma 1.3, $X$ is contained in a division subring $D'$ of $D$ with center $k'$ and such that $\mathrm{tr.deg}(k' : P) \leq N$, where $N = s^3 + ((2n^2+2)(r+1) - 1)s^2 + s$. If $\mathrm{tr.deg}(k : P) > N$, there exists a $\lambda \in k$ which is transcendental over $k'$ and, by Lemma 1.4, transcendental over $D'$. Hence, $D'(t) \cong D'(\lambda) \subseteq D$. Therefore, $u(\lambda), v(\lambda)$ freely generate a free subgroup of $D'(\lambda)_n \subseteq R$.

The last assertion is clear, because the involution in $R(t)$ fixes $t$ and the involution in $R$ fixes a subfield $k_*$ of the field of central elements $k$ which is such that $[k : k_*] \leq 2$. □

We now show that full matrix rings over fields contain free symmetric and unitary pairs. Recall that a field is called *nonabsolute* if it is not an algebraic extension of a finite field.

LEMMA 2.2. *Let $F$ be a field of characteristic different from 2 and let $P$ denote the prime field of $F$. Let $*$ be an involution of the first kind on $R = M_n(F)$, where $n > 2$. Then, there exits a positive integer $N = N(n)$ such that if $\mathrm{tr.deg}(F : P) > N$, then $U(R)$ contains free symmetric and unitary pairs.*

*Proof.* As we can see from the proofs of [2, Lemma 4.6.10, Theorem 4.6.12], by a Gram-Schmidt process, if $F$ contains square roots of suitable elements $\alpha_1, \ldots, \alpha_n$, then $*$ can be regarded as being either the transpose or the symplectic involution. Let $L$ be an extension

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

of $F$ over which the $\alpha_i$ have square roots. In $M_n(L) \cong M_n(F) \otimes_F L$ the induced involution $(\sum a_i \otimes l_i)^* = \sum a_i^* \otimes l_i$ can be regarded as being either the transpose or the symplectic involution.

If we find a positive integer $N$ such that $\mathrm{tr.deg}(F:P) > N$, then $L$ will be a nonabsolute field. In this case, if $*$ is the transpose and $n \geq 3$, then $M_n(L)$ contains a free unitary pair, by [10, Lemma 2.5]. Moreover, it is known that $M_n(L)$ contains free symmetric pairs if $n \geq 2$ and $*$ is the transpose (cf. Lemma 2.5).

Let us assume that $*$ is the symplectic involution. Then $n = 2m$, for $m > 1$ and we have

$$\begin{pmatrix} A & 0 \\ 0 & D \end{pmatrix}^* = \begin{pmatrix} D^t & 0 \\ 0 & A^t \end{pmatrix}.$$

So $\left(\begin{smallmatrix} A & 0 \\ 0 & D \end{smallmatrix}\right)$ is symmetric if and only if $D = A^t$. Clearly there are free pairs of elements of the form $\left(\begin{smallmatrix} A & 0 \\ 0 & A^t \end{smallmatrix}\right)$ in $M_n(L)$. Now let us look for unitary matrices in the symplectic case. We have

$$\begin{pmatrix} A & 0 \\ 0 & D \end{pmatrix}^* = \begin{pmatrix} A^{-1} & 0 \\ 0 & D^{-1} \end{pmatrix}$$

if and only if $A^{-1} = D^t$, or $D = (A^{-1})^t$. Thus a typical "diagonal" unitary matrix will be of the form

$$\begin{pmatrix} A & 0 \\ 0 & (A^{-1})^t \end{pmatrix}.$$

We can certainly find free pairs of matrices of this form in $M_n(L)$.

Since $L$ is a finite separable extension of $F$, it contains a primitive element $\alpha$; so $L = F(\alpha)$. Let $R_L = R \otimes_F L$. Define $\pi_\alpha : R[t] \longrightarrow R_L$ by $\pi_\alpha(p(t)) = p(1 \otimes \alpha)$ and extend $*$ to $R[t]$ and to $R_L$ by defining $t^* = t$ and $\alpha^* = \alpha$, respectively. By Lemma 1.2, the set

$$R_\alpha(t) = \{p(t)q(t)^{-1} : p(t), q(t) \in R[t] \text{ and } q(1 \otimes \alpha) \text{ is regular in } R_L\}$$

is a subring of the ring of quotients $R(t)$ of $R[t]$, and $\pi_\alpha$ can be extended uniquely to a homomorphism $\pi_\alpha : R_\alpha(t) \longrightarrow R_L$, setting $\pi_\alpha(p(t)q(t)^{-1}) = p(1 \otimes \alpha)q(1 \otimes \alpha)^{-1}$. Furthermore, $\pi_\alpha^{-1}(U(R_L)) \subseteq U(R_\alpha(t))$.

The set $\{1 \otimes 1, 1 \otimes \alpha, \ldots, 1 \otimes \alpha^{s-1}\}$, where $s = [L : F]$, is a basis for $R_L$ as a left $R$-module. By definition of $*$ in $R_L$, if $x = \sum_{i=0}^{s-1} r_i \otimes \alpha^i$, with $r_i \in R$, then $x^* = \sum_{i=0}^{s-1} r_i^* \otimes \alpha^i$. So $x$ is symmetric if and only if $r_i^* = r_i$, for all $i$. Let $p(t) = \sum_{i=0}^{s-1} r_i t^i$; so $\pi_\alpha(p(t)) = x$. We have seen that $x$ is symmetric if and only if $p(t)$ is symmetric. Thus, we can always choose pre-images of symmetric elements under $\pi_\alpha$ that are symmetric, and the same holds for antisymmetric elements. So if we have a free symmetric pair on the right, it can be lifted to a free symmetric pair on the left. If $\{z, w\}$ is a free pair of unitary matrices in $M_n(L)$, then $\{z^2, w^2\}$ is a free pair of unitary matrices of determinant 1 (see [5, Corollary 2]). In [5, Theorem 2] it is proved that a unitary element of $M_n(L)$ of determinant 1 is a product of two Cayley unitary units, that is, of invertible matrices the form $(1 - y)(1 + y)^{-1}$, for some antisymmetric matrix $y$. Therefore, since we can lift antisymmetric elements through $\pi_\alpha$, we can lift Cayley unitary units and, hence, we can lift unitary units.

In other words, we can always produce a free symmetric pair in $R(t)$ whose elements are polynomials of $R[t]$ of degree at most $s-1$, and we can always produce a 4-element set of polynomials of degree at most $s-1$ which give rise to a free unitary pair in $R(t)$. By Lemma 2.1, there exists a positive integer $N$ such that if $\mathrm{tr.deg}(F:P) > N$, then these free pairs can be pulled down to $R$ by the substitution of $t$ by a convenient element $\lambda$ of $F$. Since, as we have seen in the proof of Lemma 2.1, $N$ depends only on the degrees of the polynomials involved and these are bounded by $s-1 < s = [L:F] \leq 2^n$, we can find a bound $N$ which depends only on $n$. □

We are ready to prove the first main result of this section.

THEOREM 2.1. *Let $D$ be a division ring of finite dimension $d$ over its center $k$ of characteristic different from 2 and let $P$ denote the prime field of $k$. Suppose that $D$ has an involution of the first kind. Then*

(i) *if $d = 4$, then $D$ contains a free symmetric pair if and only if it is not a quaternion algebra of type I and $D$ contains a free unitary pair if and only if it is not a quaternion algebra of type II;*
(ii) *if $d > 4$, then there exists a positive integer $N = N(d)$ such that if $\mathrm{tr.deg}(k:P) > N$, then $D$ contains both free symmetric and free unitary pairs.*

*Proof.* Part (i) follows from Lemma 1.6. Assume, now that $d > 4$ and let $F$ be a maximal subfield of $D$ generated by an element $\alpha$ over $k$. Let us extend the involution $*$ of $D$ to $D[t]$ by $t^* = t$, and to $D_F = D \otimes_k F$ by $(\sum_i d_i \otimes f_i)^* = \sum_i d_i^* \otimes f_i$. Let $\pi_\alpha : D[t] \longrightarrow D_F$ be the map defined by $\pi_\alpha(p(t)) = p(1 \otimes \alpha)$. Note that $\pi_\alpha$ is a homomorphism of rings with involution. Since $F$ is a maximal subfield of $D$, $D_F \cong M_n(F)$, where $n^2 = d$. Apply, now, Lemma 2.2 to $M_n(F)$, lift symmetric and antisymmetric units to $D_\alpha(t)$, as in the proof of Lemma 2.2, and apply Lemma 2.1. □

This result remains valid if $D$ is taken to be locally finite.

COROLLARY 2.1. *Let $D$ be a division ring which is locally finite over its center $k$ of characteristic different from 2 and let $P$ denote the prime field of $k$. Let $*$ be an involution of the first kind in $D$. Then if $D$ is not a quaternion algebra there exists a positive integer $N$ such that if $\mathrm{tr.deg}(k:P) > N$, then $D$ contains both free symmetric and free unitary pairs.*

*Proof.* If $D$ is not a quaternion algebra over $k$, take five elements $a_1, a_2, a_3, a_4, a_5$ which are linearly independent over $k$. Let $D'$ be the division subring of $D$ generated by $\{a_i, a_i^* : i = 1, \ldots, 5\}$. Since $(D')^* \subseteq D'$ and $D$ is locally finite, we can apply Theorem 2.1 to $D'$ in order to obtain the desired result. □

We observe that the bound $N$ in the above corollary depends on $[D' : Z(D')]$ and, so, depends on the choice of the $a_i$.

Theorem 2.1 remains valid in the symmetric case if we allow $D$ to be a division ring not necessarily finite-dimensional, provided that it contains a noncentral algebraic element over $k$ and that $k$ is uncountable.

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

We start with the following well-known consequence of a theorem of Kaplansky ([2, Theorem 4.6.8]).

LEMMA 2.3. *Let $D$ be a division ring with center $k$ and let $n$ be a positive integer. Suppose that $M_n(D)$ has an involution $*$. Then one of the following holds.*

(i) *$*$ is of the transpose type. In this case, $*$ restricts to an involution $a \mapsto \overline{a}$ in $D$ and there exists a diagonal matrix $C = \mathrm{diag}\{c_1, \ldots, c_n\}$, where $c_i \in D$ with $\overline{c_i} = c_i$, such that, for all $A \in M_n(D)$,*

$$A^* = C\overline{A}^t C^{-1}, \tag{2}$$

*where, if $A = (a_{ij})$, $\overline{A} = (\overline{a_{ij}})$ and $\overline{A}^t$ stands for the usual transpose of $\overline{A}$, or*

(ii) *$*$ is of the symplectic type. In this case, $D = k$ is commutative, $n = 2m$ is even, and if $A, B, C, D \in M_m(k)$, the involution $*$ is given by the rule*

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix}^* = \begin{pmatrix} D^t & -B^t \\ -C^t & A^t \end{pmatrix}, \tag{3}$$

*where again $t$ stands for the usual transpose.*

We shall need a result similar in content to Lemma 2.2 for the infinite-dimensional case. Before we state such a result, we state a variation of [9, Lemma] which can be proved in exactly the same way.

LEMMA 2.4. *Let $A$ be an algebra over a field $k$ of positive characteristic $p$. Suppose that $A$ contains elements $a$ and $b$ such that $a^2 = b^2 = 0$ and $ba$ is not nilpotent. Let $f, g \in k[t]$ be arbitrary nonzero polynomials. Then the elements $x = 1 + fta$ and $y = 1 + gtbab$ are units of order $p$ in $A[t]$ and $\langle x, y\rangle \cong \langle x\rangle * \langle y\rangle$.*

The following is an improved version of Lemma 2.2 for the symmetric case.

LEMMA 2.5. *Let $D$ be a division ring (commutative or not) with a nonabsolute centre $k$ of characteristic different from 2. Let $n$ be a positive integer and let $*$ be an involution of $M_n(D)$, where $n \geq 2$. Then, unless $n = 2$ and $*$ is the symplectic involution, $GL_n(D)$ contains an element $x$ such that $\{xx^*, x^*x\}$ is a free pair.*

*Proof.* Suppose first that $*$ is of the transpose type. By Lemma 2.3, $*$ restricts to an involution $a \longmapsto \overline{a}$ in $D$ and there exists a diagonal matrix $C = \mathrm{diag}\{c_1, \ldots, c_n\}$, where $c_i \in D$ with $\overline{c_i} = c_i$, and $*$ is given by (2). It is enough to consider the case $n = 2$. Indeed, if $n > 2$, then, by means of the embedding of $M_2(D)$ into $M_n(D)$ given by

$$A \longmapsto \begin{pmatrix} A & 0 \\ 0 & I_{n-2} \end{pmatrix},$$

an involution of the transpose type in $M_n(D)$ restricts to an involution of the same type in $M_2(D)$. Thus, we can suppose that $n = 2$. In this case, we have

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^* = \begin{pmatrix} c_1 & 0 \\ 0 & c_2 \end{pmatrix} \begin{pmatrix} \overline{a} & \overline{c} \\ \overline{b} & \overline{d} \end{pmatrix} \begin{pmatrix} c_1^{-1} & 0 \\ 0 & c_2^{-1} \end{pmatrix} = \begin{pmatrix} c_1\overline{a}c_1^{-1} & c_1\overline{c}c_2^{-1} \\ c_2\overline{b}c_1^{-1} & c_2\overline{d}c_2^{-1} \end{pmatrix}.$$

Let us put $z = c_1c_2^{-1}$ and note that $\overline{z} = c_2^{-1}c_1$. We consider now two cases.

(i) $\mathrm{char}(k) = 0$: Let $F = \mathbf{Q}(z)$ be the subfield of $k$ generated by $z$ over $\mathbf{Q}$. We can then regard $F$ as a subfield of the complex numbers. Choose $r \in \mathbf{Q}$ large enough so that $|zr^2| \geq 2$, $|zr^2 - 2| \geq 2$, $|zr^2 + 2| \geq 2$. Then, by [3],

$$x = \begin{pmatrix} 1 & zr \\ 0 & 1 \end{pmatrix}, \quad y = \begin{pmatrix} 1 & 0 \\ r & 1 \end{pmatrix}$$

is a free pair which is switched by $*$. Hence $\{xy, yx\}$ is also a free pair.

(ii) $\mathrm{char}(k) > 0$: Let $GF(p)$ be the prime field of $k$. If $z$ is transcendental over $GF(p)$, let

$$x = \begin{pmatrix} 1 & z^2 \\ 0 & 1 \end{pmatrix}, \quad y = \begin{pmatrix} 1 & 0 \\ z & 1 \end{pmatrix} \in M_2(k).$$

If $z$ is algebraic over $GF(p)$, let $\zeta$ be an element of $k$ that is transcendental over $GF(p)$ and define

$$x = \begin{pmatrix} 1 & z\zeta \\ 0 & 1 \end{pmatrix}, \quad y = \begin{pmatrix} 1 & 0 \\ \zeta & 1 \end{pmatrix}.$$

In both cases, by Lemma 2.4, $x$ and $y$ are units of order $p$ such that $\langle x, y\rangle \cong \langle x\rangle * \langle y\rangle$ and, clearly, $x^* = y$. It is now easy to see that $\{xy, yx\}$ is a free pair.

Suppose now that $*$ is symplectic. Then, by Lemma 2.3, $D = k$ is a field, $n = 2m$ is even, and $*$ is given by (3). If $n = 2$, it is easily seen that, since $\mathrm{char}(k) \neq 2$, a symmetric element is a scalar matrix and so is central. If $n > 2$, then $m$ is at least 2 and so, using the result for the transpose type with $z = 1$, one can find a matrix $A \in GL_m(k)$ such that $AA^t$ and $A^tA$ form a free pair. The matrix

$$x = \begin{pmatrix} A & 0 \\ 0 & A \end{pmatrix}$$

is then an element satisfying the lemma. □

The method of proof used in our next result (Theorem 2.2) is similar to the one used in the proof Theorem 2.1, that is to say, we shall lift a free group from a matrix ring and then apply a cancellation argument provided by the lemma below.

LEMMA 2.6. *Let $D$ be a division ring with an uncountable center $k$. Let $n$ be a positive integer and let $R = D_n$. Suppose that $R(t)$ contains a free pair $\{u(t), v(t)\}$. Then $R$ contains a free pair of the form $\{u(\lambda), v(\lambda)\}$, for some $\lambda \in k$.*

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

*Moreover, if $R$ has an involution and the free pair in $R(t)$ is formed by symmetric elements under the induced involution, then the free pair in $R$ is also symmetric.*

*Proof.* Again write $u(t) = G(t)h(t)^{-1}$, $v(t) = L(t)m(t)^{-1}$, with $G(t)$, $L(t) \in R[t]$ and $h(t), m(t) \in D[t]$, $h(t) \neq 0$, $m(t) \neq 0$. Since $u(t)$ and $v(t)$ are units, $G(t)$ and $L(t)$ are non-zero divisors in $R[t]$. For each nontrivial element $\omega(x, y)$ of the free group $F_2$ freely generated by $x, y$, choose $P_\omega(t) \in R[t], q_\omega(t) \in D[t], q_\omega(t) \neq 0$, such that

$$\omega(u(t), v(t)) = P_\omega(t)q_\omega(t)^{-1}.$$

Now, if $P(t) = (p_{ij}(t)) \in D[t]_n$ and $q(t) \in D[t]$ are such that, for some $\lambda \in k$, $P(\lambda)q(\lambda)^{-1} = I_n$, then, in particular, $p_{11}(\lambda) = q(\lambda)$. Thus, if $\lambda$ is not a root of $p_{11}(t) - q(t)$, then $P(\lambda)q(\lambda)^{-1} \neq I_n$.

Recall that given a nonzero polynomial $f(t) \in D[t]$, the set $X_f = \{\lambda \in k : f(\lambda) = 0\}$ of roots of $f$ lying in $k$ is finite (see, *e. g.*, [13, Theorem 16.4]). This implies that given a non-zero divisor $P(t) \in R[t]$, the set $X_P = \{\lambda \in k : P(\lambda)$ is a zero divisor in $D_n\}$ is also finite.

For each $\omega \in F_2$, write $P_\omega = (p_{ij}^\omega)$, with $p_{ij}^\omega \in D[t]$. Since the free group $F_2$ is countable, the set

$$X = \bigcup_{\omega \in F_2} (X_{P_\omega} \cup X_{q_w} \cup X_{p_{11}^\omega - q_\omega}) \cup X_G \cup X_h \cup X_L \cup X_m$$

is at most countable. Since $k$ is uncountable, there must exist $\lambda \in k \setminus X$. For this $\lambda$, $\omega(u(\lambda), v(\lambda)) \neq 1$ for all $\omega \in F_2$. In other words, $u(\lambda), v(\lambda)$ form a free pair in $R$.

If $R$ has an involution, we can choose, as in the proof of Lemma 2.1, a $\lambda \in k$ which is left fixed by the involution. □

We are ready to prove the following theorem.

THEOREM 2.2. *Let $D$ be a division ring with an involution $*$ of the first kind. Suppose that the center $k$ of $D$ is uncountable and has characteristic different from 2. Assume that $D$ contains a noncentral algebraic element $\alpha$ over $k$ and that $D$ is not a quaternion division algebra of type I. Then $D$ contains a free symmetric pair.*

*Proof.* Let $F = k(\alpha)$ and let

$$\pi_\alpha : D[t] \longrightarrow D_F$$

be the homomorphism given by $\pi_\alpha(p(t)) = p(1 \otimes \alpha)$. Extend the involution $*$ of $D$ to $D[t]$ and to $D_F$ in the natural way, so that $\pi_\alpha$ is a homomorphism of rings with involution. Since $\alpha$ is algebraic over $k$, $D_F \cong M_n(E)$ for some division ring $E$ with center $F$ and $n \geq 2$ is the degree of the minimal polynomial of $\alpha$ over $k$ (see [6, Exercise 3.4.11]). By Lemma 1.2, $\pi_\alpha$ extends to a homomorphism with domain $D_\alpha(t)$ such that $\pi_\alpha^{-1}(U(D_F)) \subseteq U(D_\alpha(t))$. Now $*$ is an involution of $M_n(E)$. If $n = 2$ and $E = F$ is commutative, $[D : k] = 4$ and, by hypothesis, the induced involution in $M_n(E)$ is not symplectic. Therefore, by Lemma 2.5, there exists an element $x \in GL_n(E)$ such that $\{xx^*, x^*x\}$ is a free pair. Choose $f \in D_\alpha(t)$ such that $\pi_\alpha(f) = x$. Then $\{ff^*, f^*f\}$ is a free symmetric pair in $D(t)$.

Publicado pelo ICMC-USP
Sob a supervisão CPq/ICMC

We know evoke Lemma 2.6, to guarantee the existence of a free symmetric pair in $D$. □

Recall that a division ring $D$ with an uncountable center $k$ which is finitely generated as $k$-algebra is always algebraic over $k$ (see [6, Exercise 3.4.16]). With this fact in hand we obtain the following consequence of Theorem 2.2.

COROLLARY 2.2. *Let $D$ be a division ring with an involution of the first kind. Suppose that the center $k$ of $D$ is uncountable of characteristic different from 2, and that $D$ is finitely generated as a $k$-algebra. Then unless $D$ is a quaternion algebra of type I it contains a free symmetric pair.* □

Lemma 2.5 has another interesting consequence.

THEOREM 2.3. *Let $R$ be a primitive $k$-algebra with nonzero socle. Suppose that $k$ is a nonabsolute field of characteristic different from 2 and that $R$ is endowed with a $k$-involution $*$. Then $U(R)$ contains a free symmetric subgroup, unless $R$ is a full $2 \times 2$ matrix ring over a field extension of $k$ and $*$ is the symplectic involution.*

*Proof.* If $R \cong M_n(D)$, where $D$ is a division ring, then, by Lemma 2.5, the claim is true. If the above is not the case, we take $n > 3$ and, by Litoff's Theorem (see [2, 4.6.15]), there exists a symmetric idempotent $e$ such that $eRe \cong M_n(D)$, where $D$ is the associated division ring of $R$. Since $e$ is symmetric, $M_n(D)$ is stable under $*$. By Lemma 2.5, $M_n(D)$ contains a free symmetric subgroup which embeds in $U(R)$ via $x \longmapsto (1-e) + xe$. □

## 3. INVOLUTIONS OF THE SECOND KIND

Some of what has been proved for involutions of the first kind in Section 2 can be established for general involutions (cf. Theorem 3.1). In this section we restrict our attention to free symmetric pairs.

The following is a version of Theorem 2.2 for a general involution.

THEOREM 3.1. *Let $D$ be a division ring with center $k$ of characteristic different from 2. Suppose that $k$ is uncountable. Let $*$ be an involution in $D$. Assume that $D$ is not a quaternion algebra of type I and that it contains a noncentral symmetric algebraic element over $k$. Then $D$ contains a free symmetric pair.*

The above can be proved in the same way as Theorem 2.2, using a noncentral symmetric algebraic element $\alpha$ as the generator for the scalar extension and extending $*$ to $D \otimes k(\alpha)$ by $(\sum_i d_i \otimes \alpha^i)^* = \sum_i d_i^* \otimes \alpha^i$.

In order to obtain a version of Theorem 2.1 for general involutions, we shall first prove that a finite-dimensional division ring with involution has a maximal subfield generated by a symmetric element. This is the contents of Theorem 3.2 below. For its proof we shall make use of the following involutional version of the Jacobson-Noether Theorem, due to Chacron.

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

LEMMA 3.1 ([11, Lemma 3.2.1]). *Let $D$ be a division ring with involution, of characteristic different from 2, and denote the set of symmetric elements of $D$ by $S$. Suppose that every element of $S$ is algebraic over the center $k$ of $D$. Then either $S \subseteq k$ (and, so $[D : k] \leq 4$) or there exist separable symmetric elements which are not central.*

THEOREM 3.2. *Let $D$ be a division ring finite-dimensional over its center $k$ of characteristic different from 2. Let $*$ be an involution in $D$. Then, if it does not contain quaternion algebras which are invariant under $*$, $D$ has a maximal subfield which is generated by a separable symmetric element.*

*Proof.* Let $S$ denote the set of symmetric elements in $D$. Since $D$ is not a quaternion algebra, if follows from Lemma 3.1 that $S \setminus k$ contains separable elements. Among all $x \in S \setminus k$ that are separable choose one such that $[k(x) : k]$ is maximal. We claim that $F = k(x)$ is a maximal subfield of $D$. We shall show that $F = C_D(F)$. Since $F$ is commutative, it follows that $F \subseteq C_D(F)$. Moreover, since $F$ is simple and finite-dimensional over $k$, it follows that $F = C_D(C_D(F))$. Thus, $F$ coincides with the center of $C_D(F)$. The involution $*$ of $D$ restricts to an involution of the division subring $C_D(F)$, because if $y \in C_D(F)$, then $y^*x = (x^*y)^* = (xy)^* = x^*y^* = xy^*$. If $[C_D(F) : F] > 1$, since $D$ does not contain $*$-invariant quaternion algebras, we would have, by Lemma 3.1, a symmetric element $z \in C_D(F) \setminus F$ separable over $F$. But then we would have produced a separable extension $k(x, z)$ of $k$ of degree strictly larger then $[k(x) : k]$. Since $k$ is infinite, by the construction of primitive elements in separable extensions, $k(x, y)$ would be generated by a separable symmetric element, which is a contradiction. This proves the theorem. □

THEOREM 3.3. *Let $D$ be a division ring of finite dimension $d$ over its center $k$ of characteristic different from 2. Let $P$ denote the prime field of $k$. Let $*$ be an involution in $D$. Assume that $D$ does not contain quaternion algebras which are invariant under $*$. Then there exists a positive integer $N$ such that if* $\mathrm{tr.deg}(k : P) > N$, *then $D$ contains a free symmetric pair.*

*Proof.* Since $D$ does not contain quaternion algebras which are invariant under $*$, by Theorem 3.2, it contains a maximal subfield $F$ generated by a symmetric element $\alpha$. Now proceed as in the proof of Theorem 2.1, use Lemma 2.5 to guarantee the existence of a free symmetric pair in $M_n(F)$, and, when using Lemma 2.1 to descend from $D(t)$ to $D$, be careful to choose a symmetric element $\lambda \in k$ which is transcendental over $P$. This last choice is always possible, because $k$ is an extension of degree at most 2 of the field $k_* = \{\lambda \in k : \lambda^* = \lambda\}$. □

## 4. FREE SUBGROUPS OF DIVISION RINGS

As remarked in the Introduction, the techniques developed in this paper provide us with a method of proof of the existence of free groups in the group of units of a finite-dimensional division ring which avoids the use of Tits' Alternative in "almost" all cases. We shall see how this is done in the following.

THEOREM 4.1. *Let $D$ be a division ring of finite dimension $n^2$ over its center $k$ and let $P$ denote the prime field of $k$. If either every element of $k$ is algebraic over $P$ or* $\mathrm{tr.deg}(k:P) \geq n^3+n^2+n+1$, *then $D^+$ contains a noncyclic free group.*

*Proof.* Start by choosing two elements $a, b \in D$ such that $ab \neq ba$. By Lemma 1.3, there exists a division subring $D'$ of $D$ containing $a$ and $b$ of dimension $n^2$ over its center $k'$, a subfield of $k$ finitely generated over $P$.

If every element of $k$ is algebraic over $P$, then $P$ is isomorphic to $\mathbf{Q}$ and so $k'$ is an algebraic number field. By the Albert-Brauer-Hasse-Noether Theorem (see [16, Theorem 18.6]), $D'$ is a crossed product and therefore, by [8, Theorem 2], it must contain a free subgroup.

On the other hand, if $\mathrm{tr.deg}(k:P) \geq n^3+n^2+n+1$, let $F'$ be a maximal subfield of $D'$ generated by an element $\alpha$ over $k'$. Consider the map $\pi_\alpha : D'[t] \longrightarrow D' \otimes_{k'} F'$ defined by $\pi_\alpha(p(t)) = p(1 \otimes \alpha)$. Now $D' \otimes_{k'} F' \cong M_n(F')$, and it is well-known that $M_n(F')$ contains free groups which can be lifted to $D'(t)$ via $\pi_\alpha$. By Lemma 1.3, $\mathrm{tr.deg}(k':P) \leq n^3+n^2+n$ and, so, there is a transcendental in $k$ left and we can apply Lemma 1.4 to obtain the desired result. □

In fact, if the center $k$ of $D$ contains still one more transcendental element over $P$ we are able to exhibit free generators for the free group. We shall do this using a construction of Chiba [4]. Here one should notice a large difference from the previous proof and that in [7]. Both in Tits' theorem and in [8], the free pairs obtained arrive from matrices of hyperbolic type. In the proof below, the free pairs are of parabolic matrices.

THEOREM 4.2. *Let $D$ be a division ring of finite dimension $n^2$ over its center $k$ and let $P$ denote the prime field of $k$. Let $a, b \in D$ be such that $[a,b] = ab - ba \neq 0$. Let $D_0 = P(a,b)$ be the division subring of $D$ generated by $a$ and $b$ over $P$. If* $\mathrm{tr.deg}(k:P) \geq n^3+n^2+n+2$, *then $k$ contains two elements $x, y$ which are algebraically independent over $D_0$. In particular, letting $d_{12} = [a,b]^{-1}(a-x)$ and $d_{21} = -b^2[a,b]^{-1}(bab^{-1}-x)$, we have the following:*

(i) *if* $\mathrm{char}(P) = 0$, *then $z_1 = 1 + yd_{12}$ and $z_2 = 1 + yd_{21}$, freely generate a free subgroup of $D^+$, and*

(ii) *if* $\mathrm{char}(P) = p > 0$, *then the subgroup of $D^+$ generated by $w_1 = 1 + yd_{12}, w_2 = 1+yd_{21}d_{12}d_{21}$ and $w_3 = 1+y(1-d_{21})d_{12}d_{21}d_{12}(1+d_{21})$ is the free product $\langle w_1\rangle * \langle w_2\rangle * \langle w_3\rangle$.*

*Proof.* Let $D'$ be the division subring of $D$ with center $k'$ containing $X = \{a, b\}$ constructed in the proof of Lemma 1.3, and let $D''$ be the division subring of $D$ generated by $X$ over $k'$. Since $D'$ is finite-dimensional over $k'$, so is $D''$ and, *a fortiori*, so is its center $k''$. Let $k_0$ denote the center of $D_0$. Then, since $k_0 \subseteq k''$, $\mathrm{tr.deg}(k_0 : P) \leq \mathrm{tr.deg}(k'' : P) = \mathrm{tr.deg}(k' : P) \leq n^3+n^2+n$. Hence $k$ contains two elements $x$ and $y$ that are algebraically independent over the center $k_0$ of $D_0$. By Lemma 1.4, they are also algebraically independent over $D_0$. Now $D_0$ is a left $D_0[x]$-module via

$$\Big(\sum_i d_i x^i\Big) \cdot u = \sum_i dua^i,$$

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

for $d_i, u \in D_0$. Let $M = k_0 + bk_0$ be the right $k_0$-subspace of $D_0$ generated by the $k_0$-linearly independent elements 1 and $b$. Denote by $R = k_0\langle d_{12}, d_{21}\rangle$ the $k_0$-subalgebra of $D_0[x]$ generated by $d_{12}$ and $d_{21}$. So $D_0$ is a left $R$-module. Now $d_{12} \cdot u = [a,b]^{-1}(au - ua)$, so $d_{12} \cdot 1 = 0$ and $d_{12} \cdot b = 1$. Also, $d_{21} \cdot u = -b^2[a,b]^{-1}(bab^{-1}u - ua)$, so $d_{21} \cdot 1 = b$ and $d_{21} \cdot b = 0$. This proves that $R \cdot M \subseteq M$, therefore, $M$ is an $(R, k_0)$-bimodule. This action induces a ring homomorphism

$$\varphi : R \longrightarrow \mathrm{End}_{k_0}(M) \cong M_2(k_0),$$

given by $\varphi(r)(m) = r \cdot m$. And, as we have seen,

$$\varphi(d_{12}) = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \quad \text{and} \quad \varphi(d_{21}) = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}.$$

Now, extend $\varphi$ to

$$\overline{\varphi} : R[[y]] \longrightarrow M_2(k_0)[[y]] \cong M_2(k_0[[y]]),$$

where $R[[y]]$ stands for the power series ring of $R$ over $y$, and similarly for $M_2(k_0)[[y]]$. Since both in characteristic 0 and $p$ the elements $z_1, z_2, w_1, w_2, w_3$ are invertible in $R[[y]]$, it follows that the subgroups of $D^+$ they generate are contained in $R[[y]]$. It is well-known that if $\mathrm{char}(k_0) = 0$, then

$$\overline{\varphi}(z_1) = \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \overline{\varphi}(z_2) = \begin{pmatrix} 1 & 0 \\ y & 1 \end{pmatrix}$$

freely generate a free group in $M_2(k_0[y])$. So, $\langle z_1, z_2\rangle$ is free on $\{z_1, z_2\}$. Finally, if $\mathrm{char}(k_0) = p > 0$, it follows from [9, Lemma], that the image under $\overline{\varphi}$ of $\langle w_1, w_2, w_3\rangle$ is isomorphic to the free product $\mathbf{Z}_p * \mathbf{Z}_p * \mathbf{Z}_p$. Thus $\langle w_1, w_2, w_3\rangle \cong \langle w_1\rangle * \langle w_2\rangle * \langle w_3\rangle$. □

## REFERENCES


1. S. A. Amitsur, Rational identities and applications to algebra and geometry, *J. Algebra* **3** (1966), 304–359.
2. K. I. Beidar, W. S. Martindale III and A. V. Mikhalev, *Rings with Generalized Identities*, Marcel Dekker, New York, 1996.
3. B. Chang, S. A. Jennings and R. Ree, On certain pairs of matrices which generate free groups, *Canad. J. Math.* **10** (1958), 279–284.
4. K. Chiba, Free subgroups and free subsemigroups of division rings, *J. Algebra* **184** (1996), 570–574.
5. C. L. Chuang and P. H. Lee, Unitary elements in simple artinian rings, *J. Algebra* **176** (1995), 449–459.
6. P. M. Cohn, *Skew Fields. Theory of General Division Rings*, Cambridge University Press, Cambridge, 1995.
7. J. Z. Gonçalves, Free groups in subnormal subgroups and the residual nilpotence of the group of units of group rings, *Canad. Math. Bull.* **27** (1984), 365–370.
8. J. Z. Gonçalves, A. Mandel and M. Shirvani, Free products of units in algebras. II. Crossed products, *J. Algebra* **233** (2000), 567–593.


Publicado pelo ICMC-USP
Sob a supervisão CPq/ICMC

9. J. Z. Gonçalves and D. S. Passman, Construction of free subgroups in the group of units of modular group algebras, *Comm. Algebra* **24** (1996), 4211–4215.

10. J. Z. Gonçalves and D. S. Passman, Unitary units in group algebras, *Israel J. Math.* **125** (2001), 131–155.

11. I. N. Herstein, *Rings with Involution*, The University of Chicago Press, Chicago, 1976.

12. N. Jacobson, *Structure of Rings*, American Mathematical Society, Providence, RI, 1956.

13. T. Y. Lam, *A First Course in Noncommutative Rings*, Springer-Verlag, New York, 1991.

14. A. I. Lichtman, On subgroups of the multiplicative group of skew fields, *Proc. Amer. Math. Soc.* **63** (1977), 15–16.

15. L. Makar-Limanov, On free subobjects of skew fields, in *Methods in Ring Theory*, ed. F. van Oystaeyen, Proceedings, NATO ASI, Antwerp, 1983, NATO ASI Ser. C, Vol. 129, Kluwer Academic, Dordrecht, 1984, pp. 281–286

16. R. S. Pierce, *Associative Algebras*, Springer-Verlag, New York, 1982.

17. Z. Reichstein and N. Vonessen, Free subgroups in division algebras, *Comm. Algebra* **23** (1995), 2181–2185.

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