JOURNAL OF ALGEBRA 177, 451–462 (1995)

An Embedding Property of Universal Division Algebras

Zinovy Reichstein*

Department of Mathematics, Oregon State University, Corvallis, Oregon 97331

and

Nikolaus Vonessen†

Department of Mathematics, University of Southern California, Los Angeles, California 90089-1113

Communicated by Walter Feit

Received March 15, 1994

Let A be a central simple algebra of degree n and let k be a subfield of its center. We show that A contains a copy of the universal division algebra $D_{m,n}(k)$ generated by m generic $n \times n$ matrices if and only if $\operatorname{trdeg}_k A \geq \operatorname{trdeg}_k D_{m,n}(k) = (m-1)n^2 + 1$. Moreover, if in addition the center of A is finitely and separately generated over k then "almost all" division subalgebras of A generated by m elements are isomorphic to $D_{m,n}(k)$. In the last section we give an application of our main result to the question of embedding free groups in division algebras.

1. INTRODUCTION

Throughout this paper we shall work with a base field k and a fixed pair of integers $m, n \geq 2$. The universal division algebra over a field F generated by m generic $n \times n$ matrices will be denoted by $D_{m,n}(F)$. By the transcendence degree of a central simple algebra (or a prime PI-algebra) we shall mean the transcendence degree of its center. For example, $\operatorname{trdeg}_k D_{m,n}(k) = (m-1)n^2 + 1$; see [P, Theorem 1.8] or [Row, 3.3.31]. Our main result is the following theorem.

THEOREM 1.1. *Let A be a central simple algebra of degree n and let k be a subfield of its center. Then A contains a copy of the universal division algebra $D_{m,n}(k)$ if and only if* $\operatorname{trdeg}_k A \geq \operatorname{trdeg}_k D_{m,n}(k)$.

*E-mail address: zinovy@math.orst.edu.

†E-mail address: vonessen@math.usc.edu. This author was partially supported by NSF Grant DMS 9201465.

0021-8693/95 $12.00

Thus if A is a central simple algebra of degree n and transcendence degree at least $n^2 + 1$ over k, then

$$A = D_{2,n}(k) \otimes_{K_{2,n}(k)} F,$$

where $K_{2,n}(k)$ and F are the centers of $D_{2,n}(k)$ and A, respectively. Note that we allow the case $\operatorname{trdeg}_k(A) = \infty$. In particular, if the center of A is an uncountable field of characteristic 0 then A contains a copy of $D_{m,n}(\mathbb{Q})$ for any integer $m \geq 2$.

A proof of Theorem 1.1 is presented in Section 3. In Section 5 we show that if $\operatorname{trdeg}_k A \geq \operatorname{trdeg}_k D_{m,n}(k)$ then, in fact, "almost all" division subalgebras of A generated by m elements are isomorphic to $D_{m,n}(k)$. We call the m-tuples of elements with this property *maximal*; see Section 2. The precise statement of our result is as follows.

THEOREM 1.2. *Let k be an infinite field and let A be a central simple k-algebra of degree n whose center F is finitely and separably generated over k. Assume that* $\operatorname{trdeg}_k A \geq \operatorname{trdeg}_k D_{m,n}(k)$. *Let $U(A) \subset A^m$ be the set of all maximal m-tuples. Then $U(A)$ contains an open dense subset of $A^m \simeq F^{mn^2}$ with respect to the differential Zariski topology. If* $\operatorname{char} k = 0$ *then $U(A)$ is itself open and dense in A^m.*

The definition of the differential Zariski topology and a discussion of its basic properties can be found in Section 4. Since the differential Zariski topology is finer than the usual Zariski topology, Theorem 1.2 implies, in particular, that $U(A)$ is dense in $A^m \simeq F^{mn^2}$ with respect to the usual Zariski topology.

In the last section we give an application of Theorem 1.1 to the question of embedding free groups in division algebras. It is known that the multiplicative group of a finite-dimensional division algebra contains a copy of the free group on two generators. The proof of this fact relies on a deep theorem of Tits [T]; see, e.g., [M-L] or [G]. We give a new elementary proof under an additional assumption on the transcendence degree of the center; see Corollary 6.1.

2. PRELIMINARIES

We shall use the following notation.

m, n	integers ≥ 2,
k	base field,
F	field extension of k,
A	central simple algebra of degree n, usually with center F,

$U(A)$	set of all maximal m-tuples in A (see below),
$G_{m,n}(F)$	F-algebra of m generic $n \times n$-matrices,
$T_{m,n}(F)$	trace ring of m generic $n \times n$-matrices,
$C_{m,n}(F)$	center of $T_{m,n}(F)$,
$D_{m,n}(F)$	universal division algebra of m generic $n \times n$-matrices, and
$K_{m,n}(F)$	center of $D_{m,n}(F)$.

We will sometimes write $G_{m,n}$ for $G_{m,n}(k)$, $D_{m,n}$ for $D_{m,n}(k)$, etc.

We briefly recall the definition of the trace ring and the universal division algebra. Let $x_{ij}^{(l)}$ be mn^2 independent commuting variables; here $i,j = 1,\ldots,n$ and $l = 1,\ldots,m$. The ring of generic matrices $G_{m,n}(F)$ is the F-subalgebra of the matrix algebra $M_n(F[x_{ij}^{(l)}])$ generated by the m generic matrices $X_1 = (x_{ij}^{(1)}),\ldots,X_m = (x_{ij}^{(m)})$. The trace ring $T_{m,n}(F)$ is generated by the elements of $G_{m,n}(F)$ and the coefficients of their characteristic polynomials. The rings $G_{m,n}(F)$ and $T_{m,n}(F)$ are both PI-domains of degree n; the universal division algebra $D_{m,n}(F)$ is their common division algebra of fractions. For details of this construction see [C, 12.6] or [F_2].

An m-tuple $y = (y_1,\ldots,y_m) \in A^m$ is called *maximal* if the k-algebra generated by $y_1,\ldots,y_m$ is isomorphic to $G_{m,n}(k)$. This is equivalent to saying that $k\{y_1,\ldots,y_m\}$ is a domain whose division algebra of fractions is isomorphic to $D_{m,n}(k)$.

3. PROOF OF THEOREM 1.1

The "only if" assertion of Theorem 1.1 is obvious: if A contains a copy of $D_{m,n}(k)$ then $\operatorname{trdeg}_k(A) \geq \operatorname{trdeg}_k D_{m,n}(k) = (m-1)n^2 + 1$. In this section we present a proof of the converse. Our starting point is the following observation.

LEMMA 3.1. *Let A be a central simple algebra of degree n with center F, and let $x_{i,j}^{(l)}$ be central indeterminates over F, where $i,j = 1,\ldots,n$ and $l = 1,\ldots,m$. Then $A(x_{i,j}^{(l)})$ contains a copy of $D_{m,n}(F)$.*

Proof. Let $v_{i,j}$ $(i,j = 1,\ldots,n)$ be an F-basis of A, and set $y_l = \sum_{i,j} x_{i,j}^{(l)} v_{i,j}$. Let R be the F-subalgebra of $A(x_{i,j}^{(l)})$ generated by $y_1,\ldots,y_m$. It is enough to show that R is isomorphic to $G_{m,n}(F)$.

Consider an embedding $f\colon A \to M_n(L)$ where L is a splitting field for $A(x_{i,j}^{(l)})$. We will identify A with $f(A)$. Note that $M_n(L)$ contains the m generic matrices $X_l = (x_{i,j}^{(l)})$, $l = 1,\ldots,m$. Since the $v_{i,j}$ form an L-basis for $M_n(L)$, there are scalars $s_{i,j}^{(l)} \in L$ such that $X_l = \sum_{i,j} s_{i,j}^{(l)} v_{i,j}$. Now

extend f to a map f: $A[x_{i,j}^{(l)}] \to M_n(L)$ by setting $f(x_{i,j}^{(l)}) = s_{i,j}^{(l)}$. Then $f(y_l) = X_l$. Thus f restricts to a homomorphism g from $R = F\{y_1, \ldots, y_m\}$ onto the generic matrix algebra $G_{m,n}(F)$. Since R is generated by m elements, g is an isomorphism. ∎

Since $D_{m,n}(k) \subset D_{m,n}(F)$, A also contains a copy of $D_{m,n}(k)$. Thus in order to prove Theorem 1.1 it is enough to eliminate the central indeterminates introduced in Lemma 3.1. Proposition 3.2 below asserts that this can indeed be done.

PROPOSITION 3.2. *Let A and B be central simple k-algebras of the same degree with centers F and K, respectively. Assume that K is finitely generated over k, $\operatorname{trdeg}_k K \leq \operatorname{trdeg}_k F$, and B can be embedded in $A(x)$ where x is a central indeterminate. Then B can be embedded in A.*

Theorem 1.1 follows directly from Lemma 3.1 and Proposition 3.2. The rest of this section will be devoted to proving Proposition 3.2. Our proof relies on the following commutative result.

LEMMA 3.3. *Let F and K be two extensions of a field k such that* (i) *F is an infinite field,* (ii) *K is finitely generated over k, and* (iii) $\operatorname{trdeg}_k K \leq \operatorname{trdeg}_k F$. *Suppose K can be k-isomorphically embedded into a purely transcendental extension $F(x)$ of F. Then there are infinitely many elements $c \in F$ such that the specialization $F[x] \to F$ sending x to c induces an embedding $K \hookrightarrow F$.*

Proof. Lemma 3.3 is proved in [Roq, Lemma 1] for infinite fields k; the general case is considered in [O]. Since neither paper states this result in the exact form we need, we briefly outline a proof below.

First of all, we may assume that $\operatorname{trdeg}_k F < \infty$. Indeed, write the generators $r_1(x), \ldots, r_a(x)$ of K over k as rational functions in x. Each has only a finite number of coefficients in F. Thus we can replace F by the extension of k generated by these coefficients.

The reduction arguments in [Roq, p. 210] show that we may assume without loss of generality that $\operatorname{trdeg}_k K = \operatorname{trdeg}_k F$, and that x is transcendental over K.

If F is algebraic over k then so is K. Hence, K lies in the algebraic closure of k in $F(x)$ which is equal to F. In this case any $c \in F$ will do.

Now assume that F contains an element z which is transcendental over k. The argument in [O] shows that we can take $c = z^j$ for sufficiently large j. Thus there are infinitely many such c, as desired. ∎

Proof of Proposition 3.2. We may assume without loss of generality that B is contained in $A(x)$. Since B and $A(x)$ have the same degree, K is a subfield of $F(x)$.

We may assume without loss of generality that x is transcendental over K. Indeed, if $\operatorname{trdeg}_k F = \operatorname{trdeg}_k K$ then this is necessarily so. If, on the

other hand, $\mathrm{trdeg}_k F > \mathrm{trdeg}_k K$ and x is algebraic over K then we simply replace x by $x + b$ where $b \in F$ is transcendental over K.

Suppose that F is an infinite field. Let $\{b_i\}$ be a basis of B over K. Then $b_i = f_i(x)/g_i(x)$ where $f_i \in A[x]$ and $g_i \in F[x]$. By Proposition 3.3, there are infinitely many elements $c \in F$ such that the specialization $F[x] \to F$ sending x to c induces an embedding of K into F. Choose such a c which is not a root of any g_i. Denote by R the localization of $F[x]$ at the maximal ideal $(x - c)$, and let φ: $A \otimes_F R \to A$ be the map given by specializing x to c. Since B is contained in $A \otimes_F R$, this induces a ring homomorphism from B into A. This map is injective since B is simple.

Now suppose F is a finite field. Then $k \subseteq F$ is finite as well. Since K is finitely generated over k and $\mathrm{trdeg}_k K \leq \mathrm{trdeg}_k F = 0$, K is also a finite field. Thus in this case both A and B are finite simple rings and thus matrix algebras over F and K, respectively. By our assumption, they have the same degree. Denote it by r. Since K is finite, it is contained in the algebraic closure of k in $F(x)$, which is equal to F. Thus $K \subseteq F$, and $B = M_r(K)$ embeds into $A = M_r(F)$, as desired. ∎

Remark 3.4. Let D be a division algebra of degree n and of finite transcendence degree over k. Say that D satisfies the *embedding property* if it embeds into every central simple algebra A of degree n, provided that $\mathrm{trdeg}_k A \geq \mathrm{trdeg}_k D$. Using Theorem 1.1 and Proposition 3.2, it is now easy to determine the division algebras of degree n satisfying the embedding property: these division algebras are (up to isomorphism) precisely the division subalgebras of degree n of the algebras $D_{m,n}(k)$ for $m \geq 2$.

4. THE DIFFERENTIAL ZARISKI TOPOLOGY

The next two sections are devoted to proving Theorem 1.2. In this section we define the differential Zariski topology and discuss some of its basic properties. Throughout this section the base field k will be infinite, and L will be a finitely generated extension of k. We shall also assume that $k \subset L$ is a *separably generated* extension. This means that there exists a transcendence basis $z_1, \ldots, z_r$ of L over k such that L is separable over $k(z_1, \ldots, z_r)$. Such a transcendence basis is called *separating*. Note that L is in fact separable over k; see, e.g., [C, Sect. 6.6, Corollary 1].

We begin by recalling some well-known facts about derivations and differentials. General references for these facts are [L, Chap. X, Sect. 7] and [M, Chap. 10].

Let $\Omega_{L/k}$ denote the L-vector space of Kähler differentials of L over k and let $\mathrm{Der}_k(L)$ be the L-vector space of k-derivations from L to itself. Recall that $\Omega_{L/k}$ and $\mathrm{Der}_k L$ are dual vector spaces, i.e., $\mathrm{Der}_k(L) = \mathrm{Hom}_L(\Omega_{L/k}, L)$.

PROPOSITION 4.1. *Let L be a finitely generated separably generated extension of k of transcendence degree r, and let $z_1, \dots, z_q \in L$.*

(a) $\mathrm{Der}_k(L)$ *is an r-dimensional L-vector space.*

(b) $dz_1, \dots, dz_q$ *are L-linearly independent in $\Omega_{L/k}$ iff $z_1, \dots, z_q$ can be completed to a separating transcendence basis of L over k.*

(c) *Let $z_1, \dots, z_q \in L$, and let $D_1, \dots, D_r$ be an L-basis of* $\mathrm{Der}_k(L)$. *If the $r \times q$ Jacobian matrix $(D_i(z_j))$ has rank q then $z_1, \dots, z_q$ are algebraically independent over k. The converse holds if* $\mathrm{char}(k) = 0$.

Proof. The first two statements follow from [L, Chap. X, Proposition 7.5]. The condition on the Jacobian matrix in (c) is equivalent to L-linear independence of $dz_1, \dots, dz_q$. Hence, it implies algebraic independence of $z_1, \dots, z_q$ by (b).

To prove the last assertion in (c) assume that $z_1, \dots, z_q$ satisfy a non-trivial algebraic relation $p(z_1, \dots, z_q) = 0$. Then $0 = dp(z_1, \dots, z_q) = \Sigma(\partial p_i / \partial z_i)\, dz_i$. Since we are in characteristic zero, this shows that the differentials $dz_1, \dots, dz_q$ are L-linearly dependent. Hence, the Jacobian matrix has rank $< q$. ∎

Let s be a positive integer and let $\mathrm{Map}(L^s, L)$ be the commutative L-algebra of all set maps from L^s to L with addition and multiplication defined pointwise. Let $\mathscr{DP}_k(s)$ be the L-subalgebra generated by maps of the form $(x_1, \dots, x_s) \to x_i$ and $(x_1, \dots, x_s) \to D(x_i)$. Here i ranges from 1 to s and D ranges over $\mathrm{Der}_k(L)$. We shall refer to elements of $\mathscr{DP}_k(s)$ as *differential polynomials*.

One can think of differential polynomials more concretely in the following way. Choose a separating transcendence basis $z_1, \dots, z_r$ for L over k. By Proposition 4.1, the differentials $dz_1, \dots, dz_r$ form an L-basis of $\Omega_{L/k}$. Denote the dual basis of $\mathrm{Der}_k(L)$ by $D_1, \dots, D_r$. In other words, $D_i(z_j) = \delta(i, j)$.

Let $p(x_{ij}) \in L[x_{ij}]$ be a polynomial in $(r+1)s$ variables; here $i = 0, \dots, r$ and $j = 1, \dots, s$. Given $a_1, \dots, a_s \in L$, let $a_{0j} = a_j$ and $a_{ij} = D_i(a_j)$ for $i = 1, \dots, r$. We define the differential polynomial associated to p to be the map $f_p\colon L^s \to L$ given by

$$f_p(a_1, \dots, a_s) = p(a_{ij}).$$

One sees easily that the map $\phi\colon L[x_{ij}] \to \mathscr{DP}_k(s)$ defined by $\phi(p) = f_p$ is a surjective homomorphism of L-algebras.

LEMMA 4.2. *The map $\phi\colon L[x_{ij}] \to \mathscr{DP}_k(s)$ defined above is an isomorphism.*

Proof. For $q \in L[x_{ij}]$ let $S(q)$ be the smallest subset of $\{x_{ij}\}$ such that $q \in L[S(q)]$. In other words, q depends on the variables in $S(q)$ and is

independent of the other variables. Suppose that $f_p(a_1, \ldots, a_s) = 0$ for every $a_1, \ldots, a_s \in L$. We have to show that $p = 0$ in $L[x_{ij}]$. Assume the contrary. We may assume without loss of generality that $S(p)$ is minimal among all $S(q)$ where $q \in L[x_{ij}]$, $q \neq 0$, and $f_q = 0$.

It is enough to prove that $S(p) = \varnothing$, since in this case $p \in L$, and for such p, $f_p = 0$ clearly implies $p = 0$. First we show that $x_{0j} \notin S(p)$, for any $j = 1, \ldots, s$. Assume the contrary,

$$p = \sum_{i=0}^{d} p_i x_{0j}^i,$$

where $d \geq 1$, $p_d \neq 0$, and $S(p_i) \subset S(p) \setminus \{x_{0j}\}$. Let $t \in k$. Substituting $a_j + t$ for a_j and expanding the resulting differential polynomial in the powers of t, we obtain

$$\begin{aligned} 0 &= f(a_1, \ldots, a_{j-1}, a_j + t, a_{j+1}, \ldots, a_s) \\ &= f_{p_d}(a_1, \ldots, a_s)t^d + \sum_{i=0}^{d-1} f_{q_i}(a_1, \ldots, a_s)t^i \end{aligned}$$

for some differential polynomials $q_0, \ldots, q_{d-1}$. Since the above identity holds for every $t \in k$ and k is an infinite field, we conclude that $f_{p_d} = 0$. This contradicts the minimality of $S(p)$.

A similar argument can be used to show that $x_{\nu j}$ is not contained in $S(p)$ for any $\nu = 1, \ldots, r$ and $j = 1, \ldots, s$. In this case we substitute $a_j + tz_\nu$ for a_j. Since $x_{0j} \notin S(p)$, expanding in the powers of t leads to a contradiction in the same way as above. ∎

We shall call a subset of L^s closed in the *differential Zariski topology* if it is the zero locus of a finite number of differential polynomials. Since every ideal of $L[x_{ij}]$ is finitely generated, this indeed defines a topology on L^s.

Note that this topology is finer than the usual Zariski topology. In other words, a Zariski closed set is closed in the differential Zariski topology. The converse is false in general. For example, assume that k is algebraically closed in L. Then k^s is closed in L^s in the differential Zariski topology, since it is the locus of $D_1 = \cdots = D_r = 0$. On the other hand, since k is an infinite field, the closure of k^s in the usual Zariski topology is all of L^s. However, we shall now see that the differential Zariski topology shares two key properties with the usual Zariski topology.

THEOREM 4.3. *Let k be an infinite field, and let L be a finitely and separably generated extension of k.*

(a) *L^s is irreducible with respect to the differential Zariski topology.*

(b) *Let F be a subfield of L containing k such that L is a finite separable extension of F. Then the differential Zariski topology on F^s is induced by the differential Zariski topology on L^s. Moreover, F^s is dense in L^s.*

Proof. (a) Assume $L^s = X \cup Y$ where X and Y are proper closed subsets. Then X is contained in the zero locus of f_p and Y is contained in the zero locus of f_q for some polynomials $0 \neq p, q \in L[x_{ij}]$. Then L^s is contained in the zero locus of f_{pq}. By Lemma 4.2, $pq = 0$ in $L[x_{ij}]$, a contradiction.

(b) Note first that F is finitely and separably generated over k; see, e.g., [C, Sect. 6.6, Corollary 1]. Let V be the set of all F-vector space homomorphisms $L \to F$ which restrict to the identity map on F. For $p \in L[x_{ij}]$ and $h \in V$ let $h(p) \in F[x_{ij}]$ denote the polynomial obtained from p by applying h to each coefficient. Note that $p = 0$ if and only if $h(p) = 0$ for every $h \in V$.

Let $z_1, \ldots, z_r$ be a separating transcendence basis of F. Then it is also a separating transcendence basis of L. Choose the derivations $D_1, \ldots, D_r \in \mathrm{Der}_k(F)$ so that $D_i(z_j) = \delta(i, j)$ as before. Since L is a finite separable extension of F, $D_1, \ldots, D_r$ lift to a basis of $\mathrm{Der}_k(L)$. Thus if $p \in L[x_{ij}]$, then $f_{h(p)}$ restricts to a differential polynomial $F^s \to F$. Let $a_1, \ldots, a_s \in F$. Then $f_p(a_1, \ldots, a_s) = 0$ if and only if $f_{h(p)}(a_1, \ldots, a_s) = 0$ for every $h \in V$. This shows that the differential Zariski topology on F^s is induced from L^s.

To prove the second assertion, assume that F^s is contained in the zero locus of the differential polynomial f_p for some $p \in L[x_{ij}]$. Then $f_{h(p)}$: $F^s \to F$ is identically zero for every $h \in V$. Hence, Lemma 4.2 implies that $h(p) = 0$ for every $h \in V$, i.e., $p = 0$. ∎

Remark 4.4. One can consider a finer topology on L^s by defining the closed sets to be zero loci of differential polynomials involving higher order derivatives. A slight modification of our arguments shows that Theorem 4.3 holds for this topology as well if $\mathrm{char}(k) = 0$. (If $\mathrm{char}(k) = p$ then the argument still works if we allow derivatives of order up to $p - 1$.) We have limited our discussion to the "first order" differential Zariski topology because it simplifies the notation and is sufficient for the purpose of stating and proving Theorem 1.2.

5. PROOF OF THEOREM 1.2

We now apply the results of Section 4 to prove Theorem 1.2.

Let L be a finite separable field extension of F which splits A. Then $A \otimes_F L = M_n(L)$ and hence we may assume $A \subset M_n(L)$. Denote by $U(A)$ the set of all maximal m-tuples in A^m. Then $U(A) = U(M_n(L)) \cap A^m$.

Let $\{v_1, \ldots, v_{n^2}\}$ be an F-basis for A. Every element of $M_n(L)$ can be uniquely written as $\sum b_i v_i$ where $b_1, \ldots, b_{n^2} \in L$. This element lies in A if and only if $b_1, \ldots, b_{n^2} \in F$. In this way we identify $M_n(L)$ and A with L^{n^2} and F^{n^2}, respectively; $M_n(L)^m$ and A^m are identified with L^{mn^2} and F^{mn^2}. By Theorem 4.3, $A^m \simeq F^{mn^2}$ is dense in $(M_n(L))^m \simeq L^{mn^2}$, and the differential Zariski topology on A^m is induced from $(M_n(L))^m$. Since $U(A) = U(M_n(L)) \cap A^m$, it suffices to prove Theorem 1.2 for $A = M_n(L)$. Thus from now on we will assume that $A = M_n(L)$ for some finitely and separably generated field extension L of k.

Let $C_{m,n}$ be the center of the trace ring $T_{m,n}$. The center $K_{m,n}$ of $D_{m,n}$ is the fraction field of $C_{m,n}$. Since $K_{m,n}$ is unirational over k, it is separable over k [L, X.6.2, X.5.3, and X.6.1]). Thus we can choose a separating transcendence basis for $K_{m,n}$ from any given set of generators [L, X.6.8]). In particular, we can find a separating transcendence basis $f_1, \ldots, f_d$ for $K_{m,n}$ consisting of elements of $C_{m,n}$. Here

$$d = \operatorname{trdeg}_k C_{m,n} = \operatorname{trdeg}_k K_{m,n} = \operatorname{trdeg}_k D_{m,n} = (m-1)n^2 + 1.$$

Note that each f_i is a polynomial in the entries of the generic matrices $X_1, \ldots, X_m$. Hence, it makes sense to talk about $f_i(y)$ for any m-tuple $y = (y_1, \ldots, y_m)$ of matrices over a commutative ring.

LEMMA 5.1. *Let K be a field extension of k. An m-tuple $y = (y_1, \ldots, y_m)$ of $M_n(K)$ is maximal if and only if the elements $f_1(y), \ldots, f_d(y) \in K$ are algebraically independent over k.*

Proof. Let h: $T_{m,n} \to M_n(K)$ be the homomorphism given by specializing the generic matrices $X_1, \ldots, X_m$ to $y_1, \ldots, y_m$, respectively.

First assume that $f_1(y), \ldots, f_d(y)$ are algebraically independent. Then

$$\operatorname{trdeg}_k h(C_{m,n}) = \operatorname{trdeg}_k C_{m,n}$$

and thus $\operatorname{Ker}(h) \cap C_{m,n} = (0)$. By [Row, 1.6.27] this implies $\operatorname{Ker}(h) = (0)$. Thus the k-algebra generated by $y_1, \ldots, y_m$ is isomorphic to $G_{m,n}$.

Conversely, assume $f_1(y), \ldots, f_d(y)$ are algebraically dependent. Suppose that $(y_1, \ldots, y_m)$ is a maximal m-tuple. Then $k\{y_1, \ldots, y_m\}$ is a domain of degree n and transcendence degree d. We will derive from this a contradiction. Since $T_{m,n}$ is a finite module over $C_{m,n}$ (see [Row, 4.2.9]), $\operatorname{trdeg}_k h(T_{m,n}) = \operatorname{trdeg}_k h(C_{m,n}) < d$. Since $k\{y_1, \ldots, y_m\}$ is contained in $h(T_{m,n})$, it has transcendence degree $< d$, a contradiction. ∎

We are now ready to prove Theorem 1.2. Choose a separating transcendence basis $z_1, \ldots, z_r$ of L over k. Then $dz_1, \ldots, dz_r$ is an L-basis of $\Omega_{L/k}$. Let $D_1, \ldots, D_r$ be the dual basis of $\operatorname{Der}_k(L)$. By Lemma 5.1, the m-tuple y is maximal if and only if $f_1(y), \ldots, f_d(y)$ are algebraically

independent over k. By the Jacobian criterion of Proposition 4.1(c), this happens if the $r \times d$ Jacobian matrix $(D_i(f_j(y)))$ has rank d; in characteristic zero, the converse is also true. The condition that the $(d \times d)$-minors of this Jacobian matrix vanish is given by a collection of differential polynomials in the entries of $y_1, \dots, y_m$. Denote by $V(A)$ the set of all m-tuples $y \in A^m$ such that the Jacobian matrix $(D_i(f_j(y)))$ has rank d. Then $V(A) \subset A^m$ is open in the differential Zariski topology, and is contained in $U(A)$. Moreover, $V(A) = U(A)$ in characteristic zero.

It only remains to show that the open set $V(A)$ is non-empty; it will then automatically be dense by Theorem 4.3(a). In characteristic zero $V(A) = U(A)$ and $U(A) \neq \emptyset$ by Theorem 1.1. The following characteristic-free argument completes the proof of Theorem 1.2 in characteristic p.

Let K be the field obtained from $K_{m,n}(k)$ by adjoining all eigenvalues of the first generic matrix. Then $K/K_{m,n}$ is separable algebraic, K/k is purely transcendental, and $D_{m,n} \otimes_{K_{m,n}} K = M_n(K)$; see [P] or [F$_1$]. Since $d = \operatorname{trdeg}_k(K) \leq \operatorname{trdeg}_k(L)$, we can embed K into L by sending d algebraically independent generators of K to the first d elements of a separating transcendence basis $\{w_i\}$ of L. Since K is separable algebraic over $K_{m,n}$, replacing w_i by f_i for $i = 1, \dots, d$ gives rise to another separating transcendence basis of L. Denote this new basis by $z_1, \dots, z_r$. By our construction $z_i = f_i$ for $i \leq d$. Since $D_{m,n} \subset M_n(K)$, and K is embedded in L, we also have an embedding of $D_{m,n}$ into $A = M_n(L)$. If $y \in A^m$ is the m-tuple of generic matrices in $D_{m,n}$, then $f_i(y) = f_i$. Consequently, the first d rows of the $r \times d$ Jacobian matrix $(D_i(f_j(y)))$ form a $d \times d$ identity matrix. Thus this Jacobian matrix has rank d, proving that $y \in V(A)$ and hence that $V(A)$ is nonempty. ∎

6. FREE SUBGROUPS

In this section we apply Theorem 1.1 to produce (in an elementary way) free subgroups in finite-dimensional division algebras. As we remarked in the Introduction, the existence of such subgroups is well known. We shall only consider the free group $G_2 = \langle x, y \rangle$ on two generators since it contains a copy of the free group with a countable generating set.

COROLLARY 6.1. *Let D be a finite-dimensional division algebra of degree $n \geq 2$. If the transcendence degree of D over its prime field is greater than or equal to $n^2 + 1$ then D^* contains a copy of the free group on two generators.*

Note that Corollary 6.1 applies, in particular if D has uncountably many elements since in this case the transcendence degree of D over its prime field is infinite.

Proof. Denote the prime field of D by k. By Theorem 1.1, D contains a copy of the universal division algebra $D_{2,n}(k)$. Thus it is sufficient to show that the two generic $n \times n$ matrices X_1 and X_2 generate a free subgroup in $D_{2,n}(k)$. This follows, e.g., from Amitsur's theorem on group identities; see [Row, 8.4.2]. For completeness, we include an elementary characteristic-free proof.

Assume the contrary. A specialization argument shows that $\mathrm{GL}_n(L)$ does not contain a copy of G_2 for any extension L of k. Since $\mathrm{GL}_2(L) \subset \mathrm{GL}_n(L)$, $\mathrm{GL}_2(L)$ does not contain G_2 either. Let $L = k(s,t)$ where s, t are algebraically independent over k. We claim that

$$A = \begin{pmatrix} 1 & t \\ 0 & s \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 1 & 0 \\ t & s \end{pmatrix}$$

generate a free subgroup of $\mathrm{GL}_2(L)$. One easily shows by induction on r that any product $A^{n_1}B^{m_1} \cdots A^{n_r}B^{m_r}$ with nonzero n_i and m_i has the form

$$\begin{pmatrix} p_{11}(t) & p_{12}(t) \\ p_{21}(t) & p_{22}(t) \end{pmatrix}$$

where the degrees of $p_{11}(t)$, $p_{12}(t)$, $p_{21}(t)$, and $p_{22}(t)$ (as polynomials in t over $k(s)$) are $2r$, $2r-1$, $2r-1$, and $2r-2$, respectively. This proves that $\langle A, B \rangle$ is a free group, contradicting our assumption. ∎

The bound on the transcendence degree in Corollary 6.1 can be sharpened in the following way. Let F be the center of D. Write $n = n_1 \cdots n_r$ as a product of powers of distinct primes where $n_1 < \cdots < n_r$. Then there is a subalgebra $D_1 \subset D$ of degree n_1 with center F. Replacing D by D_1 we see that $\mathrm{trdeg}_k F \geq n_1^2 + 1$ will suffice.

ACKNOWLEDGMENTS

This paper was motivated by a theorem of David Saltman [S, Theorem 4]. We thank him and Burton Fein for discussing the results of [S] with us. We are also grateful to Robert Guralnick and Leonid Makar-Limanov for helpful comments regarding free subgroups of division algebras.

REFERENCES

[C] P. M. Cohn, "Algebra," Vol. 2, 2nd. ed., Wiley, Chichester, 1982.

[F$_1$] E. Fromanek, The center of the ring of 3×3 generic matrices, *Linear and Multilinear Algebra* **7** (1979), 203–212.

[F_2] E. Formanek, "The polynomial identities and invariants of $n \times n$ matrices," CBMS Regional Conference Series in Math., Vol. 78, Amer. Math. Soc., Providence, RI, 1991.

[G] 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.

[L] S. Lang, "Algebra," 2nd ed., Addison-Wesley, Reading, MA, 1984.

[M-L] L. Makar-Limanov, On free subobjects of skew fields, *in* "Methods in Ring Theory," (F. van Oystaeyen, Ed.), NATO Advanced Study Institute Series C, Vol. 129, pp. 281–285, Reidel, Dordrecht, 1984.

[M] H. Matsumura, "Commutative Algebra," 2nd ed., Mathematics Lecture Notes Series, Benjamin/Cummings, Reading, MA, 1980.

[O] J. Ohm, On subfields of rational function fields, *Arch. Math.* **42** (1984), 136–138.

[P] C. Procesi, Non-commutative affine rings, *Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur (8)* **6** (1967), 239–255.

[Roq] P. Roquette, Isomorphisms of generic splitting fields of simple algebras, *J. Reine Angew. Math.* **214 / 215** (1964), 207–226.

[Row] L. H. Rowen, "Polynomial Identities in Ring Theory," Academic Press, New York, 1980.

[S] D. J. Saltman, A note on generic division algebras, *Contemp. Math.* **130** (1992), 385–394.

[T] J. Tits, Free subgroups of linear groups, *J. Algebra* **20** (1972), 250–270.