ON THE CONSTRUCTION OF THE FREE FIELD

Dedicated to the Memory of Marcel-Paul Schützenberger

P. M. COHN

Mathematics, University College London
Gower street, London WC1E 6BT
United Kingdom

C. REUTENAUER*

Mathématiques, Université du Québec à Montréal, Montréal, CP 8888
succ. Centre-Ville, Canada H3C 3P8

Communicated by J.-E. Pin
Received 15 July 1997

AMS Mathematics Subject Classification: 16K40

We give a linear algebraic construction of the free field, by constructing the category of "representations": an element of the free field is characterized by the class of objects which can be connected by a chain of morphisms and inverse morphisms; we characterize minimal representations of a given element. We characterize power series and polynomials by their representations among all elements of the free field, and give a primary decomposition of the elements of the free field, extending the classical one for rational functions and that of Fliess for noncommutative rational series. We show that each rational identity in the free field may be "trivialized", that is, is a consequence of the axioms of a field. We give an algorithm for the word problem in the free field, using Gröbner bases, different from a previous algorithm of the first author.

0. Introduction

In any variety V of algebras, there exists for every set X a free V-algebra F_X on X, which is characterized by the property that every mapping from X to a V-algebra A can be extended in just one way to a homomorphism from F_X to A. This is well-known, but of little use for classes that are not varieties, such as fields. Nevertheless, there is a construction that has a claim to be called a "free field"; in the commutative case, it is the rational function field $k(X)$ in a set X of indeterminates over a ground field k. The noncommutative analogue was first constructed by Amitsur [1]; since then, there have been other more explicit constructions (see [9, 10]), but some questions still remain. In the first place, one may ask whether the free field is really free, i.e. when a formal expression represents zero, is it the case that the expression can be reduced to zero by rational operations only? This question will be answered in the affirmative in Sec. 3, while Sec. 1 is devoted to a simple description of the elements of the free (skew) field. Closely

*Supported by a grant NSERC, Canada, and Université Louis Pasteur, Strasbourg, France.

International Journal of Algebra and Computation Vol. 9 Nos. 3 & 4 (1999) 307–323

related to this question is the word problem for free fields; this was shown to be solvable in [7] (see also [10]). Here, we present another simple solution in Sec. 4. Section 2 describes a decomposition of elements of the free field analogous to the partial fraction decomposition in the commutative case.

Note that most of the results of [11] are given a new proof in the present article without the use of formal power series. Also, the techniques we use allow us to drop the hypothesis, necessary in [11], that k is the centre of D and that k is infinite. We simply assume that k is a central subfield of D. Furthermore, unlike [11], where the case $D = k$ must be treated separately, we prove directly the general case.

We recall that a matrix over a ring is said to be *full* if it is square of order n, say and if it cannot be written as a product of an $n \times n-1$ by an $n-1 \times n$ matrix. A square matrix M of order n is called *hollow* if it contains a zero submatrix of size $p \times q$ with $p + q > n$. A hollow matrix is always nonfull, as follows by an obvious factorization. Two matrices A and B are *associated* if $A = PBQ$ for some invertible matrices P and Q. If the matrices become associated when we form a diagonal sum with a unit matrix of each, then they are said to be *stably associated.* Note that if we let matrices act from the right on row vectors, then a square matrix is associated to a hollow matrix if and only if there are free submodules E and F with $\dim(E) > \dim(F)$ and both direct summands of the whole space, such that the matrix maps E into F.

1. A Linear Algebraic Construction of the Free Field

Let D be a skew field with a central subfield k and put $X = \{x_1, \ldots, x_d\}$. Our aim is to give a representation for the elements of the free field $D_k \langle\!\langle X \rangle\!\rangle$, the universal field of fractions of the tensor ring $R = D_k\langle X\rangle$ (see [10, p. 38] for the definition of the tensor ring, which informally speaking is the ring of noncommutative polynomials generated by the variables $x_1, \ldots, x_d$ over D, with no commutation allowed between the variables and the elements of D, except those of k). Each element of the free field can be represented in the form $f = c + uA^{-1}v$, where $c \in R$, u, v are a row respectively column over R and A is a full matrix over R. The order of the matrix A will be called the *dimension* of the representation. We shall say that f is represented by $\rho = c + (u, A, v)$, and we also say that f is represented by the *block*:

$$\begin{pmatrix} A & -v \\ u & c \end{pmatrix} . \tag{1}$$

Note that f is the $(n+1, n+1)$ *quasi-determinant*, in the sense of [15], of this matrix. We call A the *pivot matrix* of the representation, or of the block, and c its *scalar term.* Two representations, or blocks, are said to be *equivalent*, if they represent the same element. If the scalar term is 0, we call the representation and the block *pure*. Each representation, or block, is equivalent to a pure one.

The pivot matrix A may be replaced by any matrix stably associated to it over R by modifying u and v appropriately. For if $A = PA'Q$ where P, Q are invertible over R, then $f = c + u'A'^{-1}v'$, where u', v' are related to u, v by $u = u'Q$, $v = Pv'$.

Further, if $A = B \oplus I$, and a corresponding decomposition of u, v is $u = (u', u'')$, $v = (v', v'')^T$, then $f = c + u''v'' + u'B^{-1}v'$.

More generally, f can also be represented by $c + (uQ, PAQ, Pv)$ for any full matrices P, Q over R, since a full matrix over R is invertible in the free field. Likewise, such matrices can always be cancelled from a representation without affecting the value of f.

The process of linearization by enlargement (also called Higman's trick, see [9, p. 272], [10, p. 284f]) allows us to assume that A is linear in the x_i, and that u, v are over D. Such a representation will be called *linear*. Note that in this case, A may be written:

$$A = A_0 + \sum_{1 \le i \le d} A_i' x_i A_i'' \tag{2}$$

where A_0, A_i' and A_i'' are matrices over D of appropriate size (see [10, p. 292–293] for this notation). Each element of the free field has a representation which is both pure and linear, as is well-known. In the sequel, most of the representations will be pure and linear.

We can form a category whose objects are the pure and linear representations, where a morphism from $\rho = (u, A, v)$ to $\rho' = (u', A', v')$ is defined as a pair of matrices (P, Q) of appropriate size over D such that $u' = uQ$, $v = Pv'$, and $PA' = AQ$. To verify that this defines a category, let (P, Q) be a morphism from (u, A, v) to (u', A', v') and (P', Q') a morphism from (u', A', v') to (u'', A'', v''); then $u'' = u'Q' = uQQ'$, $v = Pv' = PP'v''$ and $PP'A'' = PA'Q' = AQQ'$, which shows that (PP', QQ') is a morphism from (u, A, v) to (u'', A'', v'') and it easily implies that we have indeed a category.

Our category is *affine* in the sense that for any two morphisms (P, Q) and (P', Q') from ρ to ρ' and any λ, μ such that $\lambda + \mu = 1$, $(\lambda P + \mu P', \lambda Q + \mu Q')$ is again a morphism.

Note that P and Q have the same rank since A and A' are full, invertible in the free field, and the rank is unchanged after field extension. Note also that P and Q have the same size. It is easy to see that the morphism (P, Q) in this category is a monomorphism (respectively an epimorphism) if and only if P and Q are both injective (respectively surjective) if we view them as linear mappings acting from the right on row vectors over D (note that we denote composition of morphisms from left to right). If the morphism (P, Q) is injective (respectively surjective), we say that ρ is a *subrepresentation* of ρ' (respectively ρ' is a *quotient* of ρ).

Note that a pure linear representation $\rho = (u, A, v)$ is equivalent to the following data: two left D-spaces E and F of the same finite dimension, a vector u in F, a linear form v on E and an R-linear mapping A from the left R-module $R \otimes_D E$ into $R \otimes_D F$ which when written as matrix in D-bases of E and F has degree at most 1 and is full. We recover the original definition by taking bases of E and F. In this framework, a morphism $\rho \to \rho'$ is a couple of D-linear mappings (P, Q), with $P : E \to E'$, $Q : F \to F'$, such that $u' = uQ$, $v = Pv'$ and $AQ = PA'$. This will be used several times in the following.

Theorem 1.1. *Two pure and linear representations are equivalent if and only if there is a chain of morphisms or inverse morphisms between them.*

We first prove a lemma.

Lemma 1.2. *Let the element f of $D_k \langle\!\langle X \rangle\!\rangle$ be represented by (u, A, v), with A linear and full over $R = D_k\langle X\rangle$, and u, v over D. Then $f = 0$ if and only if for some invertible matrices P, Q over D, one has the following block decomposition:*

$$uQ = (\times \quad 0), PAQ = \begin{pmatrix} B & 0 \\ \times & C \end{pmatrix}, Pv = \begin{pmatrix} 0 \\ \times \end{pmatrix},$$

for some square matrices B and C.

Proof The if part is easy and left to the reader. For the only if part, we let the matrices over R act as linear mappings on the right on row vectors over R. Note that all we have to show is that there exist D-subspaces E, F of $D^n = D^{1\times n}$ such that $\dim(E) = \dim(F)$, $E \subset \operatorname{Ker}(v)$, $u \in F$, and $EA \subset RF$, where RF denotes the R-subspace of R^n spanned by F: indeed, if such subspaces exist, we take bases of D^n which contain as initial subsequences bases of E, F, and the corresponding matrices P, Q of basis change will fulfill the requirement.

Now the hypothesis that $f = 0$ implies that the matrix:

$$\bar{A} = \begin{pmatrix} A & -v \\ u & 0 \end{pmatrix}$$

is not full (see [10, Theorem 4.5.11], with $-v$ in place of v, which does not affect fullness). This implies by Corollary 6.3.6 of [10] that $\bar{A}$ is associated over D to a hollow matrix. Let matrices act as before on row vectors; then the previous fact means that there exist D-subspaces E_1, F_1 of $D^n \times D = D^{n+1}$ such that: $\dim(E_1) > \dim(F_1)$ and $E_1\bar{A} \subset RF_1$. Note that for $(e, \alpha) \in D^n \times D$, we have $(e, \alpha)\bar{A} = (eA + \alpha u, ev)$.

Let p denotes the projection $D^n \times D \to D^n$. We show that the subspaces $E = p(E_1) \cap \operatorname{Ker}(v)$ and $F = F_1 \cap D^n + Du$ do the job (we identify D^n and $D^n \times \{0\}$). Evidently, $E \subset \operatorname{Ker}(v)$ and $u \in F$. Let $e \in E$, then for some $\alpha \in D$, we have $(e, \alpha) \in E_1$ and $ev = 0$. Then RF_1 contains $(e, \alpha)\bar{A} = (eA + \alpha u, ev) = (eA + \alpha u, 0)$, which implies that $eA + \alpha u \in RF_1 \cap R^n$, hence $eA \in RF_1 \cap R^n + Du$. We show that this space is contained in $R(F_1 \cap D^n + Du) = RF$ (which will imply that $EA \subset RF$). Indeed, if $F_1 \subset D^n$, the inclusion is clear; otherwise, F_1 has a basis over D of the form $(f_0, 1), (f_1, 0), \ldots, (f_l, 0)$ with f_i in D^n; then each element of $RF_1 \cap R^n$ is of the form for some r_i in R: $r_0(f_0, 1) + r_1(f_1, 0) + \cdots + r_l(f_l, 0)$; then r_0 must be 0, so that this element is in $R(F_1 \cap D^n)$. This proves the required inclusion.

For the dimensions, it is enough to show that $\dim(E) \geq \dim(F)$ since a strict inequality implies that A is associated over D to a hollow matrix, hence not full. We claim that we cannot have simultaneously: (*) $p(E_1)$ is not a subset of $\operatorname{Ker}(v)$ and F_1 is a subset of D^n. Indeed, if the first condition holds, then for some $\alpha \in D$ and $e \in D^n$, we have $(e, \alpha) \in E_1$ and $ev \neq 0$, hence $(eA + \alpha u, ev) \in RF_1$ which contradicts the second condition. We distinguish now two cases.

Suppose that p is injective on E_1; then $\dim(p(E_1)) = \dim(E_1) > \dim(F_1)$. If $p(E_1) \subset \mathrm{Ker}(v)$, then $E = p(E_1)$ and $\dim(E) = \dim(E_1) \geq \dim(F)$, the latter inequality following from the definition of F. If $p(E_1)$ is not a subset of $\mathrm{Ker}(v)$, then by (*), F_1 is not a subset of D^n, so that $\dim(E) = \dim(E_1) - 1$, and $\dim(F) \leq \dim(F_1)$ which implies the desired inequality.

Suppose now that p is not injective on E_1. This implies that $(0,1)$ is in E_1, so that upon taking its image under $\bar{A}$, we find that $(u,0)$ is in F_1, hence $u \in F_1 \cap D^n$. Then $F = F_1 \cap D^n$ and once again we must have $\dim(E) \geq \dim(F)$: indeed, either $p(E_1) \subset \mathrm{Ker}(v)$ and thus $\dim(E) = \dim(E_1) - 1 \geq \dim(F_1) \geq \dim(F)$, or $p(E_1) \not\subset \mathrm{Ker}(v)$, thus by (*), $F_1 \not\subset D^n$ and $\dim(E) = \dim(E_1) - 2 \geq \dim(F_1) - 1 = \dim(F)$. □

Proof of Theorem 1.1. For the if part, it is enough to show that if (P,Q) is a morphism from (u,A,v) to (u',A',v'), then these representations represent the same element. Note that if P (or equivalently Q) is an invertible matrix, then the conclusion follows, and we then have $uA^{-1}v = u'Q^{-1}(PA'Q^{-1})^{-1}Pv' = u'A'^{-1}v'$.

In general, we can combine (P,Q) with isomorphisms (S',T') and (S'',T'') to yield a morphism $(S'PS'',T'QT'')$, which for a suitable choice of S',S'',T',T'' takes the form $(I_r \oplus 0, I_r \oplus 0)$, where r is the common rank of P and Q. So, we may suppose that (P,Q) has this latter form, and if we correspondingly partition ρ as

$$\rho = \left(\begin{pmatrix} u_1 & u_2 \end{pmatrix}, \begin{pmatrix} A_1 & A_2 \\ A_3 & A_4 \end{pmatrix}, \begin{pmatrix} v_1 \\ v_2 \end{pmatrix} \right),$$

and similarly for ρ', we find that $u_1 = u_1'$, $u_2' = 0$, $v_1 = v_1'$, $v_2 = 0$, $A_1 = A_1'$, $A_3 = 0$, $A_2' = 0$. Hence ρ has the form:

$$\rho = \left(\begin{pmatrix} u_1 & u_2 \end{pmatrix}, \begin{pmatrix} A_1 & A_2 \\ 0 & A_4 \end{pmatrix}, \begin{pmatrix} v_1 \\ 0 \end{pmatrix} \right),$$

which implies that it represents $u_1A_1^{-1}v_1$, and ρ' has the form:

$$\rho' = \left(\begin{pmatrix} u_1 & 0 \end{pmatrix}, \begin{pmatrix} A_1 & 0 \\ A_3' & A_4' \end{pmatrix}, \begin{pmatrix} v_1 \\ v_2' \end{pmatrix} \right),$$

and represents therefore the same element of the free field.

Conversely, let (u,A,v) and (u',A',v') be two pure and linear representations that are equivalent. Then the representation $((u,u'),\bar{A},(v,-v'))$ where $\bar{A}$ is the diagonal sum of A and A', represents 0 so that by the lemma, there exist D-subspaces E,F of $D^{n+n'}$ of the same dimension such that $E \subset \mathrm{Ker}(v,-v')$, $(u,u') \in F$ and $E\bar{A} \subset RF$. Let P and Q be the projections $D^{n+n'} \to D^n$, $D^{n+n'} \to D^{n'}$. Consider the representations $((u,u'),B,(v,0))$ and $((u,u'),B,(0,v'))$ with underlying spaces E and F (with the abuse of language described before Theorem 1.1). These representations are equal since the restriction of $(v,0)$ and $(0,v')$ to E are equal because $E \subset \mathrm{Ker}(v,-v')$. Moreover, (P,P) is a morphism from the representation $((u,u'),B,(v,0))$ onto the representation (u,A,v), where B is the restriction of $\bar{A}$ to E. Similarly, (Q,Q) is a morphism of $((u,u'),B,(0,v'))$ onto (u',A',v').

Hence, we can pass from (u, A, v) to (u', A', v') by an inverse morphism followed by a morphism. $\square$

The elements 0 and 1 of the free field have the representations

$$\mathbf{0} = (\ ,\ ,\ ), \mathbf{1} = (1, 1, 1) \tag{3}$$

of dimension 0 and 1 respectively. If f and f' are elements of the free field represented by $c + (u, A, v)$ and $c' + (u', A', v')$, then their sum and their product are represented by:

$$f + f' = c + c' + \left(\begin{pmatrix} u & u' \end{pmatrix}, \begin{pmatrix} A & 0 \\ 0 & A' \end{pmatrix}, \begin{pmatrix} v \\ v' \end{pmatrix} \right); \tag{4}$$

$$ff' = cc' + \left(\begin{pmatrix} u & cu' \end{pmatrix}, \begin{pmatrix} A & -vu' \\ 0 & A' \end{pmatrix}, \begin{pmatrix} vc' \\ v' \end{pmatrix} \right). \tag{5}$$

Furthermore, if $c = 0$, the inverse of $f \neq 0$ is represented by:

$$\left(\begin{pmatrix} 0 & 1 \end{pmatrix}, \begin{pmatrix} A & -v \\ u & 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right). \tag{6}$$

(See [10, 4.3]). Thus we obtain the following result.

Corollary 1.3. *The elements of the free field $D_k \langle\!\langle X \rangle\!\rangle$ are given by equivalence classes of pure and linear representations, with the field operations given by* (3), (4), (5) *and* (6).

We say that the linear and pure representation (u, A, v) is *minimal* if it has the smallest possible dimension among all pure and linear representations of a given element of the free field.

Theorem 1.4. *If $\rho = (u, A, v)$ and $\rho' = (u', A', v')$ are equivalent pure and linear representations, of which the first is minimal, then the second is isomorphic to a representation (u_1, A_1, v_1) which has the block decomposition*

$$u_1 = \begin{pmatrix} \times & u & 0 \end{pmatrix}, A_1 = \begin{pmatrix} \times & 0 & 0 \\ \times & A & 0 \\ \times & \times & \times \end{pmatrix}, v_1 = \begin{pmatrix} 0 \\ v \\ \times \end{pmatrix}.$$

In other words, ρ is isomorphic with a subrepresentation of a factor (respectively to a factor of a subrepresentation) of ρ'.

This result will be proved by establishing first some confluence properties of morphisms.

Lemma 1.5. (1) *Each morphism is the product of a surjective morphism followed by an injective one.*

(2) *If ρ, ρ_1 and ρ' are representations with injective (respectively surjective) morphisms $\rho \to \rho_1 \leftarrow \rho'$ (respectively $\rho \leftarrow \rho_1 \to \rho'$), then there exists a representation ρ_2 and injective (respectively surjective) morphisms $\rho \leftarrow \rho_2 \to \rho'$ (respectively $\rho \to \rho_1 \leftarrow \rho'$).*

(3) *If ρ, ρ_1 and ρ' are representations with morphisms $\rho \to \rho_1 \leftarrow \rho'$ (respectively $\rho \leftarrow \rho_1 \to \rho'$), of whom the first is surjective (respectively injective) and the second injective (respectively surjective), then there exists a representation ρ_2 and morphisms $\rho \leftarrow \rho_2 \to \rho'$ (respectively $\rho \to \rho_1 \leftarrow \rho'$), of whom the first is injective (respectively surjective) and the second surjective (respectively injective).*

Proof. (1) This has been implicitly proved in the first part of the proof of Theorem 1.1.

(2) We prove only the assertion not in parenthesis (the other is obtained by duality). Let (P, Q) and (P', Q') be the two injective morphisms. Let n and n_1 and n' be the dimensions of ρ, ρ_1 and ρ', and define $E = D^n P$, $E' = D^{n'} P'$, $F = D^n Q$ and $F' = D^{n'} Q'$. We have $uQ = u_1 = u'Q'$ and $v = Pv_1$, $v' = P'v_1$. If $x \in E \cap E'$, then $x = aP = a'P'$ for some $a \in D^n$, $a' \in D^{n'}$; hence $xA_1 = aPA_1 = aAQ \in RF$, and similarly $xA_1 \in RF'$. Hence A_1 maps $E \cap E'$ into $R(F \cap F')$, u_1 is in $F \cap F'$, and we obtain a representation ρ_2 by taking bases of these two spaces, with $\rho_2 = (u_2 = u_1, A_2 = A_1|E \cap E', v_2 = v_1|E \cap E')$. Now we have an injective morphism (S, T) from ρ_2 into ρ defined by: for $x \in E \cap E'$ (respectively $y \in F \cap F'$), xS (respectively yT) is the unique pre-image in D^n of x under P (respectively Q), which is well-defined since P (respectively Q) is injective. Then $u = u_1 T = u_2 T$, $v_2 = Sv$ since for $x \in E \cap E'$, we have $x = aP$ for some $a \in D^n$, thus $a = xS$ and $xv_2 = aPv_2 = aPv_1 = av = xSv$; furthermore, we have $xSA = aA = aAQT = aPA_1T = xA_1T = xA_2T$. Thus $SA = A_2T$, which implies that (S, T) is an injective morphism from ρ_2 into ρ. Similarly, we have an injective morphism ρ_2 into ρ', which completes the proof of this part.

(3) We prove only the first assertion. Taking the same notations as in (2), let $E_2 = D^{n'} P'P^{-1}$ and $F_2 = D^{n'} Q'Q^{-1}$. Let $u_2 = u$, and $v_2 = v|E_2$. Furthermore, note that if $x \in E_2$, then there exists a unique $a' \in D^{n'}$ such that $xP = a'P'$; thus $xAQ = xPA_1 = a'P'A_1 = a'A'Q' \in R^{n'}Q'$, hence $xA \in RF_2$ and we can define $A_2 = A|E_2$, and this defines a representation $\rho_2 = (u_2, A_2, v_2)$. Define S respectively T to be the canonical injections from E_2 respectively F_2 into D^n, and S', T' by $S' = PP'^{-1}$, $T' = QQ'^{-1}$, which are well-defined surjective linear mappings from E_2 respectively F_2 onto $D^{n'}$, since P' and Q' are injective and P and Q are surjective. We have $u_2T' = uQQ'^{-1} = u_1Q'^{-1} = u'$ since $u_1 = u'Q'$, and for $x \in E_2$ as above, $xS'v' = xPP'^{-1}v' = a'v' = a'P'v_1 = xPv_1 = xv = xv_2$ so that $S'v' = v_2$; also $xA_2T' = xA_2QQ'^{-1} = xAQQ'^{-1} = xPA_1Q'^{-1} = a'P'A_1Q'^{-1} = a'A'Q'Q'^{-1} = a'A' = a'P'P'^{-1}A' = xPP'^{-1}A' = xS'A'$ so that $A_2T' = S'A'$ and (S', T') is a surjective morphism from ρ_2 onto ρ'. Now we have $u_2T = u_2 = u$, $xSv = xv = xv_2$, so that $Sv = v_2$, and finally $xA_2T = xAT = xA = xSA$. This shows that (S, T) is an injective morphism from ρ_2 into ρ. □

Proof of Theorem 1.4. Let us call a chain of morphisms and inverse morphisms from ρ_1 to ρ_2 *decreasing* if each direct morphism is surjective and each inverse morphism is injective (so that at each step of the chain, the dimension does not increase). We claim that there is a decreasing chain from ρ' to ρ. By assumption, there is a chain of length n of morphisms and inverse morphisms between ρ and ρ'. Each morphism may be decomposed into the product of a surjective one followed by an injective one, according to the first part of the lemma. Then, applying the second part of the lemma, we find representations ρ_1 and ρ_2 with decreasing chains of length 2 from ρ to ρ_1 and ρ' to ρ_2, and a chain of length $n-2$ from ρ_2 to ρ_1. Since ρ is minimal, ρ is isomorphic with ρ_1; by induction, there is a decreasing chain of length $n-2$ from ρ_2 to ρ_1, or equivalently to ρ, which implies the claim.

Now we have a decreasing chain from ρ' to ρ of length n. By applying the third part of the lemma (either assertion, depending whether the first step is surjective or the inverse of an injective morphism), we find a decreasing chain of length $n-1$, and conclude by induction that there exists a decreasing chain of length 0, 1 or 2 from ρ' to ρ. But this implies the theorem in view of the third part of the lemma. □

Corollary 1.6. *Two pure and linear representations of the same element of the free field are minimal if and only if they are isomorphic.*

We recall from [9] that an $m \times n$ matrix C over a ring is said to be *left prime* if in any equation $C = PQ$, where P is square, P has necessarily a right inverse; *right prime* matrices are defined correspondingly. We say that the representation (u, A, v), or the block (1), is *prime* if the matrix (A, v) is left prime and the matrix $(A^T, u^T)^T$ is right prime.

In (2), we may take the matrices A'_i, A''_i of order $n \times r_i$ and $r_i \times n$, with r_i minimal. Then, we say that the linear representation $\rho = (u, A, v)$, or block (1), with A as in (2), is *monic* if the matrix $(A'_1, \ldots, A'_d, v)$ has a right inverse, and the matrix $(A''^T_1, \ldots, A''^T_d, u^T)^T$ has a left inverse. Equivalently, the columns (respectively rows) of $A'_1, \ldots, A'_d$ and v (of $A''_1, \ldots, A''_d$ and u) span the whole D-space of columns (respectively rows) over D. This is well-defined.

The following result gives an intrinsic characterization of minimal representations. Note that a characterization of minimal representations has been given in [11, Corollary 2, p. 527 and Proposition 7, p. 528], but it uses the elements of the free field.

Theorem 1.7. *A linear and pure representation $\rho = (u, A, v)$ is minimal if and only if it is prime and monic.*

Proof. If ρ is not minimal, then there exists a minimal representation ρ_0 and a representation ρ' and morphisms $\rho \to \rho' \leftarrow \rho_0$, where the first is surjective and the second is injective (Theorem 1.4), and at least one of them is not an isomorphism. We may suppose that the second one is not an isomorphism (the other case is symmetric). This implies that (by applying an isomorphism) we may suppose that ρ has a nontrivial block decomposition

$$u = (u_1 \quad 0), A = \begin{pmatrix} B & 0 \\ \times & C \end{pmatrix}, v = \begin{pmatrix} \times \\ \times \end{pmatrix},$$

with B, C square. If C is not invertible over R, then $(A^T, u^T)^T$ is not right prime, since

$$\begin{pmatrix} A \\ u \end{pmatrix} = \begin{pmatrix} B & 0 \\ \times & 1 \\ u_1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & C \end{pmatrix}.$$

If C is invertible over R, then it cannot be left monic in the sense of [10] since the homogeneous part of degree 1 of C (which is of degree ≤ 1) is then right regular, (see [10, p. 293]). But then ρ is not monic either.

Suppose now that ρ is minimal. Then it must be monic; indeed, if for example $(A'_1, \ldots, A'_d, v)$ has no right inverse, then by multiplying at the left by an invertible matrix P over D, we may annihilate the first row of this matrix. Thus

$$PA = \begin{pmatrix} w \\ A_1 \end{pmatrix}, Pv = \begin{pmatrix} 0 \\ v' \end{pmatrix},$$

where w is over D, and by multiplying at the right by an invertible matrix Q over D (which amounts to make column operations on PA) to bring w to the form $(1, 0, \ldots, 0)$, we obtain the block decomposition

$$uQ = (\alpha \quad u'), PAQ = \begin{pmatrix} 1 & 0 \\ \times & A' \end{pmatrix}, Pv = \begin{pmatrix} 0 \\ v \end{pmatrix},$$

which shows that ρ is equivalent to (u', A', v') and not minimal.

Suppose now that we have $(A, v) = PB$ for some matrices P, B over R and with P square. Note that we may write $B = (A', v')$ for a square matrix A' and a column v' over R. Hence $A = PA'$. In particular, P is then full since A is, and hence not a zero-divisor. Thus P is right regular (i.e not a left zero-divisor, see [9, p. xix]). Also, B is left regular: otherwise B would be left associated to a matrix with a zero row (by the trivializability of relations in a semifir; see [9, p. 67] for the definition of a semifir, and pp. 64–65 for the notion of trivializability); this row and the corresponding column of P could then be omitted, and this would show A to be nonfull.

We now need to strengthen Lemma 6.3.4 in [10]: assume that the entries of the ith row of C have degree at most d_i; in the proof assign to y_i the degree $d - d_i$, where $d = \max\{d_1, \ldots, d_m\} + 1$ (to ensure that the y's have positive degrees); now the argument proceeds as before. So, we may suppose that A' is of degree ≤ 1 and v' of degree 0, that is over D.

Then $(u, A, v) = (u, PA', Pv')$ so that (u, A', v') is a pure and linear representation of our free field element, of the same dimension as (u, A, v). Therefore by Corollary 1.6, the two representations are isomorphic and we obtain $A' = UPA'V$ for some invertible matrices U, V over D. Now we apply Theorem 3.3.7 of [9] and find that P must be invertible over R: indeed, A' is full, hence is the product of m atomic factors; in the equation $A' = UPA'V$, the number of atomic factors must be the same on both sides, and that leaves nothing for P, U, V, so they must be units.

Thus ρ is prime. □

2. The Primary Decomposition

It is well-known that if $f(x)$ is a rational function in x over k, then it has a unique decomposition

$$f(x) = P(x) + \sum_{i=1}^{i=m} \frac{A_i(x)}{B_i(x)}, \tag{7}$$

where P, A_i and B_i are polynomials. Each B_i is nonzero and prime to A_i, $\deg(A_i) < \deg(B_i)$. All the B_i are pairwise coprime and m is maximal subject to these conditions. This is the well-known *primary decomposition* of $f(x)$, and P is the *integral part* of f. Our aim is to extend this notion to elements of the free field $D_k \langle\!\langle X \rangle\!\rangle$.

By the inertia theorem [9], Theorem 2.9.15, the tensor ring $D_k\langle X\rangle$ is honestly embedded in its power series completion (honestly means that the embedding preserves the fullness of matrices) and a minimal *fraction* (i.e representation) (u, A, v) can be written as a power series precisely when A_0 is invertible, with the notations of (2), and then it can be taken to be I. Let us call a representation with this property *unital.* The fraction lies in $D_k\langle X\rangle$ if and only if A is invertible over this ring. It follows from the construction of the minimal representation by left transductions in [11] (see Lemma 6, p. 520) that A may be chosen *upper unitriangular*, that is, upper triangular with 1's on the diagonal. Let us denote by e_i the canonical row vector of appropriate dimension. We define the *rank* of an element f of the free field as the dimension $r(f)$ of any of its minimal representations. We thus obtain the following result.

Proposition 2.1. (i) *An element of the free field is a power series if and only if in any minimal representation, the constant term of its pivot matrix is invertible, and there is then a minimal representation which is unital.*

(ii) *An element of the free field is a polynomial if and only if in any unital minimal representation, the matrix $\sum_{i=1,\dots,d} A_i' x_i A_i''$ is nilpotent; there is then a minimal representation with a unitriangular pivot matrix.*

(iii) *Any element f of the free field of rank n has a minimal representation with $u = e_1$, $v = e_n^T$; thus f is the $(1, n)$-entry of A^{-1}.*

(iv) *If moreover f is a polynomial, A may be taken unitriangular, up to multiplying f by some nonzero element of D.*

Proof. It remains to prove (iii) and (iv). If (u, A, v) is a representation of dimension n, then so is (uP, QAP, Qv) for invertible matrices over D. We may choose P and Q so that $uP = e_1, Qv = e_n^T$. For (iv), we already know that A is unitriangular. Suppose that $v = (v_1, \dots, v_r, 0, \dots, 0)^T$, where v_r is the last nonzero entry; then we can reduce this entry to 1 by dividing the rth row of A and v by v_r; moreover, we multiply the rth column of u and A by v_r so that A remains unitriangular. If we now add appropriate multiples of the rth row to earlier rows of A and v, we can reduce v to the form e_r^T and still leave A upper triangular. If $r < n$, we see that ρ has the form

$$\left((u', u''), \begin{pmatrix} A' & B \\ 0 & A'' \end{pmatrix}, e_r^T\right),$$

where A' is square of size $r \times r$. Hence ρ is equivalent to $(u', A', (0, \dots, 0, 1)^T)$ of dimension r, which contradicts the fact that ρ was minimal. Hence $r = n$, and arguing symmetrically with u, we can bring u to the form e_1 at the cost of replacing $v = e_n^T$ by a nonzero scalar multiple. This proves (iv). □

Note that when $D = k$, by a result of Lewin [19], the free field embeds naturally in the ring of Malcev-Neumann series on the free group, and by a result of Fliess [13] (see also [5]), the intersection of this ring with the ring $k\langle\langle X\rangle\rangle$ of formal power series is exactly the ring of rational series (see [4] for the latter notion). It seems likely that a similar result holds in the general case when $D \neq k$.

The rank of a sum of elements of the free field never exceeds the sum of the ranks; this is a consequence of Eq. (4) in Sec. 1. We say that the elements $f_1, \dots, f_s$ of the free field are *disjoint* if $r(f_1 + \dots + f_s) = r(f_1) + \dots + r(f_s)$. In the one-variable case, one has the following result.

Proposition 2.2. (1) *The rank of* $\frac{A(x)}{B(x)}$, *where A and B are pairwise coprime, is deg(B) if deg(A) $<$ deg(B), and deg(A) $+ 1$ if deg(A) $\geq$ deg(B).*
(2) *Let* $f_i(x) = \frac{A_i(x)}{B_i(x)}$ $(i = 1, \dots, s)$ *be s rational fractions with A_i, B_i pairwise coprime. If they are disjoint, then for at most one i, deg(A_i) $\geq$ deg(B_i). Suppose that deg(A_i) $<$ deg(B_i) for $i = 1, \dots, s-1$; then they are disjoint if and only if $B_1, \dots, B_s$ are pairwise coprime.*

Proof. (1) When the constant term of B is nonzero, the fraction is a formal power series; its rank is the rank of its Hankel matrix, and the result is well-known (see e.g. [4, Corollary IV.1.3]). The general case is a slight generalization of the latter, and we omit the proof.

(2) It is enough to prove this for $s = 2$. Suppose that the condition does not hold, by Euclidean division, we have $\frac{A_i}{B_i} = Q_i + \frac{R_i}{B_i}$ (with evident notations), hence $f_1 + f_2 = Q_1 + Q_2 + \frac{R_1}{B_1} + \frac{R_2}{B_2}$. Using (1) several times, we find that $r(Q_1 + Q_2) = \deg(Q_1 + Q_2) + 1 \leq \max(q_1, q_2) + 1$ (small letters indicate degrees) $= \max(a_1 - b_1, a_2 - b_2) + 1 = a_1 - b_1 + 1$ (say), and $r(f_1 + f_2) \leq r(Q_1 + Q_2) + r(\frac{R_1}{B_1}) + r(\frac{R_2}{B_2}) = r(Q_1 + Q_2) + b_1 + b_2 = q_1 + 1 + b_1 + b_2 = a_1 - b_1 + 1 + b_1 + b_2 = a_1 + b_2 + 1$. This is strictly smaller than $r(f_1) + r(f_2) = a_1 + a_2 + 2$ (by assumption and 1), since $b_2 \leq a_2$.

Suppose now that $a_1 < b_1$. Let C be the gcd of B_1, B_2 and write $B_i = CB_i'$. Then $f_1 + f_2 = \frac{A_1B_2' + A_2B_1'}{CB_1'B_2'}$. If $a_2 < b_2$, then $\deg(A_1B_2' + A_2B_1') \leq \max(a_1 + b_2', a_2 + b_1') < \max(b_1 + b_2', b_2 + b_1') = c + b_1' + b_2' = \deg(CB_1'B_2')$; thus by (1), $r(f_1 + f_2) = c + b_1' + b_2'$ and this is equal to $r(f_1) + r(f_2) = 2c + b_1' + b_2'$ if and only if $c = 0$, i.e. B_1 and B_2 are pairwise coprime. If on the contrary $b_2 \leq a_2$, then $a_1 + b_2 < b_1 + a_2$. And subtracting c, we find $a_1 + b_2' < b_1' + a_2$, which implies that $\deg(A_1B_2' + A_2B_1') = a_2 + b_1' \geq b_2 + b_1' = c + b_1' + b_2' = \deg(CB_1'B_2')$; hence $r(f_1 + f_2) = a_2 + b_1' + 1$ and this is equal to $r(f_1) + r(f_2) = b_1 + a_2 + 1 = c + b_1' + a_2 + 1$ if and only if $c = 0$. □

For our category of pure and linear representations, there is a forgetful functor which to every representation associates its pivot matrix and to each morphism its action on the pivots. Hence, the objects of our new category are the linear matrices over $D_k\langle X\rangle$. This is easily seen to be an abelian category in which all objects satisfy both chain conditions on subobjects; hence the Krull–Remak–Schmidt theorem applies (cf. [20, Theorem 5.1.4]), which shows that each pivot can be written as a direct sum of indecomposable matrices in just one way, up to association over D and permutation of the factors. Thus, if our block has the form

$$\left((u_1 \quad u_2), \begin{pmatrix} A_1 & 0 \\ 0 & A_2 \end{pmatrix}, \begin{pmatrix} v_1 \\ v_2 \end{pmatrix}\right),$$

then the corresponding free field element can be written as a sum of two fractions (u_1, A_1, v_1) and (u_2, A_2, v_2). An element of the free field represented by a block with an indecomposable pivot will itself be called *indecomposable* or *primary*; what has been said shows that every element of the free field can be expressed as a sum of indecomposable elements.

The result below extends a result of Fliess ([14, Theorem 2.2.4]), who proved it for rational series; he used the classical Krull–Remak–Schmidt theorem.

Theorem 2.3. *Each element f of the free field may be uniquely written as a sum of disjoint primary elements; at most one of them is a polynomial.*

Observe that by Proposition 2.2, the decomposition of the theorem coincides with the decomposition (1) in the one-variable case. Moreover, the unique polynomial in the sum, if any, may be called the *integral part* of f.

Proof. Let $\rho = (u, A, v)$ be a minimal representation of f.

The pivot A is a direct sum of indecomposable pivots $A_i, i = 1, \dots, m$; then we have corresponding decompositions $u = \oplus_i u_i, v = \oplus_i v_i$, which define representations $\rho_i = (u_i, A_i, v_i)$ of primary elements f_i and $f = \sum_i f_i$. These representations are minimal since ρ is, and the f_i are disjoint for the same reason.

Conversely, suppose that $f = \sum_{i=1}^{i=m'} f'_i$, with the f'_i disjoint and primary. Taking a minimal representation $\rho'_i = (u'_i, A'_i, v'_i)$ for f'_i, their direct sum is a representation of f. It must be minimal by disjointness of the f'_i. Hence, the pivot matrix A is isomorphic to the direct sum of the indecomposable pivot matrices A'_i and we deduce from the Krull-Remak-Schmidt theorem that $m = m'$ and that there exists an isomorphism (P_i, Q_i) from A_i onto A'_i. The two representations $\oplus_i \rho_i$ and $\oplus_i \rho'_i$ are minimal representations of f, and hence isomorphic by Corollary 1.6; applying the isomorphism, we may suppose that both are equal to ρ and that $\oplus(P_i, Q_i)$ is an automorphism of ρ. In particular, $Q = \oplus_i Q_i$ is an automorphism of D^n, where n is the dimension of ρ. Moreover $u = \oplus_i u_i = \oplus_i u'_i$. Applying Q, we find that $\oplus_i u'_i = u = uQ = \oplus_i uQ_i$; thus, we see by the directness of the sum that uQ_i must be equal to u'_i. Similarly, $v_i = P_i v'_i$ shows that (P_i, Q_i) is an isomorphism from ρ_i onto ρ'_i and hence $f_i = f'_i$.

To conclude it is enough to show that two nonzero polynomials are never disjoint, let f and g be any nonzero polynomials; we may take their minimal representations as in Proposition 2.1 (iv): their pivots are upper unitriangular matrices A, B, and

$f+g$ has the representation

$$\left((1,0,\dots,0,1,0,\dots,0), \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}, (0,\dots,0,1,0,\dots,0,1)^T\right).$$

Let f, g have ranks m, n respectively, so that A, B have orders m, n. In the block for $f+g$, we subtract row $m+n$ from row m and then subtract column 1 from column $m+1$. This reduces the row and column of the block to e_1, e_{m+n}^T respectively. Moreover, the $(m+1)-st$ column has a diagonal entry 1 and another entry -1, so we can reduce the nondiagonal entries of row $m+1$ to zero by adding multiples of column $m+1$ to later columns. As a result, we get a matrix in which row $m+1$ has the diagonal entry 1 and all other entries equal to zero; moreover, the resulting matrix is still linear and unitriangular. This means that the $(m+1)$-st row and column can be omitted. Next, we can reduce column m to zero except for the 1 on the diagonal, by adding multiples of row m to earlier rows. Thus, we find for any polynomials the inequality $r(f+g) \le r(f)+r(g)-2$ (this bound is sharp by taking $f = x^{m-1}, g = y^{n-1}$, of respective rank m, n, while $f+g$ has rank $m+n-2$). Hence f and g are not disjoint. □

Let f have the (nonpure) linear representation $c+(u, A, v)$, and suppose that its dimension is smallest possible. Then it is not true in general that c is the integral part of f. Indeed, we may take $f = 1+(1-x)^{-1}y$ which has the representation of minimal dimension $1+((1,0), \begin{pmatrix} 1-x & -y \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix})$. The integral part of f is 0 since f has the pure linear representation $((1,1), \begin{pmatrix} 1-x & -y \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix})$ which is minimal and indecomposable.

3. The Triviality of Rational Identities

Consider the following rational identity:

$$y^{-1}+y^{-1}(z^{-1}x^{-1}-y^{-1})^{-1}y^{-1} = (y-zx)^{-1}. \tag{8}$$

It is not immediately obvious that this is an identity. But we clearly have

$$\begin{aligned}(z^{-1}x^{-1}-y^{-1})(y-xz)+y^{-1}(y-xz)\\ &= (z^{-1}x^{-1}-y^{-1})y-1+y^{-1}xz+y^{-1}(y-xz)\\ &= (z^{-1}x^{-1}-y^{-1})y.\end{aligned}$$

If we now multiply by $y^{-1}(z^{-1}x^{-1}-y^{-1})^{-1}$ on the left and by $(y-xz)^{-1}$ on the right, we obtain (1).

We shall prove in this section that every identity in the free field can be trivialized in this way, using only algebraic operations and the fact that f^{-1} is the inverse of f for each nonzero element f of the free field.

We recall that a ring is said to be *weakly finite* if for any two square matrices A and B of the same order, $AB = I$ implies $BA = I$. Clearly any field is weakly finite; our first observation is that the same holds for *local* rings (rings in which the set of all the nonunits is an ideal, the Jacobson radical).

Lemma 3.1. *Every local ring is weakly finite.*

Proof. Let R be a local ring with residue-class field K, its quotient by the unique maximal ideal, with canonical homomorphism $u : R \to K$. Given square matrices A and B such that $AB = I$, we have $u(A)u(B) = I$, so $u(A)$ is invertible over K with inverse $u(B)$ and hence $BA = I + C$, where C has entries in the maximal ideal of R. Since the Jacobson radical of a matrix ring consists of all matrices over the Jacobson radical of the original ring ([17, Theorem 3, p. 11]), it follows that $I + C$ is invertible and $(I + C)^{-1}BA = I$, so A has a left inverse which of course must equal B, the right inverse, showing that R is weakly finite. □

Consider the free algebra $D_k\langle X\rangle$ and its universal field of fractions $D_k\langle\!\langle X\rangle\!\rangle$, the free field, with the natural embedding $\phi : D_k\langle X\rangle \to D_k\langle\!\langle X\rangle\!\rangle$. Starting from $D_k\langle X\rangle$, we form a ring $R(X) = R(X, D, k)$ in the following way: for $n = 0$, (R_n, u_n) is $(D_k\langle X\rangle, \phi)$, and for any n, R_{n+1} is the free product over k of R_n and the (noncommutative) polynomial k-algebra $k\langle x_f | f \in R_n, u_n(f) \neq 0\rangle$, divided by the relations $x_f f = f x_f = 1$; in other words, R_{n+1} is obtained by adjoining to R_n inverses of those elements who do not lie in $\operatorname{Ker}(u_n)$. Then u_{n+1} is the natural extension of u_n to R_{n+1}. There is a natural homomorphism $R_n \to R_{n+1}$, and $(R(X), u)$ is the inductive limit of the (R_n, u_n). Thus u is a homomorphism of $R(X)$ into $D_k\langle\!\langle X\rangle\!\rangle$ where every element of $R(X)$ not in $\operatorname{Ker}(u)$ is a unit and it follows that $R_k(X)$ is a local ring. The nonzero elements of $\operatorname{Ker}(u)$ may be regarded as the "nontrivial" relations holding in the free field; as we shall now show, there are no such relations.

Theorem 3.2. *The canonical map $u : R(X) \to D_k\langle\!\langle X\rangle\!\rangle$ is an isomorphism.*

Proof. The surjectivity follows from the definition of u. It remains to show that u is injective, i.e. for any rational expression f in $R(X)$, $f = 0$ if $u(f) = 0$. By the construction of the free field, there exist matrices b, A, c over $D_k\langle X\rangle$ with A square of order n, b a row of length n, c a column of length n such that A is invertible in $R(X)$ and that $f = bA^{-1}c$ (see [10, 4.2]). Thus $bu(A)^{-1}c = 0$, so that by Malcolmson's criterion ([10, Theorem 4.5.11]), the matrix

$$\begin{pmatrix} A & c \\ -b & 0 \end{pmatrix} \tag{9}$$

is nonfull. Now the matrix (2) is stably associated to f over $R(X)$:

$$\begin{pmatrix} I & 0 \\ 0 & f \end{pmatrix} = \begin{pmatrix} A^{-1} & 0 \\ bA^{-1} & 1 \end{pmatrix} \begin{pmatrix} A & c \\ -b & 0 \end{pmatrix} \begin{pmatrix} I & -A^{-1}c \\ 0 & 1 \end{pmatrix}.$$

It follows that the matrix on the left is nonfull over $R(X)$, say

$$\begin{pmatrix} I & 0 \\ 0 & f \end{pmatrix} = \begin{pmatrix} P \\ p \end{pmatrix} \begin{pmatrix} Q & q \end{pmatrix},$$

where P and Q are square of order n, p is a row and q a column, both of length n, and all four matrices over $R(X)$. We have $PQ = I$, $Pq = 0$ and $pQ = 0$, $pq = f$. By Lemma 3.1; P and Q are invertible so that $p = 0$ and $f = pq = 0$ as we wished to show. □

We remark that this result answers a question of Bergman [3]; he asks whether each rational identity $f = 0$ in the free field is an algebraic consequence of the fact that g^{-1} is the inverse of g, for each nonzero element g of the free field. However, this cannot be proved using only those elements that are actually inverted in f. Otherwise, each "absolute rational identity", i.e. each identity in the free field would also be valid in any ring, which is not so; for example in the ring $k < x, y > /(xy-1)$, the identity $y(xy)^{-1}x = 1$ does not hold. Generally, it can be shown (by methods similar to that used to prove Theorem 3.2) that every absolute rational identity holds in every weakly finite ring (see [8, Theorem 5.5]).

Amitsur's construction of the free field [1] is similar to that of $R(X)$, but instead of $D_k \langle\!\langle X \rangle\!\rangle$ he uses an ultraproduct of skew fields over k; he then shows that this may (for infinite k) be replaced by a skew field infinite-dimensional over its centre which contains k.

Note that an analogue to the theorem has been proved by Krob [18] for non-commutative rational power series; there he uses only rational expressions which represent series, that is, expressions involving only inverses of expressions whose constant term (which may be defined formally on the expression) is nonzero.

4. The Word Problem in Free Fields

We have seen in Sec. 1 that the elements of the free field can be formed either by repeated ring operations together with inversion, or by inverting a full matrix. This reduces the word problem for free fields to the problem of deciding whether a given square matrix over the free algebra is full. By linearization and enlargement, it is enough to test the linear matrices. In this form, the question has been answered in 6.6 of [10] by means of the specialization lemma. Below we give another proof for the special case $D = k$.

Our task is to find an algorithm for deciding whether a linear matrix over $k\langle X\rangle$ is full. Let M be a linear square matrix over $k\langle X\rangle$, and write $M = M_1 + \sum_{x\in X} xM_x$ where M_1 and the M_x are matrices over k. Let A and B be generic matrices of order n whose entries are commutative variables, and denote by $k[a, b]$ the corresponding k-algebra in the variables a_{ij}, b_{ij}. The next result reduces our problem to one in the polynomial ring.

Theorem 4.1. *For each r in $\{1,\ldots,n\}$, denote by I_r the ideal of $k[a,b]$ generated by the polynomials $det(A) - 1, det(B) - 1$, and the coefficients of each $x \in X$ in the i, j entries of the matrix AMB for $1 \le i \le r, r \le j \le n$. Then the linear matrix M is full if and only if for each $r \in \{1,\ldots,n\}$, the ideal I_r is equal to $k[a,b]$.*

This result implies that one can decide if such a matrix is full, since by Hermann's, Gordan's or Buchberger's algorithm (see [16] or the theory of Gröbner bases, Chap. 5 in [2], or [12]), one can effectively test if 1 belongs to an ideal of (commutative) polynomials given by a finite number of generators.

Proof. Let $\bar{k}$ be the algebraic closure of k. Since the embedding $k\langle X\rangle \to \bar{k}\langle X\rangle$ is honest, i.e. preserves full matrices ([10, Theorem 6.4.6], it follows that M is full if and only if M is full when considered as an element of $\bar{k}\langle X\rangle$. Now, by Corollary 6.3.6 in [10], M is nonfull if and only for some $r \in \{1, \ldots, n\}$, there exist invertible matrices A, B over $\bar{k}$, which we may assume to have determinant 1 such that AMB has rectangle of zeros of size $r \times (n+1-r)$ in the upper right-hand corner. Equivalently, the ideal I_r has a zero over $\bar{k}$. So M is full if and only if for each r, the ideal I_r has no zero, that is, I_r contains 1 when considered as ideal in $\bar{k}[a,b]$; but this is equivalent to I_r containing 1 as an ideal in $k[a,b]$. □

Now, a classical enumeration argument implies that if M is not full, and if the field of scalars k is enumerable, then one can effectively find matrices P, Q over k of order $n \times (n-1)$ and $(n-1) \times n$ such that $M = PQ$. Indeed, if M is not full, then we know that for some r, I_r has a zero in k; so we enumerate the $2n^2$-tuples of elements of k simultaneously for $r = 1, \ldots, n$, until we find a zero of one of the ideals I_r. This process terminates in a finite number of steps; when it does, we have invertible matrices A, B over k such that AMB is hollow and now we can easily find P, Q.

For the free field $D_k < X >$, the word problem is solvable provided that D is *dependable* over k, i.e. there is an algorithm which for any finite family of expressions for elements of D in a finite number of steps either leads to a linear dependence relation over k or shows them to be linearly independent over k (see [7, 10]). This condition was also shown to be necessary when $|X| \geq 2$; as Schofield has remarked, X may be taken to be any nonempty set. Thus when $X = x$ and $D_k \prec\!\!\langle X \rangle\!\!\succ$ has solvable word problem, D is dependable over k for the elements $u_1, \ldots, u_n \in D$ are linearly dependent over k if and only if the Capelli polynomial $\sum sgn(\sigma) u_{\sigma 1} x u_{\sigma 2} x \cdots x u_{\sigma n}$ vanishes, where the sum is taken over all permutations of $1, \ldots, n$. This also provides a solution of Example 6.6.4 of [10].

References

1. S. A. Amitsur, *Rational identities and applications to algebra and geometry*, J. Algebra **3** (1966), 304–359.
2. T. Becker and V. Weispfenning, *Gröbner bases, a computational approach to commutative algebra*, Springer, 1993.
3. G. M. Bergman, *Skew fields of noncommutative functions after Amitsur*, Séminaire Lentin–Nivat–Schützenberger, Paris, (1969/1970).
4. J. Berstel and C. Reutenauer, *Rational series and their languages*, Springer Verlag, 1988.
5. G. Cauchon, *Séries de Malcev-Neumann sur le groupe libre et questions de rationalité*, Theor. Comput. Sci. **98** (1992), 79–97.
6. P. M. Cohn, *Universal skew fields of fractions*, Symposia Math. **VIII** (1972), 135–148.
7. P. M. Cohn, *The word problem for free fields*, J. Symb. Logic **38** (1973), 309–314; *correction and addendum ibid.* **40** (1975), 69–74.
8. P. M. Cohn, *The universal field of fractions of a semifir. I. Numerators and Denominators*, Proc. London. Math. Soc. **44** (3) (1982), 1–32.

9. P. M. Cohn, *Free rings and their relations*, 2nd edition, LMS Monographs No. 19, Academic Press, 1985 (1st edition 1971).
10. P. M. Cohn, *Skew fields, theory of general division rings*, Encyclopedia of Mathematics and its Applications, Vol. 57, Cambridge University Press, 1995.
11. P. M. Cohn and C. Reutenauer, *A normal form in free fields*, Can. J. Maths. **46** (1994), 517–531.
12. D. Eisenbud, *Commutative algebra with a view toward algebraic geometry*, Springer, 1995.
13. M. Fliess, *Sur le plongement de l'algèbre des séries rationnelles non commutatives dans un corps gauche*, Comptes Rendus Acad. Sci. Paris **A271** (1970), 926–927.
14. M. Fliess, *Matrices de Hankel*, J. Maths. Pures Appliquées **53** (1974), 197–224.
15. I. M. Gelfand and V. Retakh, *A theory of noncommutative determinants and characteristic functions on graphs I*, Publications du LACIM, Université du Québec à Montréal, 14, 1993.
16. G. Hermann, *Die Frage der endlich vielen Schritte in der Theorie der Polynomideale*, Math. Annalen **95** (1926), 736–788.
17. N. Jacobson, *Structure of rings*, Amer. Math. Soc., Providence RI, 1956, reprint 1964.
18. D. Krob, *Expressions rationnelles sur un anneau*, Lecture Notes in Mathematics **1478** (1991), Springer 215–243.
19. J. Lewin, *Fields of fractions for group algebras of free groups*, Trans. Amer. Math. Soc. **192** (1974), 339–346.
20. N. Popescu, *Abelian categories with applications to rings and modules*, Academic Press, 1973.