Malcev-Neumann series and the free field

Christophe Reutenauer [*]

February 11, 1999

Abstract

After reviewing some aspects of Cohn's theory of the free field, we give another proof of a theorem of Lewin: the subfield of rational elements in the field of Malcev-Neumann series on the free group is isomorphic to the free field.

1 Introduction

There are several ways to construct the free (skew) field: the first construction, due to Amitsur (1966), uses partial rational functions on a big auxiliary skewfield (see also Bergman (1970); Rowen (1980) chapter 8). The construction by Cohn inverts full matrices over the ring of noncommutative polynomials: this amounts to localize this ring at the prime matrix ideal of nonfull matrices. A third construction is provided by Lewin (1974): he shows that the subfield generated by the variables in the field of Malcev-Neumann series on the free group is isomorphic with the free field.

In order to have some intuition on this result, one may think to the case of one variable: Laurent series in one variable form a field, and the subfield generated by the variable is isomorphic with the field of rational functions in one variable.

In the present article, we give a new proof of the theorem of Lewin. His proof is not self-contained and rests on a previous article by Hughes (1970).

---

[*] Université du Québec à Montréal; Département de mathématiques; Case postale 8888, succursale Centre-ville; Montréal, Québec; H3C 3P8. Supported by a grant NSERC (Canada). This work was done during a one month stay in 1998 of the author at Institut Gaspard Monge, Université de Marne la Vallée.

Our proof will be self-contained, and will also imply Cohn's characterization of the free field through full polynomial matrices.

The main result, its consequences and its proof are in Section 3. The proof is combinatorial, and elementary. The fact that the group on which the series are constructed is free will be very apparent: indeed, in a crucial and simple way, we use the fact that its Cayley graph is a tree (see the proof of Lemma 1 and the end of the proof of the theorem in Section 3.2).

In Section 2.1, we shall review some results, all due to Cohn, on full matrices over the ring of noncommutative polynomials. In Section 2.2, we review Cohn's construction of the free field. This will make this article entirely self contained; the reader may also view section as an introduction to some ideas of Cohn's theory.

In Section 2.3, we briefly review Malcev-Neumann series on the free group.

2 Free field

2.1 Full matrices over noncommutative polynomials

Let k be a commutative field and X a finite set of noncommuting variables. We denote by $k < X >$ the k-algebra of noncommutative polynomials over k.

Let R be a ring. A square matrix A over R, of order n, is *not full* if for some $p < n$ and some matrices B, C over R of size $n \times p$ and $p \times n$, one has $A = BC$. Clearly, if R is a field, A is not full if and only A is noninvertible. Observe that if A is *hollow*, that is, if it has a zero submatrix of size $r \times s$ with $r + s > n$, then A is not full, as is easily seen.

Note that if two square matrices A, A' of the same size, are *associated*, i.e. $A' = PAQ$ with P, Q invertible over R, then A, A' are simultaneously full or not. Note also that if A is not full, then so is $\begin{pmatrix} A & 0 \\ 0 & I \end{pmatrix}$, for any identity matrix I.

The converse is also true when $R = k < X >$. Indeed, suppose that $\begin{pmatrix} A & 0 \\ 0 & 1 \end{pmatrix}$ is not full, with A square of order n. Then for some $p \leq n$, and some matrices B, C of size $n \times p$ and $p \times n$, we have $\begin{pmatrix} A & 0 \\ 0 & 1 \end{pmatrix} = BC$. If $x_1, \ldots, x_p$ and $y_1, \ldots, y_p$ denote the elements of the last row of B and of the last column of C, we therefore have: $x_1 y_1 + \ldots + x_p y_p = 1$. By repeated uses of Cohn's weak algorithm (see Cohn (1985), p.96 and Cor. 4.3 p.106), which is a generalization to $k < X >$ of the classical Euclidean algorithm, we may find a $p \times p$ invertible matrix P over $k < X >$ such that $B_1 = BP$, $P^{-1}C = C_1$ have respectively last row $(0, \dots, 0, 1)$ and last column $(0, \dots, 0, 1)$. Then, by inspection of the product $A = B_1 C_1$, we see that B_1, C_1 are respectively of the form $\begin{pmatrix} B' & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} C' & 0 \\ 0 & 1 \end{pmatrix}$, which implies that $A = B'C'$ is not full.

The previous argument implies that if two square matrices A, A' over $k < X >$ are *stably associated*, that is, $\begin{pmatrix} A & 0 \\ 0 & I \end{pmatrix}$ and $\begin{pmatrix} A' & 0 \\ 0 & I' \end{pmatrix}$ are associated for some identity matrices of appropriate size, then A and A' are simultaneously full or not.

Call a matrix A over $k < X >$ *linear* if each entry of it is a polynomial of degree ≤ 1. Then, by Higman's trick of *linearization by enlargment* (see Cohn (1985), p.272), which is best illustrated by the following two operations, on the rows and then on the columns,

$$\begin{pmatrix} f+ab & 0 \\ 0 & 1 \end{pmatrix} \rightarrow \begin{pmatrix} f+ab & a \\ 0 & 1 \end{pmatrix} \rightarrow \begin{pmatrix} f & a \\ -b & 1 \end{pmatrix},$$

one sees at once that each matrix over $k < X >$ is stably associated to a linear matrix.

2.2 The free field

Suppose that K is a field containing a ring R. Then each square matrix over R which is nonfull is noninvertible, when viewed over K. The converse is not true in general: there may be full matrices over R which are noninvertible over K (this holds even when R is the ring of *commutative* polynomials in at least three variables over k, see Cohn (1985), p.252).

When the converse holds, that is, when each full matrix over R is invertible over K, then the embedding $R \hookrightarrow K$ is called *fully inverting.* Note that in this case, the embedding makes invertible the maximum possible of matrices over R.

A basic result of Cohn is that there exists a field K, containing the algebra of noncommutative polynomials $k < X >$, such that the mapping $k < X > \hookrightarrow K$ is fully inverting. It will be called the *free field.*

The existence of such a field will be consequence of our approach to Lewin's theorem (see Corollary 1).

This field is also unique; it is not the scope of this article to prove it, but we may indicate the idea of a possible proof. It is the fact that each identity in K, that is, each *rational identity*, may be encoded in $k < X >$, in the following sense: such an identity is represented by a square matrix over $k < X >$ which is not full (cf. Cohn (1995) Th. 4.5.11). Hence rational identities in K depend only on $k < X >$ and K is unique.

To conclude this section, and in order to be functorially correct, one has to justify the adjective "free" of free field. Following Cohn, one defines the category of *epic* $k < X >$ *- fields and specializations*: an object in this category is a field L together a k-algebra homomorphism $k < X > \rightarrow L$ whose image generates L as field. A morphism in this category is a *specialization* $f : L \rightarrow L'$, i.e. a k-algebra homomorphism defined on a subring L_0 of L, such that if $x \in L_0$ and $f(x) \neq 0$, then x has an inverse in L_0; these homomorphisms however are considered up to a natural equivalence. For details, see Cohn (1985), chapter 7.

Then the free field is a universal object in this category.

2.3 Malcev-Neumann series on the free group

Let Γ be the free group on X. Consider a total order $\leq$ on Γ compatible with its group structure.

Remark

Such an order is not so easy to obtain, that's why we describe now a classical one: put the lexicographical order on the free monoid X^* generated by $X : u < v$ if either u is shorter than v, or if both have the same length n and $u < v$ in the lexicographic order from left to right in X^n. Then the ring $\mathbb{Z} << X >>$ of noncommutative series on X over $\mathbb{Z}$ gets an order compatible with its ring structure: a nonzero series $\sum_{w \in X^*} \alpha_w w$ is positive if the smallest word w in X^* with $\alpha_w \neq 0$ satisfies $\alpha_w > 0$. Then, embed Γ into the multiplicative group of invertible series by the Magnus embedding: $x \mapsto 1 + x, \Gamma \rightarrow (\mathbb{Z} << X >>, \cdot)$. This embedding gives Γ a compatible total order.

Let $k((\Gamma))$ denote the ring of *Malcev-Neumann series* on Γ over k relative to this order: an element of $k((\Gamma))$ is an infinite series $S = \sum_{g \in \Gamma} \alpha_g g$, with α_g in k, such that the *support* of S, that is, the set $\{g \in \Gamma | \alpha_g \neq 0\}$ is a well-ordered subset of Γ. Recall that a well ordered set is an ordered set such that each nonempty subset has a minimum. Note that in the one variable case, this reduces to the definition of Laurent series.

Then, one defines sum and product in $k((\Gamma))$ as in the group algebra $k\Gamma$; the fact that the product is well-defined is not evident a priori, and requires a proof. Actually, according to a theorem by Malcev and Neumann, $k((\Gamma))$ is a field; see Passman (1985), Th.13.2.11.

3 The main result

3.1 Statement and consequences

We shall prove directly the following result, which will imply Lewin's theorem (it may also be obtained as a consequence of the latter).

Theorem

If a square linear matrix over $k < X >$ *is noninvertible over the field* $k((\Gamma))$ *of Malcev-Neumann series on the free group, then it is not full over* $k < X >$ *.*

The proof will be made in the next section. We note first the following easy consequences.

Corollary 1 (Lewin)

Let K *be the field of rational elements in* $k((\Gamma))$*, i.e.* K *is the subfield of* $k((\Gamma))$ *generated by the variables over* k*. Then* K *is the free field, that is, each full matrix over* $k < X >$ *is invertible over* K*.*

Proof

We have just to show that if A is a full square matrix over $k < X >$, then it is invertible over K. But A is stably associated over $k < X >$ to a square linear matrix A', which is full (see Section 2.1). Then, according to the theorem, A' is invertible over $k((\Gamma))$. But the coefficients of its inverse are in the subfield generated by the coefficients of A' (by solving linear equations), so in K. Hence A' is invertible over K. But A' is stably associated to A also over K, so that A is invertible over K, since stably associated matrices over a field are simultaneously invertible or not. $\Box$

Corollary 2 (Cohn)

If $k \subseteq k'$ *is an extension of commutative fields, then the free field on* X *over* k *is canonically embedded in that over* k'*. It other words, each full matrix over* $k < X >$ *is also full over* $k' < X >$ *.*

Remarks

1. There is a fourth construction of the free field, due to Linnell (1993): Let $U(\Gamma)$ denote the ring of closed densely defined unbounded operators which are affiliated to the group von Neumann algebra of the

free group Γ, and let $D(\Gamma)$ be the division closure of $\mathbb{C}\Gamma$ in $U(\Gamma)$, that is, the smallest subring of $U(G)$ containing $\mathbb{C}\Gamma$ which is closed under taking inverses. Then Linnell shows that $D(\Gamma)$ is the free field.

2. There is a Hankel criterion characterizing noncommutative rational series, see Fliess (1974). In Duchamp and Reutenauer (1997), this criterion is extended to Malcev-Neumann series on the free group, by adapting the condition of Connes (1994), p. 342.

Terminology:

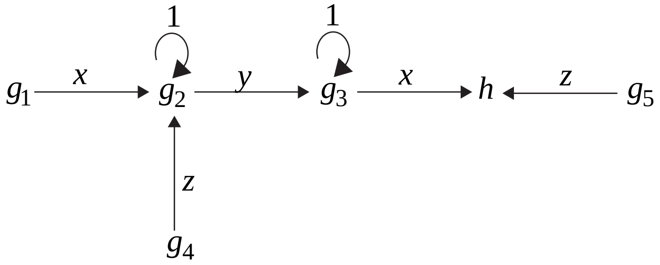
The *leading term* of a nonzero Malcev-Neumann series is the smallest element of its support; a *head* in a directed graph is a vertex which is the terminal vertex of some edge (it may be the initial vertex of some other edge).

3.2 Proof of the theorem

Let $g_1, \ldots, g_n$ be $n \geq 1$ distinct elements in the free group Γ generated by X. We associate to them a directed and labelled graph G as follows: the vertices are $g_1, \ldots, g_n$, together with the elements $g \in \Gamma$ such that for some $i \neq j$ and some x, y in $X \cup \{1\}$, one has $g = g_i x = g_j y$; the latter vertices are called *special* (note that some g_i may be special); there is an edge, labelled x, $g_i \xrightarrow{x} g_i x$ if and only if $g_i x$ is special.

Example

$X = \{x, y, z\},\ n = 5,\ g_2, g_3, h$ special



Note that if we remove the loops $g_i \xrightarrow{1} g_i$ in G, then it becomes a subgraph of the Cayley graph of Γ, hence a *disjoint union of trees*. Note also that each head is a special vertex, and conversely. Furthermore, the only loops in G are of the form $g_i \xrightarrow{1} g_i$, that is, are around a vertex which is among the g_i and which is special.

Lemma 1

Let e be the number of edges in G and k be the number of special vertices. Then $e \leq n + k - 1$.

Proof

Let l be the number of loops, and k' be the number of special vertices without loop around them. Then $k = k' + l$ and $n = n' + l$, where n' is the number of g_i without loop. The total number of vertices in G is $n + k' = n + k - l$.

In G, replace each loop around vertex v by an edge $v \to \bar{v}$, where $\bar{v}$ is a new vertex. In such a way, we obtain a graph G' that is a union of trees. This graph has e edges, and $n + k - l + l = n + k$ vertices.

Recall the following easy result: in a union of trees, number of edges $\leq$ number of vertices -1 (it is $=$ when the union of trees is actually a tree).

Thus we have $e \leq n + k - 1$, which proves the lemma. □

Now let $S_1, \ldots, S_n$ be Malcev-Neumann series on Γ with respective leading terms $g_1, \ldots, g_n$, which we suppose distinct. Given a matrix M in $k < X >^{n \times p}$, we associate to it a subgraph $G(M)$ of G, with the same vertices and a subset of the edges: an edge $g_i \xrightarrow{x} g_i x$ in G is an edge of $G(M)$ if x appears in the i-th row of M.

We assume in the sequel that M is linear and satisfies $(S_1, \ldots, S_n)\ M = 0$. Denoting by m_{ij} the i, j entry of M, we therefore have for $j = 1, \ldots, p$

$$S_1\ m_{1j} + S_2\ m_{2j} + \ldots + S_n\ m_{nj} = 0 \tag{1}$$

Lemma 2

If for some i, some $g \in \Gamma$ and some $x \in X \cup \{1\}$, g appears in S_i and x appears in m_{ij}, then there is a head in $G(M)$ which is $\leq gx$; if moreover $g \neq g_i$, it is $< gx$.

Proof

We have $g_i \leq g$. Let $y \in X \cup \{1\}$ appearing in m_{ij}, and minimum. Then $y \leq x$ and $g_i y \leq gx$. By minimality of g_i and y, there is only one occurrence of $g_i y$ in the product $S_i\ m_{ij}$. Thus, by (1), there exists $i' \neq i$ such that $g_i y = g' x', g'$ appears in $S_{i'}$, x' appears in $m_{i'j}$. If $g' = g_{i'}$, we have found in G the special vertex $g_i y = g_{i'} x'$, which is a head of $G(M)$ since $g_{i'} \xrightarrow{x'} g_{i'} x'$ is an edge of $G(M)$, and moreover $g_i y \leq gx$; note that if moreover $g_i \neq g$, then $g_i < g$, hence $g_i y < gx$. If on the other hand, $g' \neq g_{i'}$, then $g_{i'} < g'$, and we have $g_{i'} x' < g' x' = g_i y \leq gx$, and we continue with $(g_{i'}, x')$ instead of (g, x). The process must stop since the g_i and x are finite in number. □

The following lemma is the heart of the proof. Recall that M is of size $n \times p$.

Lemma 3

Let h be the smallest head of $G(M)$. Let $e(h)$ be the number of edges in G with head h. Assume that $p \geq e(h) - 1$. Then by column operations over k, we can bring M to the form (M_1, M'), where M' is of size $n \times p'$ with $(S_1, \ldots, S_n)M' = 0$, with $p' = p - e(h) + 1$, and such that h is not head of $G(M')$.

Proof

We may without harm assume that the edges in G with head h are $g_1 \xrightarrow{x_1} h, \ldots, g_f \xrightarrow{x_f} h$, with $f = e(h)$. Denote by $m_{ij}(x)$ the coefficient of x in m_{ij}. We claim that the coefficient of h in (1) is

$$\alpha_1 m_{1j}(x_1) + \alpha_2 m_{2j}(x_2) + \ldots + \alpha_f m_{fj}(x_f),$$

where α_i is the coefficient of g_i in S_i. Indeed, otherwise, there is some $g \in \Gamma$ and some $x \in X \cup \{1\}$ such that g appears in S_i and x appears in m_{ij}, and that $gx = h$ and either $i \leq f$ and $(g, x) \neq (g_i, x_i)$, or $i > f$.

In the first case, since $gx = h = g_i x_i$, we have $g \neq g_i$, hence by Lemma 2, we find in $G(M)$ a head which is $< g_i x_i = h$, which contradicts the minimality of h.

In the second case, since $gx = h, \quad g \neq g_i$ by assumption on the edges in G whose head is h. Thus Lemma 2 implies that there is in $G(M)$ a head $< gx = h$, a contradiction.

We thus obtain that, for any $j = 1, \ldots, p$:

$$\alpha_1 m_{1j}(x_1) + \ldots + \alpha_f m_{fj}(x_f) = 0.$$

This shows that the rows of the $f \times p$ matrix

$$(m_{ij}(x_i))_{1 \leq i \leq f,\ 1 \leq j \leq p}$$

over k are linearly dependent. Thus its rank is at most $f - 1$. Since $p \geq f - 1$, we may bring it by column operations over k to the form (A_1, A'), where $A' = 0$ is of size $f \times (p - f + 1) = f \times p'$. Performing the same column operations on M, we obtain a matrix (M_1, M'), with M' of size $n \times p'$, and such that x_i does not appear in the $i-$th row of M', for $i = 1, \ldots, f$. Hence the edge $g_i \xrightarrow{x_i} h$ does not exist in $G(M')$. $\square$

Lemma 4

If $G(M)$ has no edges, then $M = 0$.

Proof

Suppose that $M \neq 0$; then for some i, j, some $x \in X \cup \{1\}$ appears in m_{ij}. Since g_i appears in S_i, Lemma 2 shows that some vertex in $G(M)$ is a head, so that $G(M)$ has an edge. □

Proof of the theorem

Let A be a linear matrix over $k < X >$, of size $p \times p$, and $S_1, \ldots, S_p$ be Malcev-Neumann series, not all 0, such that $(S_1, \ldots, S_p)A = 0$. If their rank over k is n, we may, by performing row operations over k on A, assume that $(S_1, \ldots, S_p) = (S_1, \ldots, S_n, 0, \ldots, 0)$, and that the leading elements $g_1, \ldots, g_n$ of $S_1, \ldots, S_n$ are distinct. Then A may be written $A = \begin{pmatrix} M \\ N \end{pmatrix}$, where M is of size is $n \times p$. We then have $(S_1, \ldots, S_n)M = 0$.

Observe that if M' is obtained from M by column operations, and if the edge $g_i \xrightarrow{x} g_i x$ of G is not in $G(M)$, it is not in $G(M')$ either. Similarly if M' is obtained from M by suppressing some columns.

We now apply Lemma 3 several times: first, note that by Lemma 1, we have $e = \sum_h e(h)$ (sum over all special vertices h in G) $\leq n+k-1 \leq p+k-1$. Thus $p \geq 1 + \sum_h (e(h) - 1)$. Now, if M has an edge, it has a head h, which we choose minimum; then we apply to it Lemma 3, and obtain a matrix $M' = M_1$ of size $n \times (p - e(h) + 1)$, with h no more a head in $G(M_1)$. If M_1 has an edge, we continue with Lemma 3. Finally, we obtain a matrix $M_{k'}$, with $k' \leq k$, of size $n \times \left(p - \sum_h (e(h) - 1)\right)$, where the sum this time is over some subset of cardinality k' of the set of special vertices in G, and such that $G(M_{k'})$ has no edges, hence $M_{k'} = 0$ by Lemma 4.

This shows that by performing column operations on M, we can produce a rectangle of $0'$s in M of size $n \times (p - e + k)$. Since $n + p - e + k \geq p + 1$ (by Lemma 1), M is not full. □

The proof shows also the following known result (Cohn (1995), Cor.6.3.6)

Corollary 3

A square linear matrix A over $k < X >$ of order p is not full if and only if for some invertible matrices P, Q over k, the matrix PAQ is hollow.

References

Amitsur, A. (1966). Rational identities and applications to algebra and Geometry. *J. Algebra*, 3:304–359.

Bergman, G. M. (1970). Skew field of Noncommutative Rational Functions, After Amitsur. *Séminaire Schützenberger-Lentin-Nivat*, 16.

Cohn, P. M. (1985). *Free rings and their relations.* Academic Press. (First edition 1991).

Cohn, P. M. (1995). *Skew fields.* Cambridge University Press.

Connes, A. (1994). *Noncommutative geometry.* Academic Press.

Duchamp, G. and Reutenauer, C. (1997). Un critère de rationalité provenant de la géométrie non commutative. *Inventiones Mathematicae*, 128:613–622.

Fliess, M. (1974). Matrices de Hankel. *Journal de Mathématiques Pures et Appliquées*, 53:197–222.

Hughes, I. (1970). Division rings of fractions for group rings. *Comm. Pure Appl. Math.*, 23:181–188.

Lewin, J. (1974). Fields of fractions for group algebras of free groups. *Trans. Amer. Math. Soc.*, 192:339–346.

Linnell, P. A. (1993). Division rings and group von Neumann Algebras. *Forum Mathematicum*, 5:561–576.

Passman, D. S. (1985). *The algebraic structure of group rings.* Robert E. Krieger Publishing Company, Malabar, Florida.

Rowen, L. H. (1980). *Polynomial identities in Ring Theory.* Academic Press.