THE JOURNAL OF SYMBOLIC LOGIC
Volume 38, Number 2, June 1973

THE WORD PROBLEM FOR FREE FIELDS

P. M. COHN

§1. Introduction. It has long been known that every free associative algebra can be embedded in a skew field [11]; in fact there are many different embeddings, all obtainable by specialization from the 'universal field of fractions' of the free algebra (cf. [5, Chapter 7]). This makes it reasonable to call the latter the free field; see §2 for precise definitions. The existence of this free field was first established by Amitsur [1], but his proof is rather indirect and does not provide anything like a normal form for the elements of the field. Actually one cannot expect to find such a normal form, since it does not even exist in the field of fractions of a commutative integral domain, but at least one can raise the word problem for free fields: Does there exist an algorithm for deciding whether a given expression for an element of the free field represents zero?

Now some recent work has revealed a more direct way of constructing free fields ([4], [5], [6]), and it is the object of this note to show how this method can be used to solve the word problem for free fields over infinite ground fields. In this connexion it is of interest to note that A. Macintyre [9] has shown that the word problem for skew fields is recursively unsolvable. Of course, every finitely generated commutative field has a solvable word problem (see e.g. [12]).

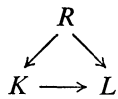
The construction of universal fields of fractions in terms of full matrices is briefly recalled in §2, and it is shown quite generally for a ring R with a field of fractions inverting all full matrices, that if the set of full matrices over R is recursive, then the universal field has a solvable word problem. This holds more generally if the precise set of matrices over R inverted over the field is recursive, but it seems difficult to exploit this more general statement. To complete the solution of the word problem for free fields we show in §3 that the full matrices over a free associative algebra form a recursive set.

§2. Universal fields of fractions. This section outlines the construction of the universal field of fractions given in [4], [6]; see also [5, Chapter 7]. Throughout, all rings have a unit-element which is preserved by homomorphisms and inherited by subrings. By a field we mean a not necessarily commutative division ring.

Let R be any ring. An *epic R-field* is a field K with a homomorphism $f: R \to K$ such that K is the field generated by $\operatorname{im} f$. If f is injective, K is called a *field of fractions* of R. When R is a commutative integral domain—or more generally, a right Ore domain—there exists a field of fractions, unique up to isomorphism, but for general integral domains, there may be no field of fractions, or several [10], [3].

Received October 2, 1972.

Given two epic R-fields K, L, a *specialization* $K \to L$ is a homomorphism α: $K_0 \to L$ from a subring K_0 of K containing the image of R, such that the triangle shown commutes and, for any $x \in K_0$, $x\alpha \neq 0$ implies $x^{-1} \in K_0$. Two specializations are equal if they agree on a subring K_0 and the common restriction is a specialization.



If R has a field of fractions U from which there is a unique specialization to each epic R-field, then U is called a *universal field of fractions* of R.

Any epic R-field K can be described as the residue class field of a local ring R_Σ, where Σ is the set of all square matrices over R which becomes invertible over K, and R_Σ is the ring obtained from R by adjoining formal matrix inverses to all the elements of Σ; thus R_Σ is the "universal Σ-inverting ring"; cf. [5] [6]. In particular, if it is possible to choose the set Σ greatest, i.e., so as to contain all other possible choices, we obtain a universal field of fractions.

There is one case of importance to us, in which the above construction simplifies a little; to describe it we need the notion of a full matrix. A square matrix A over a ring R is called *full* if it cannot be written in the form $A = PQ$, where P is $n \times r$, Q is $r \times n$ and $r < n$. E.g., over a field (even skew), a matrix is full if and only if it is invertible. We also recall that a ring is called a *free ideal ring* (*fir* for short) if every left or right ideal is free, of uniquely determined rank, as a module over the ring. More generally, a *semifir* is a ring over which every finitely generated left (or equivalently right) ideal is free of unique rank. The main examples of firs are free associative algebras and free products of fields. The following result was proved for firs in [4], [6] and, more generally, for semifirs in [5]:

THEOREM 1. *Let R be a semifir, and U the ring obtained from R by formally adjoining matrix inverses for all full matrices over R. Then U is a universal field of fractions for R.*

It is clear that in any field of fractions K of R, the elements may be expressed as words in the elements of R. By this we mean that any element of K has an expression which is built up from elements of R by repeated addition, subtraction, multiplication and inversion. However, not every such expression will correspond to an element of K; e.g. $(a - abb^{-1})^{-1}$ does not represent a field element, and two quite different expressions may represent the same field element. Now the word problem for K is the problem of finding a recursive procedure allowing us to decide (i) when a given expression represents a field element, and (ii) when two given expressions represent the same field element. In fact (ii) can be reduced to (i); for clearly, two words u, v will represent the same field element if and only if $(u - v)^{-1}$ does not represent a field element. Thus the word problem requires a procedure for deciding when a given field word represents a field element.

The latter problem can be reduced to the question of whether a certain matrix is invertible, as follows. If K is a field, generated as field over a central ground field k by elements $x_1, \cdots, x_n$, then every field word (possibly representing an element of K) is built up from $x_1, \cdots, x_n$ and the elements of k by the four operations of

arithmetic. As was shown in [5, Chapter 7], every such expression f is a component of the solution vector u of an equation

$$Au + a = 0, \tag{1}$$

where A is a matrix and a a column in the elements $x_1, \cdots, x_n$ and the elements of k. Moreover, f represents a field element precisely when A is nonsingular over K. The equation (1) is built up recursively according to the way in which f was constructed. Thus if f is x_i or an element of k, it is a solution of

$$1 \cdot f - a = 0 \qquad (a = x_i \text{ or } a \in k).$$

If $f = u_1 - v_1$, where u_1, v_1 are the first components of the solutions of $Au + a = 0$, $Bv + b = 0$ respectively, then f is the first component of the solution of

$$\begin{pmatrix} A & a_1 & 0 \\ 0 & & B \end{pmatrix} y + \begin{pmatrix} a \\ b \end{pmatrix} = 0, \tag{2}$$

where a_1 is the first column of A, and $u_1 + v_1$ is defined similarly, while $u_1 v_1$ is the first component of the solution of

$$\begin{pmatrix} A & a & 0 \\ 0 & & B \end{pmatrix} z + \begin{pmatrix} 0 \\ b \end{pmatrix} = 0. \tag{3}$$

Finally, u_1^{-1} is the first component of the solution of

$$A_1 t + a_1 = 0,$$

where $A = (a_1, \cdots, a_n)$, and $A_1 = (a, a_2, \cdots, a_n)$ is the matrix obtained by exchanging the first column of A against a. Only the last step can lead to a singular matrix, since the matrices in (2) and (3) are nonsingular whenever A and B are.

Suppose now that R is a semifir and U its universal field of fractions. Then a matrix A over R is singular over U if and only if it is nonfull in R. Thus we obtain the following reduction for the word problem in U:

THEOREM 2. *Let R be a semifir and U the universal field of fractions of R. Then each element of U can be obtained in the form $x = u_1$ where u_1 is the first component of the solution of a matrix equation* (1), *with a full matrix A. More generally, any expression (field word) is obtained as the first component of the solution of an equation* (1), *and it defines an element of U precisely if A is full.*

It is clear from this result that if the full matrices over R form a recursive set, then we have a solution of the word problem for U. We enumerate the full matrices A and all columns a; this will give us an enumeration of expressions for all the elements of U. In fact it is enough to assume that the set of full matrices is recursively enumerable, because its complement, the set of nonfull matrices, is always recursively enumerable (in an enumerable ring).

More generally, let K be an epic R-field and Σ the precise set of matrices over R which become invertible over K. Suppose that Σ is recursive; then the word problem for K is solvable. This follows as before, using the description of epic R-fields given earlier.

§3. **Full matrices over free algebras.** The free associative algebra in $X = \{x_1, \cdots, x_d\}$ over a commutative field k is defined as the ring of k-linear combinations of formal products of the x's (cf. [5]), and is written $k\langle x_1, \cdots, x_d \rangle$ or

$k\langle X\rangle$. This differs from the polynomial ring $k[x_1, \cdots, x_d]$ in that the x_i do not commute with each other, though they still commute with elements of k. It is a natural step to allow a noncommutative coefficient field which need not commute with the indeterminates. However, some elements will always lie in the centre, e.g. the prime subfield, and it is best to specify this in advance. For technical reasons which will become clear later, we must also exclude finite fields.

Thus we consider a field K with an infinite central subfield C, and form the free product (cf. [2])

$$K *_C C\langle X\rangle.$$

This will be denoted by $K_C\langle X\rangle$ and may be called the *free K-ring on X over C*. It is known that $K_C\langle X\rangle$ satisfies the weak algorithm and hence is a fir (cf. [5, Chapter 2]); of course, for $K = C = k$, it reduces to the free k-algebra considered earlier. By Theorem 1, $K_C\langle X\rangle$ has a universal field of fractions U inverting all full matrices, and to complete the solution of the word problem for U we need only show that the full matrices over $K_C\langle X\rangle$ form a recursive set.

For the proof we need two remarks, of which the first concerns the relation of a free K-ring to its completion. The ring $K_C\langle X\rangle$ may be graded in an obvious fashion by assigning degree 1 to each x_i. We can form the completion with respect to this grading; this is essentially the ring of formal power series, written $K_C\langle\langle X\rangle\rangle$, and it follows from Bergman's inertia theorem, in the form given in [5, Theorem 2.8.12, p. 103], that every full matrix over $K_C\langle X\rangle$ remains full, when considered over $K_C\langle\langle X\rangle\rangle$; in other words, the embedding $K_C\langle X\rangle \to K_C\langle\langle X\rangle\rangle$ is 'honest'.

The second remark generalizes the well known fact that a nilpotent matrix A of order n over a field satisfies $A^n = 0$.

LEMMA. *Let P be an $n \times n$ matrix, Q a matrix with n rows and R a matrix with n columns over a skew field. If*

$$RP^\nu Q = 0 \quad \text{for } \nu = 0, 1, \cdots, n-1, \tag{4}$$

then $RP^\nu Q = 0$ for all $\nu \geq 0$.

PROOF. Denote the field by K and let V be the right K-space of column vectors with n components. The columns of Q span a subspace V_0 of V, while the columns annihilated by the rows of R form a subspace W of V, and since $RQ = 0$ by (4), we have $V_0 \subseteq W$. Regarding P as an endomorphism of V, we may define a subspace V_ν of V for $\nu > 0$ inductively by the equation

$$V_\nu = V_{\nu-1} + PV_{\nu-1}.$$

Thus $V_\nu = V_0 + PV_0 + \cdots + P^\nu V_0$, and it follows that

$$V_0 \subseteq V_1 \subseteq \cdots \subseteq V_{n-1}. \tag{5}$$

Moreover, by (4), $V_\nu \subseteq W$ for $\nu = 0, \cdots, n-1$. Now if $Q = 0$ or $R = 0$, there is nothing to prove. Otherwise $V_0 \neq 0$, $W \neq V$, and we must have equality at some point in (5), since $\dim V_{n-1} \leq n-1$. Suppose that $V_{k-1} = V_k$ $(k < n)$. Then $PV_{k-1} \subseteq V_{k-1}$; hence $PV_k = PV_{k-1} \subseteq V_k$; therefore $V_{k+1} = V_k + PV_k = V_k$; and so the sequence is stationary from that point on. Since the sequence has become stationary by the $(n-1)$th stage at the latest, we conclude that $V_\nu \subseteq W$ for all ν, i.e., $RP^\nu Q = 0$ for all ν, as we wished to show.

THEOREM 3. *Let K be a field with an infinite central subfield C, then the set of all full matrices over $K_C\langle X\rangle$, the free K-ring over C on X, is recursive.*

PROOF. Let A be any square matrix over $K_C\langle X\rangle$; we shall prove the theorem by describing an algorithm for deciding whether A is full. We first observe that the fullness of A is unaffected by elementary transformations, and by bordering A with a row and column of zeros meeting in 1. This allows us to reduce A to a matrix linear in the x_i, the process of "linearization by enlargement" (sometimes called Higman's trick, cf. [8]). To describe a typical case of this process, suppose that the (n, n)-entry of an $n \times n$ matrix has the form $f + ab$; on enlarging the matrix we can replace the term ab by terms a, b by applying elementary transformations, as follows. We give the series of moves, showing only the nth and $(n + 1)$th row and column:

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

By repeated applications we can therefore reduce A to the form

$$A' = A_0 + A_1, \tag{6}$$

where A_0 is homogeneous of degree 0 and A_1 of degree 1 in the x's.[1] Moreover, A' is full if and only if A is. Suppose that A' is not full; then it will remain nonfull when the x_i are replaced by 0; i.e. A_0 must then be singular over K. Hence if A_0 is nonsingular, then A' is necessarily full.

We may therefore suppose that A_0 is singular, of rank $r < n$ say, where n is the order of A'. By diagonal reduction over K (which leaves the fullness of A' unaffected) we can reduce A_0 to the form $\left(\begin{smallmatrix} I & 0 \\ 0 & 0 \end{smallmatrix}\right)$ (cf. [5, Chapter 8]; clearly this is effective). Let us partition A_1 accordingly.

$$A' = \begin{pmatrix} I - P & Q \\ R & S \end{pmatrix}$$

where P, Q, R, S are homogeneous of degree 1. Now pass to the completion $K_C\langle\langle X\rangle\rangle$; by the remark made earlier, A' is full over $K_C\langle X\rangle$ if and only if it is full over $K_C\langle\langle X\rangle\rangle$. The matrix $I - P$ is invertible over $K_C\langle\langle X\rangle\rangle$, and by elementary transformations we obtain

$$\begin{pmatrix} I - P & Q \\ R & S \end{pmatrix} \to \begin{pmatrix} I & (I - P)^{-1}Q \\ R & S \end{pmatrix} \to \begin{pmatrix} I & (I - P)^{-1}Q \\ 0 & S - R(I - P)^{-1}Q \end{pmatrix}. \tag{7}$$

To find whether

$$S - R(I - P)^{-1}Q = 0, \tag{8}$$

we have to check that, for each $d = 0, 1, \cdots$, the homogeneous terms of degree d are 0. Now $S - R(I - P)^{-1}Q = S - \sum RP^{\nu}Q$, and equating terms of degree d, we find that (8) is equivalent to

$$S = 0, \quad RP^{\nu}Q = 0 \qquad (\nu = 0, 1, \cdots). \tag{9}$$

These are equations of matrices over $K_C\langle X\rangle$, and since the latter is embeddable in a field, we can apply the Lemma and conclude that (9) holds whenever the first

[1] An element is homogeneous of degree d if it is a linear combination of products of degree d in the x's. Thus 0 is homogeneous of degree d for every d.

$r + 1$ equations hold, where r is the order of P. This then provides us with an algorithm for determining whether (8) holds. If this equation holds, then the matrix on the right of (7) has at least one row of zeros and hence A' is then nonfull. If (8) does not hold, then since C is infinite, we can specialize the x_i within C to values α_i such that $I - P$ remains nonsingular and $S - R(I - P)^{-1}Q$ remains nonzero (cf. [7]). Translating back to A', we find that by specializing x_i to α_i we obtain a matrix of rank greater than r. We now replace x_i by $x_i + \alpha_i$ and start again from (6). This time we have a matrix A_0 over K of rank greater than r. By repeating this process a finite number of times (at most n times, where n is the order of A'), we can thus decide whether or not A' is full, and this completes the proof.

REFERENCES

[1] S. A. AMITSUR, *Rational identities and applications to algebra and geometry*, ***Journal of Algebra,*** vol. 3 (1966), pp. 304–359.

[2] P. M. COHN, *On the free product of associative rings*, ***Mathematische Zeitschrift,*** vol. 71 (1959), pp. 380–398.

[3] ———, ***Universal algebra,*** Harper and Row, New York and London, 1965.

[4] ———, *The embedding of firs in skew fields*, ***Proceedings of the London Mathematical Society (3),*** vol. 23 (1971), pp. 193–213.

[5] ———, ***Free rings and their relations,*** Academic Press, London and New York, 1971.

[6] ———, *Universal skew fields of fractions*, ***Symposia Mathematica,*** vol. 8 (1972), pp. 135–148.

[7] ———, *Generalized rational identities*, ***Ring theory*** (Proceedings of a conference on ring theory, Park City, Utah, 1971), Academic Press, 1972, pp. 107–115.

[8] G. HIGMAN, *The units of group rings*, ***Proceedings of the London Mathematical Society (2),*** vol. 46 (1940), pp. 231–248.

[9] A. MACINTYRE, *The word problem for division rings* (to appear).

[10] A. I. MAL'CEV, *On the immersion of an algebraic ring into a field*, ***Mathematische Annalen,*** vol. 113 (1937), pp. 686–691.

[11] R. MOUFANG, *Einige Untersuchungen über geordnete Schiefkörper*, ***Journal für die reine und angewandte Mathematik,*** vol. 176 (1937), pp. 203–223.

[12] H. SIMMONS, *The solution of a decision problem for certain classes of rings*, ***Pacific Journal of Mathematics,*** vol. 34 (1970), pp. 547–557.

BEDFORD COLLEGE
LONDON NW1 4NS, ENGLAND