THE JOURNAL OF SYMBOLIC LOGIC
Volume 40, Number 1, March 1975

THE WORD PROBLEM FOR FREE FIELDS: A CORRECTION AND AN ADDENDUM

P. M. COHN

§1. In [1] it was claimed that the word problem for free fields with infinite centre can be solved. In fact it was asserted that if K is a skew field with infinite central subfield C, then the word problem in the free field on a set X over K can be solved, relative to the word problem in K.

As G. M. Bergman has pointed out (in a letter to the author), it is necessary to specify rather more precisely what type of problem we assume to be soluble for K: We must be able to decide whether or not a given finite set in K is linearly dependent over its centre. This makes it desirable to prove that the free field has a corresponding property (and not merely a soluble word problem). This is done in §2; interestingly enough it depends only on the solubility of the word problem in the free field (cf. Lemma 2 and Theorem 1′ below).

Bergman also notes that the proof given in [1] does not apply when K is finite-dimensional over its centre; this oversight is rectified in §4, while §3 lifts the restriction on C (to be infinite). However, we have to assume C to be the precise centre of K, and not merely a central subfield, as claimed in [1].

I am grateful to G. M. Bergman for pointing out the various inaccuracies as well as suggesting remedies.

§2. The word problem in a variety of algebras, e.g. groups, is the problem of deciding for a given presentation of a group when two expressions represent the same group element. In the case of skew fields we do not have a presentation in the usual sense, but we again have a set of expressions for the elements of our field, and we require an algorithm for deciding when two expressions represent the same field element. Generally there is also a coefficient field K, possibly skew, and we need to know how K is given. It may be that K has a soluble word problem, and the algorithm achieving this is then incorporated in the algorithm to be constructed; or more generally we merely postulate that certain questions about K can be answered in a finite number of steps, and we use this fact to construct a relative algorithm. We shall take the second course, thus our solution will not depend on the precise algorithm in K, but merely that it exists.

Let K be a field (generally skew) and C a subfield of its centre. We recall that the free K-ring F on a set X over C is defined as the free product of K with the free C-algebra on X:

$$F = K *_C C\langle X\rangle = K_C\langle X\rangle.$$

Received January 17, 1974.

The universal field of fractions of $K_C\langle X\rangle$ is called the *free K-field on X over C* and is written $U = K_C(\langle X\rangle)$. We shall solve the word problem for $K_C(\langle X\rangle)$ under two restrictions. The first is definitely necessary and relates to the nature of the word problem in K, whereas the second is probably superfluous.

Given a field K and a central subfield C, we shall say that K is *dependable* over C if there is an algorithm which for each finite family of expressions for elements of K, in a finite number of steps leads either to a linear dependence relation between the given elements over C or shows them to be linearly independent over C.

When K is dependable over C, K and hence C has a soluble word problem, as we see by testing 1-element sets for linear dependence. To solve the word problem for $K_C(\langle X\rangle)$ it will be necessary to assume K dependable over C; this assumption is indispensable for we see that it holds whenever $K_C(\langle X\rangle)$ has a soluble word problem.

Secondly we shall assume C to be the precise centre of K (and not merely a subfield of the centre). This assumption is needed in the proof, which essentially verifies that expressions are nonzero by substituting elements of K for the variables. It is probably not essential; to dispense with it would need a closer study of the centre of $K_C(\langle X\rangle)$. We hope to return to this problem on another occasion. In any case our results provide a solution of the word problem for $C(\langle X\rangle)$, where C is any commutative field, relative to the word problem for C.

There is another difficulty which needs to be briefly discussed. As observed earlier, we shall be dealing with *expressions* of elements in a skew field, and our problem will be to decide when such an expression represents the zero element. But in forming these expressions we need to invert nonzero elements, therefore we need to solve the word problem already in order to *form* meaningful expressions. This problem could be overcome by allowing formal expressions such as $(a - a)^{-1}$; but we shall be able to bypass it altogether: instead of building up rational functions step by step, we can obtain them in one step by solving suitable matrix equations.

We recall that the universal field of fractions U of F is obtained by formally inverting all full matrices, where a matrix A is *full* if it is square, $n \times n$ say, and cannot be written as PQ, where P is $n \times r$, Q is $r \times n$ and $r < n$. In [1] it was shown that the word problem for U is soluble if the set of all full matrices over F is recursive.

Let us assume that C is infinite and that K is infinite-dimensional over C. Of course this must be understood in a constructive sense: Given $n > 0$, we can in a finite number of steps find n distinct elements of C and n elements of K linearly independent over C. Now the application[1] of the Proposition from [2] (whose hypothesis should include $(K:C) = \infty$) is justified in the proof of Theorem 3 of [1], and it follows that the set of all full matrices over F is recursive, provided that K is dependable over C.

When K is dependable over C we can decide when a square matrix over K is singular: We can reduce the matrix to diagonal form by PAQ-reduction and read off the rank. Now let A be any square matrix over $F = K_C\langle X\rangle$; if A is full, then by

[1] See the Added in proof at the end of this paper.

the Proposition in [2] we can specialize X to values in K for which A is nonsingular, and these values can be found in a finite number of steps. In fact, given any square matrix A over F, we can apply the Proposition in [2]; this will in a finite number of steps lead either to a set of values making A nonsingular, or to an equation showing A to be nonfull. To see this we need only restate Lemma 2 of [2] in a more precise form (where 'infinite' is understood in the constructive sense explained earlier):

LEMMA 1. *Let K be a field with an infinite centre C, such that K is dependable over C, and form the polynomial ring $K[t]$ in a central indeterminate t. Given a matrix $A(t)$ over $K[t]$, the rank r of $A(t)$ over the field of fractions $K(t)$ equals the supremum of the ranks of the matrices $A(\alpha)$ for $\alpha \in C$, and we can in a finite number of steps find $\alpha \in C$ such that $A(\alpha)$ has rank r.*

For we obtain a diagonal form for $A(t)$ by PAQ-reduction over the principal ideal domain $K[t]$, and the product of the diagonal terms gives us a polynomial f in t, whose zeros in C we must avoid. Since the number of such zeros is at most $\deg f$, we find the desired value α after at most $1 + \deg f$ trials.

With the help of this lemma we obtain a proof of Theorem 3 of [1] in the following form:

Let K be a field dependable over its centre C, and assume that C is infinite and $(K:C) = \infty$. Then for any square matrix A over $K_C\langle X\rangle$ we can in a finite number of steps either obtain a set of values of X in K for which A is nonsingular, or an equation showing that A is nonfull.

This establishes that the set of full matrices over F is recursive and hence the word problem in U is soluble. It remains to show that U is dependable over C. This will follow from the next lemma, where C need not be the exact centre of K.

LEMMA 2. *Let K be a field with central subfield C. If for every finite set Y the word problem for the free K-field on Y over C is soluble, then the free K-field on any set X over C is dependable over C.*

PROOF. Let U be the free K-field on X over C. We may assume X infinite, by embedding U in a free K-field on an infinite set containing X (that such an embedding exists, follows from Lemma 3 below, but is also easy to see directly). Given $u_1, \cdots, u_n \in U$, we have to determine whether the u's are linearly independent over C; we shall use induction on n, the case $n = 1$ being essentially the word problem for U. Let $n > 1$; we may assume $u_1 \neq 0$ and hence, on dividing by u_1 we may suppose that $u_1 = 1$. Only finitely many elements of X occur in $u_2, \cdots, u_n$, so we can find another element in X, y say. Write $u_i' = u_i y - y u_i$ and check whether $u_2', \cdots, u_n'$ are linearly dependent over C. If so, let $\sum_2^n u_i'\alpha_i = 0$, where $\alpha_2, \cdots, \alpha_n \in C$ and not all are zero, then $u = \sum_2^n u_i\alpha_i$ satisfies $yu = uy$. Since u does not involve y, it follows that u represents an element α in C (which can be computed by suitably specializing the x's), and hence $1\cdot\alpha - \sum_2^n u_i\alpha_i = 0$ is a dependence relation over C. Conversely, if there is a dependence relation $\sum_1^n u_i\alpha_i = 0$, where not all the α_i vanish, then not all of $\alpha_2, \cdots, \alpha_n$ can vanish (because $u_1 = 1 \neq 0$), and so $\sum_2^n u_i'\alpha_i = 0$ is a dependence relation between $u_2', \cdots, u_n'$. This completes the proof.

We note that since K is a subfield of U, K is dependable over C; thus the dependability of K is a consequence of the solubility of the word problem for U (on an infinite set).

We can state our conclusion as follows:

THEOREM 1. *Let K be a field dependable over its centre C. Assume further that C is infinite and that K is infinite-dimensional over C. Then the free K-field on any set X over C is dependable over C.*

§3. We now show how to modify our construction when C is finite. Given a field K with centre C, we form the polynomial ring $K[t]$ in a central indeterminate t. Its field of fractions is denoted by $K(t)$ or briefly by K'. By embedding $K(t)$ in the field of formal Laurent series $K((t))$ we see that the centre of K' is $C' = C(t)$.

First a general result, showing how free fields change under extension of the centre. We recall that a ring homomorphism is said to be *honest* if it keeps full matrices full.

LEMMA 3. *Let K be a field with centre C; further let K' be an extension field of K with centre C' which is a purely transcendental extension of C and such that $C' \cap K = C$. Then, for any set X, the mapping*

$$K_C\langle X\rangle \to K'_{C'}\langle X\rangle \tag{1}$$

is honest, and hence there is an embedding $K_C(\langle X\rangle) \to K'_{C'}(\langle X\rangle)$.

PROOF. Write $U = K_C(\langle X\rangle)$ as before, and assume that C is a simple transcendental extension of C, say $C' = C(\alpha)$. Then we can form $U(\alpha)$ as a field of fractions of the polynomial ring $U[\alpha]$, and $U(\alpha)$ contains $K(\alpha)$ as a subfield; further if L denotes the universal field of fractions of $U(\alpha)*_{K(\alpha)}K'$, then there is a natural mapping

$$K'_{C'}\langle X\rangle \to L. \tag{2}$$

Let A be a full matrix over $K_C\langle X\rangle$, then A is invertible over U and hence over L. Since any homomorphism maps nonfull matrices to nonfull matrices, it follows from (2) that A is full over $K'_{C'}\langle X\rangle$ and this shows (1) to be honest. Now the general case follows by induction on the number of indeterminates.

In fact we shall just need the case where there is a single indeterminate; thus if $K' = K(t)$, $C' = C(t)$, then $C' \cap K = C$ and we can apply Lemma 3.

We next observe that the field $K' = K(t)$ is dependable over C' whenever K is dependable over C. For let $u_1, \cdots, u_n \in K'$ and write these elements as rational fractions in t with a common denominator: $u_i = f_i g^{-1}$ where $f_i, g \in K[t]$; clearly it will be enough to test $f_1, \cdots, f_n$ for linear dependence over $C' = C(t)$. We may assume the f's numbered so that f_1 has the highest degree. Consider the leading coefficients of $f_1, \cdots, f_n$; if they are linearly independent over C, then the f's are linearly independent over C'. Otherwise we can find $\alpha_2, \cdots, \alpha_n \in C$ and positive integers $\nu_2, \cdots, \nu_n$ such that $f'_1 = f_1 - \sum_2^n f_i \alpha_i t^{\nu_i}$ has lower degree than f_1. Now the linear dependence of $f_1, \cdots, f_n$ over C' is equivalent to that of $f'_1, f_2, \cdots, f_n$ and here the sum of the degrees is smaller; using induction of the sum of the degrees of the f's we obtain the result.

Let us now return to Theorem 1. If in that theorem C is finite, or more generally, if there is no constructive process of obtaining infinitely many elements in C, we adjoin a central indeterminate t, so that K, C are replaced by $K' = K(t)$, $C' = C(t)$. By what we have just seen, K' is dependable over C' whenever K is so over C. Moreover, C' is infinite (in the constructive sense; e.g. we can take $1, t, t^2, \cdots$) and $(K' : C') = (K : C)$. It follows that the set of full matrices over $K'_{C'}\langle X\rangle$ is recursive

and hence, by Lemma 3, the set of all full matrices over $F = K_C\langle X\rangle$ is also recursive. Hence the word problem in U is soluble and, by Lemma 2, U is dependable over C. Thus Theorem 1 remains true even when the centre of K is finite.

§4. We now turn to the case where K is finite-dimensional over its centre, or where no process for constructing infinite linearly independent sets exists. Instead of adjoining a central indeterminate we form a skew extension.

Let K be a field with centre C, and let σ be an endomorphism of K leaving C elementwise fixed. We form the skew polynomial ring $R = K[y; \sigma]$ and its field of fractions

$$K' = K(y; \sigma). \tag{3}$$

If no power of σ is an inner automorphism, then the centre of K' is C. To see this we embed K' in the field of skew Laurent series $K((y; \sigma))$; let $f = \sum y^\nu a_\nu$ be in the centre of this field, then $fy = yf$, hence $a_\nu^\sigma = a_\nu$, and $cf = fc$ for all $c \in K$, hence $c^{\sigma^\nu} a_\nu = a_\nu c$. Since σ^ν is not inner for $\nu \neq 0$, it follows that $a_\nu = 0$ except when $\nu = 0$, and $a_0 c = c a_0$, i.e., $f = a_0 \in C$. Clearly K' is infinite-dimensional over its centre, e.g. the powers of y are linearly independent. Taking $C' = C$ in Lemma 3, we find that the natural embedding

$$K_C\langle X\rangle \to K'_C\langle X\rangle \tag{4}$$

is honest. Moreover, if K is dependable over C,[2] then so is K'. For let $u_1, \cdots, u_n \in K'$; as before we can write $u_i = f_i g^{-1}$, where $f_i, g \in K[y; \sigma]$ and it is again enough to test $f_1, \cdots, f_n$ for linear dependence over C. This time we single out the f's of maximal degree, $f_1, \cdots, f_r$ say. If their leading terms are linearly independent over C, then so are the f's; otherwise let $f_1' = f_1 - \sum_2^r f_i \alpha_i$ ($\alpha_i \in C$) have lower degree than f_1 and continue with $f_1', f_2, \cdots, f_n$ as before; again this process ends after a finite number of steps.

Now let K be a field with centre C such that K is dependable over C. To prove that the free K-field U is dependable over C we need only solve the word problem for U, by Lemma 2. Moreover, by the reduction in §3 we may take C to be infinite. Assume that K has an endomorphism over C no power of which is inner, and form the skew function field K'. Then K' is infinite-dimensional over its centre C, and K' is dependable over C, hence the set of all full matrices over $K'_C\langle X\rangle$ is recursive and so is the set of all full matrices over $K_C\langle X\rangle$, because (4) is honest. This solves the word problem for U.

Finally if K has no endomorphism over C whose powers are never inner, we carry out the construction (3) with the identity automorphism. The result is a field K' with centre $C(y)$; now repeat the process with the endomorphism $f(y) \mapsto f(y^2)$. Certainly no power of this is inner and we obtain a field K'' whose centre is C and $(K'':C) = \infty$.

We have thus proved the following sharper form of Theorem 1; the last part follows from the remark after Lemma 2.

---

[2] σ is computable, in an obvious sense.

THEOREM 1′. *Let K be a field, dependable over its centre C, and denote by U the free K-field on a set X over C. Then U has soluble word problem and is again dependable over C. Conversely, if the word problem in U is soluble (for an infinite set X), then K is dependable over C.*

ADDED IN PROOF. Proposition 2 depends on Amitsur's Theorem on generalized polynomial identities (cf. S. A. AMITSUR, *Generalized polynomial identities*, ***Transactions of the American Mathematical Society***, vol. 114 (1965), pp. 210–226) and it is necessary to assume a constructive form of this theorem here for K: Given $f \in K_C\langle X\rangle$ such there is a method (an 'oracle') for obtaining a set of arguments for which f is nonzero in a finite number of steps.

REFERENCES

[1] P. M. COHN, *The word problem for free fields*, this JOURNAL, vol. 38 (1973), pp. 309–314.

[2] ———, *Generalized rational identities*, ***Ring theory*** (R. Gordon, Editor), *Proceedings of a Conference on Ring Theory* (Park City, Utah, 1971), Academic Press, New York, 1972, pp. 107–115.

BEDFORD COLLEGE
LONDON NW1 4NS, ENGLAND