MODULES OVER RINGS OF WORDS

WILLIAM G. LEAVITT

Introduction. A right module M over a ring K with unit is called a *free module* if it is finitely based. If the basis number of such a module is not invariant then it must necessarily contain an infinite independent set [1, Theorem 7]. A free module may, on the other hand, contain infinite independent sets but nevertheless have invariant basis number. If, for example, K contains no zero divisors, then the ring K considered as a module over itself must have invariant basis number (1), since otherwise there would exist independent $\{a_i\}$ $(i=1, \cdots, n \geqq 2)$ such that $1=\sum_1^n a_i x_i$. But the independence of the $\{a_i\}$ would then imply that $x_i a_j=0$ $(i \neq j)$. Now it has been shown by Ore [2, p. 466] that if a ring K without zero divisors satisfies the "right multiple" property: for any $a, b \in K$ there exist nonzero $x, y \in K$ such that $ax+by=0$, then K is imbeddable in a division ring. Thus the nonimbeddable ring of Malcev [3] is a module of the required type.

In the present paper we consider the question of invariance of basis number for modules over a number of "word" rings of the type introduced by Malcev, the purpose being to fill certain gaps left in [1] as open possibilities. It was shown, for example, that for a ring K without zero divisors the right multiple property was sufficient to ensure the invariance of the basis number for all modules over K, but it was left open as to whether or not this condition is necessary. The first example considered, however (the ring of words itself) shows that this is not the case. A somewhat weaker condition, that of imbeddability in a division ring, is also sufficient for the invariance of basis number and again the question of its necessity was left open. This question is settled, also in the negative, by considering Malcev's ring.

Another possibility left open in [1] is based on the following considerations: It was shown [1, Theorem 15] that invariance of basis number is a property which carries downward with decreasing basis number. That is to say, if over a ring K a module M exists whose basis number is invariant, then every module over K having a basis no longer than that of M must also have invariant basis number. The possibility thus exists, that for some fixed integer n a ring K might

Presented to the Society, November 26, 1954; received by the editors May 20, 1954 and, in revised form, May 8, 1955.

exist such that a module over K has invariant basis number if and only if it has a basis of length $<n$. We show, in the final section, that such a ring may be constructed for the case $n=2$.

Certain of the methods used in establishing the properties of this ring are due to Shepherdson [4], although his theorems are not directly applicable.

The Ring of Words. Consider a set $\{x_i\}$ $(i=1, \cdots, n \geqq 2)$ of symbols and let R be the ring of all finite sums of "words" built from these symbols; that is, R is the ring of all polynomials in $\{x_i\}$ with integral coefficients, cf. [4, p. 73]. Note that R is also assumed to contain words of zero length, so R has a unit. We prove first that R has no zero divisors. Suppose $\alpha, \beta \in R$ and consider the product $\alpha\beta$. If $\alpha \neq 0$ it must contain words of maximum length. For definiteness, suppose one of these has x_1 as leading symbol, so that α contains a term nx_1z with z a word and $n \neq 0$ an integer. (We assume that all like words are collected.) Any other longest word of α beginning with x_1 must then be of form x_1z' with $z' \neq z$. Now it is clear that the longest words of $\alpha\beta$ are products of longest words from α and β, thus if β contains a longest term my, the product contains nmx_1zy. Any other longest word whose initial symbol is x_1, since it must come from a longest word of α, will begin with x_1z'. Thus since two words are equal only if their respective symbols are the same, no other term can cancel nmx_1zy and hence $\alpha\beta \neq 0$.

Now let us suppose that there exists a relation $x_1\alpha = x_2\beta$ with $\alpha, \beta \in R$. Since every word on the left begins with x_1, and no word on the right, it follows that $\alpha = \beta = 0$. Thus R contains independent members, and hence [1, Theorem 6 and Theorem 7] every module over R contains an infinite independent set. We shall next show that modules over R nevertheless have invariant basis number.

If a module over R exists having bases of length m and n $(m>n)$, then there must exist matrices U and V, respectively m by n and n by m, such that $UV = I_m$ and $VU = I_n$ (with I_m and I_n identity matrices). Now if $\{y_i\}$ is the set of all words appearing in either U or V we may write

$$U = \sum U_i y_i, \qquad V = \sum V_i y_i, \tag{1}$$

with U_i and V_i matrices of integers. Clearly the product UV only contains constants if one of the words, say $y_0, = 1$ and if $U_0V_0 = I_m$, and $V_0U_0 = I_n$. But U_0V_0 has rank $\leqq n < m$, and hence the first of these relations is impossible. Thus:

THEOREM 1. *There exists a ring without zero divisors over which all*

free modules contain infinite independent sets, but have invariant basis number.

The ring of Malcev. We now establish a similar result for the ring constructed by Malcev.

THEOREM 2. *There exists a ring without zero divisors not imbeddable in a division ring over which all free modules contain infinite independent sets, but have invariant basis number.*

Let K be the ring of Malcev [3]. It was shown that K has no zero divisors, but is not imbeddable in a division ring. From the result of Ore [2] it follows that K must contain independent members, and hence every module over K contains an infinite independent set. We thus need only show that all modules over K have invariant basis number.

This ring is a residue class ring $K=R/H$ of the ring R of words in symbols $\{a, b, c, d, x, y, u, v\}$, where H is the ideal with basis $\{ax-by, cx-dy, au-bv\}$. This ideal satisfies the conditions of [4, Theorem 3.0 (p. 75)] so that an effective means exists for deciding whether or not a member of R belongs to H. (This was of course also shown by Malcev.) The process consists of successive elimination from an $\alpha\in R$ of members of a set S: $\{ax, cx, au\}$ using relations

$$ax = by, \qquad cx = dy, \quad \text{and} \quad au = bv. \tag{2}$$

This may be continued, arriving in a finite number of steps to a normal form $N(\alpha)$ containing no members of S. Then since $\alpha-N(\alpha)\in H$ and $N(\alpha)\in H$ if and only if $N(\alpha)=0$, we have that $\alpha\in H$ if and only if $N(\alpha)=0$.

We now suppose again that a module M has bases of length m, n with $m>n$, so that m by n and n by m matrices U, V exist with $UV=I_m$. Now in reducing elements of UV to normal form by (2) it is clear that, as in the previous section, we only get a constant term from constant terms of both U and V. Thus using the expression (1) we again get the contradictory relation $U_0V_0=I_m$.

Modules without invariant basis number. We now proceed to the construction for $n=2$ of a ring over which a module will have invariant basis number if and only if it has a basis of length $<n$.

Let R be the word ring in symbols $\{a_{ij}, b_{st}\}$ $(i, t=1, 2, 3; j, s=1, 2)$. If A and B are the matrices whose elements are respectively $\{a_{ij}\}$ and $\{b_{st}\}$, we define H to be the set of all sums of members of R of form $\beta\alpha\gamma$ with $\beta, \gamma\in R$ and α any element of $AB-I_3$ or $BA-I_2$. In order to show that H is actually an ideal of R, it is necessary to show

that a solution exists for the decision problem as to whether or not an $\alpha \in R$ belongs to H. Define a set S: $\{a_{i1}b_{1j},\ b_{s1}a_{1t}\}$ $(i, j=1, 2, 3;\ s, t=1, 2)$. For any $\alpha \in R$, let α' be the result of eliminating a member of S from any word of α using some relation from

$$AB - I_3 = 0 \quad \text{and} \quad BA - I_2 = 0. \tag{3}$$

Any member of R obtainable from α by a finite number of such transformations will be said to be *equivalent* to α. Clearly $\alpha - \alpha' \in H$, so that $\alpha \in H$ if and only if $\alpha' \in H$. The same applies at any further stage in a sequence of such transformations and thus to a normal form $N(\alpha)$ (if it exists) equivalent to α and containing no member of S.

We now show that such a form not only exists but is also independent of the manner in which the reduction is effected.

LEMMA 1. *For any $\alpha \in R$ there exists a unique form $N(\alpha)$ equivalent to α, and containing no member of S.*

Clearly every word of length $\leqq 1$ is in normal form, and we suppose for induction that a unique normal form exists for any word of length $\leqq n-1$. Let x be a word of length n; we consider three cases:

Case I. $x=yz$ where the word formed by the final symbol of y and the first symbol of z is not a member of S. The first transformation of x must involve only symbols of y or z alone. A transformation (say of y) will yield a set of words of equal length whose final symbol has unchanged second subscript, together (possibly) with shorter words. Thus the only future transformation which could involve a descendant of both y and z will be in a word of length $\leqq n-1$. By induction, the reduction to normal form of such a word is unique, and could therefore have been obtained by first reducing separately the descendants of y and of z, and then reducing the products. Thus any reduction of x could be obtained by first reducing y and z separately, and then reducing any products (of shorter words). Since by induction $N(y)$ and $N(z)$ exist, it follows, using the above argument on shorter words, that $N(x)$ also exists.

Case II. All subscripts of symbols of x are 1 (say, for example, $x=a_{11}b_{11}\cdots b_{11}a_{11}$). An initial transformation will be of $a_{11}b_{11}$ (or $b_{11}a_{11}$), and the transformed x will be of form $x'=a_{11}b_{11}\cdots(-\sum b_{1t}a_{t1})\cdots b_{11}a_{11}+y$, where $y=a_{11}b_{11}\cdots b_{11}a_{11}$ is of length $n-2$. By induction $N(y)$ exists. Also, the words of x' come under Case I so $N(x')$ exists, and in fact, proceeding outward from the initially transformed pair, $N(x')=(-1)^{n-1}\sum a_{1i}b_{ij}\cdots b_{uv}a_{v1}$. Since this form, and also y, are independent of where the initial pair was chosen, it follows that the final reduced form is unique.

Case III. All interior subscripts of symbols of x are 1, but one or more exterior subscripts are not (say, for example, $x=a_{h1}b_{11}\cdots$). If the initial transformation involves an end pair $x'=-\sum_i a_{hi}a_{i1}\cdots$, then by Case I further reduction is unique and we reach

$$N(x') = (-1)^{n-1}\sum_{i,j,\cdots} a_{hi}a_{ij}\cdots. \tag{4}$$

If, on the other hand, the initial transformation involves a pair such as $a_{11}b_{11}$ (say the kth and $(k+1)$st symbols), then $x'=a_{h1}b_{11}\cdots(-\sum a_{1s}b_{s1})\cdots+y$, where $y=a_{h1}b_{11}\cdots$ is of length $n-2$, and is independent of where the initial pair was chosen. Again, as in Case II, $N(x')$ exists. If we proceed with further transformations from the left, we reach $(-1)^{k-2}\sum_{i,j,\cdots} a_{hi}b_{ij}\cdots a_{tr}b_{r1}(-\sum a_{1s}b_{s1})a_{11}\cdots$. Now for each r there is in this sum an equal s, and since $(b_{r1}a_{1r})'=1-\sum_i b_{ri}a_{ir}$, we obtain from the next transformation

$$(-1)^k\sum_{i,j,\cdots} a_{hi}b_{ij}\cdots a_{tr}b_{ru}a_{us}b_{s1}a_{11}\cdots + (-1)^{k-1}\sum_{i,j,\cdots} a_{hi}b_{ij}\cdots a_{tr}b_{r1}a_{11}\cdots.$$

The first portion clearly reduces to the form (4) above, while the second portion is the negative of the form to be obtained from y. Thus again the reduction exists and is unique.

By induction it follows that $N(x)$ exists for a word of any length. Since any $\alpha\in R$ contains no more than a finite number of words, and since the reduction of each word is unique, it follows that $N(\alpha)$ exists for all $\alpha\in R$. The uniqueness also implies

$$N(\alpha+\beta) = N(\alpha)+N(\beta), \tag{5}$$

$$N(\alpha\beta) = N[N(\alpha)N(\beta)]. \tag{6}$$

It is now clear that a solution exists for the decision problem as to whether or not an $\alpha\in R$ is a member of H, for if $\alpha\in H$ then a finite set of transformations exist leading to zero and so $N(\alpha)=0$. Conversely, if $N(\alpha)=0$ then $N(\alpha)\in H$ and so $\alpha\in H$. Thus again the criterion $\alpha\in H$ if and only if $N(\alpha)=0$. H is therefore a two-sided ideal of R, and we may speak of the factor ring $K=R/H$. From the way H was constructed, a module over K exists (the module of all couples) which does not have invariant basis number. Thus no module with a basis of length $\geqq 2$ can have invariant basis number.

LEMMA 2. *The ring K contains no zero divisors.*

This is equivalent to saying that if $\alpha,\ \beta\notin H$ then $\alpha\beta\notin H$; that is, $N(\alpha),\ N(\beta)\neq 0$ implies $N(\alpha\beta)\neq 0$. Since $N(\alpha\beta)$ can be reached by

first reducing α and β, we may assume α and β in normal form with $\alpha, \beta \neq 0$. Let us suppose, now, that $N(\alpha\beta)=0$; then it is clear that neither α nor β can be a constant, for the product would be simply a multiple of nonzero α or β. Thus α and β must contain words of length $\geqq 1$. If one of the longest words appearing in α is xa_{hk} then α contains $\sum_j m_j x a_{hj}$ with $m_k \neq 0$. (A similar proof will apply if a longest word of α ends in some b_{hk}.) We have two cases:

Case I. β contains a sum of longest words $\sum_i n_i a_{it} y$ with some $n_s \neq 0$. The product of these terms is already in normal form and since they are longest words of $\alpha\beta$ they cannot be canceled by any other words of the product. We would thus have the relation $m_j n_i = 0$, contradicting $m_k n_s \neq 0$.

Case II. β contains a sum of longest words $\sum_i n_i b_{it} y$ with some $n_s \neq 0$, then $N(\alpha\beta)$ will contain $\sum_{j \neq i} m_j n_i x a_{hj} b_{it} y + \sum_{j=2}^{3} (m_j n_j - m_1 n_1) x a_{hj} b_{jt} y$. Again these terms cannot be canceled by any other terms in $N(\alpha\beta)$ and thus all coefficients must be zero. From the first term this could mean all $n_j = 0$ $(j \neq k)$. But the second term would then give the contradicting relation $m_k n_k = 0$. Hence the conclusion $N(\alpha\beta) \neq 0$.

Since K has no zero divisors, it is clear that every module with basis of length 1 has invariant basis number, since otherwise a column A and row B exist for which $AB = I_2$. We thus have

THEOREM 3. *There exists a ring K without zero divisors such that a free module over K has invariant basis number if and only if it has a basis of length* 1.[1]

REFERENCES

1. W. G. Leavitt, *Finite dimensional modules*, Anais da Academia Brasileira de Ciências, Rio de Janeiro, vol. 27 (1955) pp. 241–250.

2. Oystein Ore, *Linear equations in non-commutative fields*, Ann. of Math. vol. 32 (1931) pp. 463–477.

3. A. Malcev, *On the immersion of an algebraic ring into a field*, Math. Ann. vol. 113 (1937) pp. 686–691.

4. J. C. Shepherdson, *Inverses and zero divisors in matrix rings*, Proc. London Math. Soc. (3) vol. 1 (1941) pp. 71–85.

UNIVERSITY OF NEBRASKA

[1] It may be remarked that a ring similar to that described above is constructable for any n. It is clear that the proofs of Lemmas 1 and 2 may be extended to this case, so the ring is an integral domain over which no module with basis of length $\geqq n$ has invariant basis number. When $n>2$ the possibility thus exists that for some k with $1<k<n$ a module over the ring has invariant basis number if and only if it has a basis of length $\leqq k$.

Added in proof. The author is now able to show that in fact $k=n-1$.