PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 27, Number 3, March 1971

MINIMAL GENERATING SETS FOR FREE MODULES

L. M. BRUNING AND W. G. LEAVITT

ABSTRACT. Let R be a ring admitting a free module with generating set shorter than the length of a basis. If n is the shortest basis among all such modules and m the length of its shortest generating set then $n=m+1$ and every free module with basis of length $\geqq m+1$ has a generating set of length m. If R has module type (h, k) then $m=h$, that is an R-module with basis of length $u<h$ not only has all bases of length u but also has no generating set of length $<u$. The integer m together with the module type define a new ring invariant which satisfies many of the properties of the module type.

1. **Introduction.** In the following, we will consider only rings with unit. A finitely based module over a ring is said to have rank t, if it has a basis of length t. A module may not necessarily have unique rank. Modules with unique rank are said to have *dimension* and a ring admitting only such modules is termed *dimensional*. The second author [2, p. 114, Theorem 1] has shown that a given ring admits only certain characteristic finitely based modules; that is, for any nondimensional ring R there exist unique positive integers, h, k, such that (i) any R-module M with a basis of length $<h$ has dimension; (ii) for any R-module M with a basis of length $\geqq h$ there exists an integer p, where $h \leqq p < h+k$ such that M has a basis of length r if and only if $r=p+uk$ for some integer $u \geqq 0$. Moreover, such an R-module exists for arbitrary p. Thus an R-module M with rank $<h$ is isomorphic only to a module with the same rank, while if its rank is $p \geqq h$ then $M \cong M'$ if and only if M' has rank $r \geqq h$ with $r \equiv p \pmod{k}$. Such a ring is said to have *module type* (h, k). Dimensional rings are designated *module type d*.

Certain rings admit finitely based modules of rank t which can be generated by fewer than t elements. Clearly all nondimensional rings have this property. P. M. Cohn [1, p. 221] has given an example of a dimensional ring which has this property, but shows that no module of rank t of a Noetherian ring, Artinian ring, or commutative ring can be generated by fewer than t elements. He also proposes a classification of rings admitting a free module with a set of generators shorter than the length of a basis by the two integers m and n, where

Received by the editors April 8, 1970.
AMS 1969 *subject classifications*. Primary 1640, 1650.
Key words and phrases. Generators of free modules, rank of a module, module type.

n is the least rank of a free module which can be generated by fewer than n elements and m is the least number of elements required to generate it.

In this paper, we will investigate (for such a ring) the possibilities for m and n. Our main tool will be a certain epimorphism theorem of P. M. Cohn [1, p. 216]. We will show first that n must be equal to $m+1$ and that if a module has a rank $t \geqq m+1$, the module has a minimal generating set of length m. In the special case where the ring is nondimensional, that is, has module type (h, k), we find that no module of rank less than h can be generated by fewer elements than the length of a basis, and thus it follows that $m=h$.

In the final section, a classification of rings by m, the least number of elements required to generate a module of greater rank, and the module type of a ring is developed. This classification has a natural partial order imposed by the partial ordering of the module types, and is shown to satisfy many of the theorems valid for the module type.

2. **Determination of the length of minimal generating sets.** Clearly any module having a basis of length t is isomorphic to any other module having a basis of length t. We designate such a module by F_t. We will use the result [1, p. 216]:

THEOREM A (COHN). *F_t has a generating set of length m if and only if $F_m \cong F_t \oplus K$ for some R-module K.*

Let $\mathcal{S}$ be the class of all R-modules, M, such that for some k, M has a generating set of length k and a basis of length greater than k. Let m and n be positive integers with the property:

(i) n is the length of the shortest basis of any $M \in \mathcal{S}$ which can be generated by fewer than n elements, and m is the least number of elements required to generate F_n.

THEOREM 1. *Let R be a ring with nonempty $\mathcal{S}$. Suppose m and n have property* (i), *then $n=m+1$.*

PROOF. $n>m$, therefore $n \geqq m+1$. Suppose $n>m+1$. Since F_{m+1} is isomorphic to the module generated by the first $m+1$ elements of a basis of F_n and $F_{n-(m+1)}$ is isomorphic to the module generated by the remainder of the basis of F_n, we have $F_n \cong F_{m+1} \oplus F_{n-(m+1)}$. But by Theorem A this implies that F_{m+1} has a generating set of length m because F_n does. Therefore F_{m+1} belongs to $\mathcal{S}$. Since n is the length of the smallest basis of any module belonging to $\mathcal{S}$, $n=m+1$.

THEOREM 2. *Let R have nonempty $\mathcal{S}$ and n and m have property* (i), *then if $t \geqq n$, F_t has a minimal generating set of length m.*

PROOF. By Theorem 1 and the definition of m and n, we have that $F_n = F_{m+1}$ has a minimal generating set of length m and hence there exists by Theorem A an epimorphism from F_m onto F_{m+1}. Assume for induction that F_{m+k} has a minimal generating set of length m. Then $F_{m+k+1} \cong F_{m+k} \oplus F_1$ has a generating set of length $m+1$. Thus F_{m+k+1} is the epimorphic image of F_m and hence has a minimal generating set of length m. The result thus follows by induction.

We now consider a ring R with module type (h, k). We will show that $m = h$, that is, no R-module with a basis of length $u \leqq h$ can be generated by fewer than u elements. On the other hand, those modules with bases of length $u > h$ have minimal generating sets of length h.

LEMMA 1. *Let R be of module type (h, k) and let r be the minimum length of a generating set for F_h. Whenever F_t has a minimal generating set of length $s < t$ then $r = s < t$.*

PROOF. First, suppose $t < r \leqq h$. We have $F_r \cong F_t \oplus F_{r-t}$ and $F_r \cong F_h \oplus A$ for some A. Also $F_s \cong F_t \oplus B$ for some B and therefore $F_s \oplus F_{r-t} \cong F_h \oplus A \oplus B$. But, $F_s \oplus F_{r-t}$ has a basis of length $s + (r-t)$, hence F_h has a generating set of length $s + (r-t) < r$. This contradicts the minimality of r, and so we conclude that $r \leqq t$.

If $r = t$, then $F_s \cong F_t \oplus B \cong F_r \oplus B \cong F_h \oplus A \oplus B$ and again $r \leqq s$ by the minimality of r. Actually this case is impossible, since $s < t$.

We therefore have $r < t$. By a similar argument to that above, we have $F_s \cong F_t \oplus B \cong F_r \oplus F_{t-r} \oplus B \cong F_h \oplus A \oplus F_{t-r} \oplus B$. Therefore F_h has a generating set of length s. By the minimality of r this implies $r \leqq s$.

Now suppose $h \geqq t$, then $F_r \cong F_h \oplus A \cong F_t \oplus F_{h-t} \oplus A$, which implies that F_t has a generating set of length r. Therefore $s \leqq r$. On the other hand, if $h < t$, there exists an integer u such that $t < h + uk$. $F_{h+uk} \cong F_t \oplus F_{h+uk-t}$ and $F_{h+uk} \cong F_h$, since R has module type (h, k). Thus F_t has again a generating set of length r. In either case it follows that $r = s$.

Note, that by the definition of m in (i), this lemma shows that $m = r$. We will now show that actually $m = h$.

THEOREM 3. *Let R be of module type (h, k), m as in* (i), *and r the minimum length of a generating set for F_h, then $m = r = h$.*

PROOF. (Clearly $r \leqq h$.) F_h has a generating set of length r, therefore $F_r \cong F_h \oplus A$ for some A. Now, since R has module type (h, k), we have $F_{h+k} \cong F_h$. Therefore $F_{r+k} \cong F_h \oplus A \oplus F_k \cong F_{h+k} \oplus A \cong F_h \oplus A \cong F_r$.

But by the definition of module type this implies that $r \geqq h$, and hence we have $r=h$. Thus by the lemma $m=r=h$.

3. **The module class of a ring.** It is thus clear by Theorems 2 and 3 that for a ring R with nonempty $\mathcal{S}$, there is a unique integer m (equal to h, when R has type (h, k)) such that no R-module with a basis of length $u \leqq m$ can be generated by fewer than u elements, whereas a module with a basis of length $u > m$ has a minimal generating set of length m. We will call $(m, t) = C(R)$ the *module class* of a ring R, where m is this unique integer and t is the module type of R. We also set $C(R) = D$ when $\mathcal{S}$ is empty, that is, when no F_r is generated by fewer than r elements, and $C(R) = 0$ when R is the ring with 0 as its only element.

The following partial order was established for module types in [2]. (i) $0 < (h, k) < d$ for all (h, k) and (ii) $(h, k) \leqq (h', k')$ if and only if $h \leqq h'$ and $k \mid k'$. Using this partial ordering, we may partially order module classes by $0 < (m, t) < D$ for all module classes (m, t), and $(m, t) \leqq (m', t')$ if and only if both $m \leqq m'$ and $t \leqq t'$. Note, that when $t' < d$, the condition $t \leqq t'$ automatically implies $m \leqq m'$.

In [2], examples are given of rings of arbitrary module type and hence of all classes (m, t) where $t < d$. The ring $U_{m,n}$ constructed by Cohn [1, p. 221] is clearly of class (m, d). Since, for example, fields have class D, we thus have examples of rings of all module classes.

Now it is well known that the existence of an R-module with a generating set of length m and a basis of length n is equivalent to the existence of m by n and n by m matrices C and D over R such that $DC = I_n$, where I_n is the identity matrix. From this observation, the following propositions easily follow and will be stated without proof.

PROPOSITION 1 (COHN). *If $\phi: R \to R'$ is a unit-preserving homomorphism then $C(R') \leqq C(R)$ where $C(R')$ and $C(R)$ are the respective module classes of R' and R. Thus $C(R') = D$ implies $C(R) = D$.*

PROPOSITION 2. *If R is a subring of a ring R', with the same unit, then $C(R') \leqq C(R)$.*

PROPOSITION 3. *If R' is the ring of polynomials over R in a set $\{x_i\}_{i \in I}$ of symbols, then $C(R') = C(R)$.*

PROPOSITION 4. *If I is a right (left) ideal of R and I is itself a ring with unit, then $C(I) \leqq C(R)$.*

In the following theorem, it is shown that we can have $C(R_1)$ not equal to $C(R)$ where $R \cong R_1 \oplus R_2$. Thus the condition in Proposition 1 that ϕ be unit-preserving cannot be removed.

THEOREM 4. *If* $R \cong R_1 \oplus R_2$ *is a ring direct sum with* $C(R_i) = (m_i, t_i)$ $(i=1, 2)$ *then* $C(R) = (\max(m_1, m_2), t_1 \cup t_2)$. *If either* $C(R_i) = D$ *then* $C(R) = D$.

PROOF. The natural homomorphisms of R onto R_1 and R_2 require that $C(R_1) \leqq C(R)$ and $C(R_2) \leqq C(R)$. Thus, if either $C(R_1)$ or $C(R_2)$ equals D then $C(R) = D$. Therefore suppose $C(R_1) = (m_1, t_1)$ and $C(R_2) = (m_2, t_2)$. By above we have $(\max(m_1, m_2), t_1 \cup t_2) \leqq C(R)$.

For definiteness, let $m_2 \geqq m_1$ and set $s = m_2 - m_1$. By Theorem 1, there exists an R_1-module M_1, with a generating set of length m_1 and a basis of length m_1+1. Therefore $M_1' = M_1 \oplus F_s$, where F_s is the free R_1-module generated by s elements, has a generating set of length $m_1 + s = m_2$ and basis of length $m_1 + 1 + s = m_2 + 1$. There also exists an R_2-module M_2, with a generating set of length m_2 and a basis of length m_2+1. Define $R_1 M_2 = 0$ and $R_2 M_1' = 0$, then $M_1' \oplus M_2$ is an R-module with a generating set of length m_2 and a basis of length m_2+1. Set $C(R) = (m', t)$, then what we have just shown is that $m' \leqq \max(m_1, m_2)$. By [2, Theorem 3] $t = t_1 \cup t_2$ and hence $C(R) = (\max(m_1, m_2), t_1 \cup t_2)$.

REFERENCES

1. P. M. Cohn, *Some remarks on the invariant basis property*, Topology **5** (1966), 215–228. MR **33** #5676.

2. W. G. Leavitt, *The module type of a ring*, Trans. Amer. Math. Soc. **103** (1962), 113–130. MR **24** #A2600.

UNIVERSITY OF NEBRASKA, LINCOLN, NEBRASKA 68101