

DEPENDENCE IN RINGS. II. THE DEPENDENCE NUMBER

BY
P. M. COHN

1. **Introduction.** Free ideal rings, introduced in [6], have the property that all relations of the form

$$(1.1) \quad a_1 b_1 + \cdots + a_n b_n = 0$$

are 'trivial' in some sense. In fact this statement, with the appropriate notion of triviality, characterizes locally free ideal rings (semifirs). More restrictive notions of triviality lead to strong *GE*-rings (called *GE*-semifirs in [8]) and rings with a weak algorithm [5].

A natural generalization is to consider rings in which all relations (1.1) are trivial, for a fixed n . It turns out that such rings share many of the properties of semifirs, strong *GE*-rings or rings with a weak algorithm, depending on the notion of triviality used. They resemble these rings more closely, the higher the value of n , although they form a wider class, by the examples given in [9] and in §4 below.

The widest notion of triviality, *GL-triviality*, of (1.1) is obtained by assuming that there exists an invertible matrix P such that for each $i=1, \dots, n$, either the i th coordinate of the row $(a_1, \dots, a_n)P$ or the i th coordinate of the column $P^{-1}(b_1, \dots, b_n)$ is zero. A ring in which every relation (1.1) such that $n \leq N$ is *GL-trivial*, is called an *N-fir*. These rings were introduced and studied in [1]. For $N=1$ they are the (noncommutative) integral domains, and for $N=2$ they are the weak Bézout rings.

A narrower class of rings, the strong *GE_n-rings*, is obtained by insisting in the above definition that P be a product of elementary matrices. For a more precise definition the reader is referred to [1], where these rings are described in some detail and their relation to *N*-firs and the *GE*-rings defined in [8] is clarified.

In general it is difficult to determine whether or not a given ring is an *n-fir* or a strong *GE_n-ring*, and the main object of the present paper is to describe a means of making this determination easier. The method consists in a modification of the weak algorithm introduced in [3], called the *n-term weak algorithm*. This is defined in §2, where it is shown that any ring with an *n-term weak algorithm* is an *n-fir* and in fact a strong *GE_n-ring*; it only remains to have a method for deciding when the *n-term weak algorithm* holds. Put another way, we want to find the largest n such that the *n-term weak algorithm* still holds. This leads to the definition of a

numerical invariant associated with any ring R , its *dependence number* $\lambda(R)$, as the least integer n for which no weak algorithm exists in R . An answer to our problem is now provided in §3, where a theorem is proved giving a lower bound on the dependence number of a ring given by a suitable presentation (Theorem 3.1). Special cases of this theorem were proved and applied in [9]. From the present version, these and many other results can be deduced with little extra effort. Some examples are given in §4.

I am grateful to G. M. Bergman and A. J. Bowtell for a critical reading of parts of this paper, especially §3, which led to the removal of some inaccuracies.

2. The n -term weak algorithm and the dependence number. Throughout, all rings are associative, with 1, all modules are unital and homomorphisms preserve 1. Further, by an integral domain we understand a not necessarily commutative ring without zero-divisors other than zero, and a division ring will be called a field, the prefix "skew" being sometimes used for emphasis.

We recall that in [5] the notion of a weak algorithm was defined for (positively) filtered rings; the definition may be generalized as follows.

A filtered ring R is said to satisfy the *n -term weak algorithm* if in any right dependent set of at most n elements, each element of maximal value is right dependent on the rest. If instead, R is negatively filtered and each element of minimal value in the set is R -dependent on the rest, R is said to satisfy the *n -term inverse weak algorithm*.

Thus R satisfies the weak algorithm precisely when the n -term weak algorithm holds for all n . The *dependence number* (cf. [9]) of R relative to the filtration v , denoted by $\lambda_v(R)$, may now be defined as the least integer n for which the n -term weak algorithm fails to hold or $+\infty$ if it holds for all n . Similarly the *inverse dependence number* of R relative to v , denoted by $\mu_v(R)$, is the least integer n (or $+\infty$) for which the n -terms inverse weak algorithm fails to hold. In what follows, $\lambda_v(R)$ is used mainly for positively filtered rings, while $\mu_v(R)$ occurs for negative filtrations (cf. [4]).

As an example we note that for a field K with the trivial filtration, $\lambda_v(K) = \mu_v(K) = \infty$; in the opposite direction, if R satisfies the 2-term weak algorithm relative to the trivial filtration then R is a (skew) field, as is easily seen.

We note without proof (cf. Theorem 3.2 of [3]) that the dependence number is left-right symmetric, i.e., $\lambda_v(R) = \lambda_v(R^0)$, where R^0 is the opposite ring. Later we shall see that $\lambda_v(R)$ can assume any (positive integral) value, but in the commutative case the only possible values for $\lambda_v(R)$ are 1, 2, ∞ . This follows from the next result, whose proof is left to the reader.

THEOREM 2.1. *Let R be a positively filtered ring in which any two elements not both zero have a common right multiple with coefficients not both zero, then there are exactly three possibilities:*

- (i) $\lambda_v(R) = 1$: v is not a valuation,

(ii) $\lambda_v(R)=2$: v is a valuation, but the (Euclidean) division algorithm does not hold,

(iii) $\lambda_v(R)=\infty$: v is a valuation and the division algorithm holds in R .

Of course a corresponding result holds for the inverse weak algorithm.

In order to make these notions applicable to any rings, we define (as in [9]) the *dependence number* $\lambda(R)$ as the supremum of $\lambda_v(R)$ as v ranges over all positive filtrations of R . This is a numerical invariant associated with any ring; it is always defined, since every ring has e.g., the trivial filtration, and it is a positive integer or $+\infty$. We stress that $\lambda(R)=\infty$ means: for every n there exists a filtration v such that $\lambda_v(R) > n^{(1)}$.

We can now describe the connexion between the dependence number and strong GE -rings, but first we need to interpret the condition $\lambda(R)=1$.

PROPOSITION 2.2. *A ring R is an integral domain if and only if $\lambda(R) > 1$.*

Proof. The sufficiency follows by choosing v with $\lambda_v(R) > 1$ (cf. [9]); conversely, in an integral domain, $\lambda_v(R) > 1$ holds for the trivial filtration.

THEOREM 2.3. *Let R be a ring and n any integer such that $n < \lambda(R)$. Then R is a strong GE_n -ring and hence also an n -fir.*

Proof. Choose v such that $\lambda_v > n$. For $n=1$ the result follows from Proposition 2.2 and the definitions, so we may assume $n > 1$, as well as the fact that R is an integral domain. We have to show that every relation of at most n terms is GE -trivial. Let

$$(2.1) \quad a_1b_1 + \dots + a_kb_k = 0 \quad (b_i \text{ not all } 0, k \leq n)$$

be a relation in R ; we have to find a matrix $P \in GE_k(R)$ (the group generated by elementary $k \times k$ matrices over R) such that $(a'_1, \dots, a'_k) = (a_1, \dots, a_k)P$ has a zero coordinate. Suppose that no such P exists and choose $P \in GE_k(R)$ such that $\sum v(a'_i)$ assumes its least value. By applying the corresponding transformation (viz. P^{-1}) to b_1, \dots, b_k and writing again $a_1, \dots, a_k, b_1, \dots, b_k$ for the elements obtained, we again have a relation of the form (2.1). We now renumber the a 's and b 's according to decreasing values of a_ib_i , say

$$v(a_1b_1) = \dots = v(a_hb_h) > v(a_jb_j) \quad (j > h),$$

then (2.1) states that a_1, \dots, a_h are right R -dependent (cf. [5] or [9]). Since $h \leq k \leq n < \lambda_v(R)$, any a_i ($1 \leq i \leq h$) of maximal value among a_1, \dots, a_h is R -dependent on the others, say

$$a_1 = a'_1 + \sum_2^h a_i c_i, \quad v(a'_1) < v(a_1), \quad v(a_i c_i) \leq v(a_1).$$

⁽¹⁾ Examples of rings with $\lambda(R)=\infty$ but not satisfying the weak algorithm have recently been constructed by G. M. Bergman.

Thus (2.1) may be rewritten as

$$a'_1 b_1 + \sum_2^h a_i (b_i + c_i b_1) + \sum_{h+1}^k a_j b_j = 0.$$

Clearly (a'_1, a_2, \dots, a_k) is obtained from (a_1, a_2, \dots, a_k) by elementary transformations, but

$$v(a'_1) + \sum_2^k v(a_i) < \sum_1^k v(a_i),$$

and this contradicts the minimality. Hence R is a strong GE_n -ring, as we wished to show.

As a consequence of this theorem, all the results proved in [1] for strong GE_n -rings and for n -firs apply to rings with an n -term weak algorithm, i.e., to rings with dependence number greater than n . We note in particular, the following result, part of which is contained also in [9] (Theorem 4.3):

COROLLARY. *Let R be any ring, then*

(i) *given a free R -module F , every submodule of F which can be generated by less than $\lambda(R)$ elements is free,*

(ii) *if F_n denotes the free R -module of rank n , then for $n < \lambda(R)$, the rank of F_n is uniquely determined and any set of n generators of F_n is free.*

We conclude this section by deriving a consequence of the n -term weak algorithm which is not shared by n -firs or strong GE_n -rings. A ring R is said to satisfy ACC_n in case its n -generator right ideals satisfy the ascending chain condition. If the n -generator left ideals of R satisfy the ascending chain condition we shall say that R satisfies ${}_nACC$.

THEOREM 2.4. *Let R be a ring and n an integer such that $2 \leq n < \lambda(R)$. Then R satisfies ACC_n and ${}_nACC$.*

Proof. Let v be any positive filtration of R such that $\lambda_v(R) > n$ and write

$$K = \{x \in R \mid v(x) \leq 0\}.$$

The rules for a filtration show that K is a subring of R (with the same 1). The filtration induced on K by v is trivial and the corresponding dependence number again exceeds 2. It follows that K is a (skew) field, hence every element of value zero in R is a unit.

Now take an ascending chain

$$(2.2) \quad a_1 \subseteq a_2 \subseteq \dots,$$

of right ideals a_i on at most n generators each; we have to show that (2.2) becomes stationary. By Theorem 2.3, Corollary, each a_i is free on a basis (a_{ir}) ($r=1, \dots, k_i$) of at most n elements. For each i we may take this basis to be such that

$(v(a_{i1}), \dots, v(a_{ik_i}))$ comes lowest in the lexicographic ordering. It follows that for a given i the a_{ir} are right R -independent and

$$(2.3) \quad v(a_{i1}) \leq v(a_{i2}) \leq \dots \leq v(a_{ik_i}).$$

Let us assume that for some $k \geq 1$, a_{i1}, \dots, a_{ik-1} are independent of i , and prove that the basis of each α_i can be modified so that this holds from some i onwards also for a_{ik} . For $k=0$ the conclusion is vacuous, so we may assume that $k \geq 1$ and use induction on k .

Write $c = a_{i1}R + \dots + a_{ik-1}R$, then by (2.2),

$$(2.4) \quad a_{i-1k} \equiv \sum_{r=k}^{k_i} a_{ir}c_{ir} \pmod{c},$$

and since the a_{ir} are right R -independent, we have

$$(2.5) \quad v(a_{i-1k}) = \max_{r \geq k} \{v(a_{ir}c_{ir})\}.$$

Clearly $c_{ir} \neq 0$ for some r , so by (2.3) the right-hand side of (2.5) is at least $v(a_{ik})$, i.e., $v(a_{i-1k}) \geq v(a_{ik})$. Since the $v(a_{ik})$ for varying i are nonnegative integers, they must all be equal from some i onwards, and omitting finitely many terms from (2.2) we then have

$$(2.6) \quad v(a_{i-1k}) = v(a_{ik}).$$

By (2.5), (2.6), and (2.3) we find that

$$v(a_{ir}) + v(c_{ir}) \leq v(a_{ik}) \leq v(a_{ir}) \quad (r = k, \dots, k_i).$$

This inequality shows that any a_{ir} occurring in (2.4) has value $v(a_{ik})$ and that $v(c_{ir}) \leq 0$, so each nonzero c_{ir} is a unit. We can therefore change the basis of α_i so as to include a_{i-1k} , without affecting a_{i1}, \dots, a_{ik-1} or $v(a_{ik})$. If we do this for $i=1, 2, \dots$ in turn, we obtain a basis (a_{ir}) for α_i in which a_{i1}, \dots, a_{ik} are all independent of i (from some i onwards). This completes the induction step. If we now take $k=n$, we find that from some point onwards, all terms in (2.2) have the same basis, and this proves that (2.2) becomes stationary. Hence R satisfies ACC_n and by symmetry, using Theorem 2.1 we find that R also satisfies ${}_nACC$.

The hypothesis of the theorem implies that $\lambda(R) > 2$, and this condition cannot be omitted since there are integral domains not satisfying ACC_1 . To see this we recall that an *atom* in a ring is a nonunit which cannot be written as a product of two nonunits. In [10, Proposition 4.2], it was shown that in an integral domain satisfying ACC_1 , every nonunit $\neq 0$ has an atom as left factor. Now any integral domain has dependence number greater than 1 (by Proposition 2.2), but it is easy to give examples of integral domains with elements (not 0 or units) which do not have atoms as left factors, e.g., the semigroup algebra of the additive semigroup of nonnegative rational numbers over any field. This is even a semifir.

On the other hand, when $\lambda(R) > 2$, we can assert more, namely we have

THEOREM 2.5. *Any ring R such that $\lambda(R) > 2$ is a unique factorization domain (not necessarily commutative).*

Proof. This will follow from Theorem 2.3 and the results of [1] once we have shown that R is atomic, i.e., every nonunit $\neq 0$ can be written as a product of atoms. Now R satisfies ACC_1 and ${}_1ACC$ by Theorem 2.4, and these two conditions imply atomicity. We can also prove it directly by recalling from the proof of Theorem 2.4 that any element of zero value is a unit, and observing that for any factorization $c = a_1 a_2 \cdots a_r$ of a nonunit $\neq 0$,

$$v(c) = v(a_1) + \cdots + v(a_r),$$

hence the number of nonunit factors in any factorization of c is bounded by $v(c)$. By taking a factorization of c into a maximum number of nonunit factors we can express c as a product of atoms.

3. Computation of the dependence number. In order to be able to use λ we must find a convenient means of computing it. We saw that R is better, the larger λ , so we have to look for a filtration v giving us a large λ . The case $\lambda = 1$ is trivial, by Proposition 2.2. For $\lambda > 1$, R is an integral domain and as soon as $\lambda > 2$, the units together with 0 form a field. We shall therefore lose little by assuming from the outset that R is an algebra over a commutative field K . If U is a generating set for R over K , we can express R as homomorphic image of the free K -algebra F on U : $R = F/N$. On F we define a filtration by assigning an arbitrary positive integer value $v(u)$ to each $u \in U$, putting $v(u_1 u_2 \cdots u_n) = v(u_1) + \cdots + v(u_n)$ and for general elements f of F defining

$$v(\sum \alpha_m m) = \max \{v(m) \mid \alpha_m \neq 0\},$$

where m runs over all products of u 's. Let $a \mapsto a^*$ be the given homomorphism $F \rightarrow R$, then a filtration is defined on R by writing

$$(3.2) \quad v(r) = \inf \{v(a) \mid a^* = r\}.$$

This is easily verified to be a filtration on R , depending only on the given presentation and on the values $v(u)$ of the generators.

Let us consider the form of the defining relations more closely. If one of the relations is linear,

$$\sum \alpha_i u_i + \beta = 0 \quad (\alpha_i, \beta \in K),$$

we may use it to eliminate one of the generators, because the coefficients lie in a field. We may therefore assume that there are no linear relations. A relation of higher degree can always be expressed in terms of quadratic relations, by introducing further generators if necessary. Thus every defining relation of R may be taken to be of the form

$$(3.3) \quad \Phi: \sum x_i y_i - b = 0,$$

where $x_i, y_i \in U$ and b is a linear term in the generators. The number n of terms of degree two in (3.3) is called the *rank* of the relation Φ . Our aim will be to relate the dependence number of R to the minimum of the ranks of the defining relations. More specifically we shall show in Theorem 3.1, that under suitable conditions

$$(3.4) \quad \lambda_v(R) \geq \min \text{rank} (\Phi),$$

where Φ ranges over a complete set of defining relations and v is the filtration defined in (3.2).

To find sufficient conditions for (3.4) to hold it is necessary to specify the defining relations rather more precisely. Let H, I, J be any sets (taken to be ordinals for convenience) and n a positive integer. Further let R be the K -algebra generated by a set U of elements x_{iv}, y_{vj}, z_h ($i \in I, j \in J, h \in H, v = 1, \dots, n$), where the x_{iv} are all distinct, and likewise the y_{vj} , but $\{x_{iv}\}$ need not be disjoint from $\{y_{vj}\}$ with defining relations

$$(3.5) \quad \sum x_{iv}y_{vj} = b_{ij}$$

for all pairs (i, j) in a certain subset T of $I \times J$; here b_{ij} is an expression in the x 's, y 's, and z 's of value $\leq 1 + v(y_{vj})$ and contains no term of this value beginning with any x_{iv} .

Every element of R can be written as a linear combination of products of the generators, but of course such an expression will not be unique, due to the presence of the relations (3.5). We shall say that any such expression, representing an element of R , is in *reduced form (for the suffix I)* if for any $(i, j) \in T$, no term contains a factor $x_{i1}y_{1j}$. Any element f of R can be expressed in reduced form by writing down an expression for f and then applying the moves

$$(3.6) \quad x_{i1}y_{1j} \rightarrow b_{ij} - \sum_{v \neq 1} x_{iv}y_{vj}$$

which arise from the defining relations (3.5). Under fairly mild conditions (which can easily be checked in any particular case), a reduced form is reached after a finite number of such moves, but in general there may be more than one reduced form for a given element f of R . If for each $f \in R$, there is just one reduced form we shall call it *the normal form for f* , and we shall say that a normal form for the suffix I exists. It is clear how the reduced form and the normal form for any suffix $\mu = 1, \dots, n$ may be defined, using instead of (3.6) the moves

$$x_{i\mu}y_{\mu j} \rightarrow b_{ij} - \sum_{v \neq \mu} x_{iv}y_{vj}.$$

Given $f \in R$, we shall denote the normal form for the suffix μ by $[f]_\mu$. We assume this normal form to be such that

N_μ . If fg is in normal form for μ and $v(g) > 0$, then for any $h \in R$, the terms of highest value in $f[gh]_\mu$ are in normal form for μ .

Whether this condition holds depends of course on the precise form of the defining relations and on the choice of the normal form. Examples where it is

satisfied are given later, others can be found in [2] and [9]. We now show that for any K -algebra R with defining relations (3.5) such that for $\mu = 1, \dots, n$ a normal form exists and satisfies N_μ , we have

$$(3.7) \quad \lambda(R) \geq n.$$

Of course we may assume that $n > 1$, since there is nothing to prove for $n = 1$. We shall use the filtration v on R which is defined by (3.2) in terms of the given presentation, with preassigned values for the generators such that $v(x_{i\nu}) = 1$, while $v(y_{vj})$ is independent of v .

To prove (3.7) it is enough to show that $\lambda_v(R) \geq n$. Let us write

$$H^N = \{f \in R \mid v(f) \leq N\},$$

then we must show that if $r < n$ and

$$(3.8) \quad f_1 g_1 + \dots + f_r g_r \equiv 0 \pmod{H^{N-1}}, \quad v(f_\alpha) + v(g_\alpha) = N,$$

then each g_α of maximal value is left dependent on the rest. In fact it will be enough to show that *some* g_α is left dependent on the g 's of value not exceeding $v(g_\alpha)$, for if

$$(3.9) \quad g_\alpha = \sum c_\beta g_\beta + g_\alpha^*, \quad v(g_\alpha^*) < v(g_\alpha), \quad v(c_\beta g_\beta) \leq v(g_\alpha),$$

then we can substitute from (3.9) into (3.8) and obtain a relation of the same form as (3.8) but with fewer than r terms.

In order to reduce (3.8) we shall work with the normal form for the suffix 1, and therefore write $[f]$ for $[f]_1$ in what follows. We also introduce the following notation (due to Bergman): for any $u \in U$ we denote the right cofactor of u in any element f of R by $({}^u f)$ and the left cofactor by (f^u) . Thus if e.g., $f = u^2 v + uvu$, then $({}^u f) = uv + vu$, $(f^v) = 0$, $(f^u) = uv$, $(f^v) = u^2$.

Now return to (3.8): if $v(f_\alpha) = 0$ for some α , the result is clear, so let $v(f_\alpha) > 0$ for all α . We take the terms of highest value in f_α and g_α in normal form; let

$$(3.10) \quad f_\alpha \equiv \sum u({}^u f_\alpha) \quad (u \in U),$$

be the expression of f_α in normal form (mod terms of less than the value of f_α). Inserting this expression in (3.8), we obtain a congruence which may be written as

$$(3.11) \quad \sum u[({}^u f_\alpha) g_\alpha] \equiv 0 \pmod{H^{N-1}}.$$

If $v(f_\alpha) > 1$ for all α , the left-hand side of (3.11) has all its terms of highest value in normal form, for there can be no reduction in $u[({}^u f_\alpha) g_\alpha]$ unless this was already possible in f_α , by N_1 . From the uniqueness of the normal form it now follows that the coefficient of each u in (3.11) must vanish, and going back to the original form of this coefficient, we find that

$$(3.12) \quad \sum ({}^u f_\alpha) g_\alpha \equiv 0 \pmod{H^{N-v(u)-1}}.$$

Now the result follows by induction on N .

It follows that for some α , say $\alpha=1$, $v(f_1)=1$ and $f_1 g_1$ is not in normal form (for the suffix 1). This means that for some $i \in I$, say $i=0$, f_1 contains a term x_{01} and $x_{01} g_1$ is not in normal form. Let us write

$$(3.13) \quad f_\alpha = x_{01}(x_{01}f_\alpha) + f'_\alpha$$

and

$$(3.14) \quad g_\alpha = \sum y_{1j}(y_{1j}g_\alpha) + g'_\alpha.$$

Substituting from (3.13) and (3.14) into (3.8) we obtain

$$\sum (x_{01}(x_{01}f_\alpha) + f'_\alpha) (\sum y_{1j}(y_{1j}g_\alpha) + g'_\alpha) \equiv 0 \pmod{H^{N-1}}.$$

Now reduce the terms of the first sum and equate terms of value N beginning with x_{01} . We may assume the f_α so numbered that $(x_{01}f_\alpha)$ has value 0 for $\alpha=1, \dots, s$ and positive value for $\alpha > s$. Then since

$$x_{01}y_{1j} = - \sum_{v \neq 1} x_{0v}y_{vj} + b_{0j},$$

we have

$$\begin{aligned} - \sum_{\beta=1}^s \sum_{v=2}^n \sum_j (x_{01}f_\beta)(x_{0v}y_{vj}(y_{1j}g_\beta) - b_{0j}(y_{1j}g_\beta)) + \sum_{\beta=1}^s x_{01}(x_{01}f_\beta)g'_\beta \\ + \sum_{\gamma=s+1}^r x_{01}(x_{01}f_\gamma)g_\gamma + \sum_{\alpha=1}^r f'_\alpha g_\alpha \equiv 0 \pmod{H^{N-1}}. \end{aligned}$$

Equating the cofactor of x_{01} we find

$$(3.15) \quad \sum_{\beta=1}^s (x_{01}f_\beta)g'_\beta + \sum_{\gamma=s+1}^r (x_{01}f_\gamma)g_\gamma \equiv 0 \pmod{H^{N-2}}.$$

Now by hypothesis $(x_{01}f_1)$ is a nonzero scalar λ say; write

$$(3.16) \quad g_1^* = g_1 + \lambda^{-1} \left(\sum_{\beta=2}^s (x_{01}f_\beta)g_\beta + \sum_{s+1}^r (x_{01}f_\gamma)g_\gamma \right),$$

then by (3.15), on putting $\lambda^{-1}(x_{01}f_\beta) = \mu_\beta$, $\mu_\beta(y_{1j}g_\beta) = h_{j\beta}$, we find

$$(3.17) \quad g_1^* = \sum_{\beta j} y_{1j}h_{j\beta} + \text{terms of lower value}.$$

Now (3.16) represents an elementary transformation of the g 's which does not affect g_α for $\alpha \neq 1$. Hence if $f_1 g_1$ is not in normal form (for the suffix 1), we can by an elementary transformation bring g_1 to the form g_1^* given by (3.17) without disturbing the other g 's. Since the y 's are all distinct, $f_1 g_1$ is now in normal form for any suffix $\mu \neq 1$. Next take $\mu=2$; as before there is a term $f_\alpha g_\alpha$ not in normal form for the suffix 2. By what has been said, $\alpha \neq 1$ and after suitable renumbering we may take $\alpha=2$. The same argument now shows that there is an elementary transformation bringing g_2 to the form

$$g_2^* = \sum y_{2j}h_{2j} + \text{terms of lower value},$$

without disturbing the other g 's. Thus we may suppose by induction on m that g_β is replaced by

$$(3.18) \quad g_\beta^* = \sum_j y_{\beta j} h_{\beta j} + \text{lower terms} \quad (\beta = 1, \dots, m-1);$$

then some term $f_\alpha g_\alpha$ is not in normal form for the suffix m . This means that $\alpha \neq 1, \dots, m-1$ and by renumbering the f 's and g 's we may take α to be m . As before we can bring g_m to a form g_m^* given by (3.18) (for $\beta=m$) without affecting the g_β ($\beta \neq m$). This applies for $m=1, 2, \dots, n$ and since $r < n$, we eventually reach a contradiction. So we have proved

THEOREM 3.1. *Let R be a K -algebra generated by a set U containing a family of distinct elements $(x_{i\nu})$ ($i \in I, \nu=1, \dots, n$), another family of distinct elements (y_{vj}) ($j \in J, \nu=1, \dots, n$) and possibly other elements z_h ($h \in H$). These generators are assigned positive integer values in any way such that $v(x_{i\nu})=1$ and $v(y_{vj})$ is independent of ν . Assume that R has a set of defining relations indexed by some subset T of $I \times J$:*

$$\sum x_{i\nu} y_{vj} = b_{ij},$$

where b_{ij} is an expression of value at most $1 + v(y_{vj})$ in U and has no term of this value with any $x_{i\nu}$ as left factor. Moreover, a normal form exists for each suffix μ , satisfying N_μ . Then $\lambda(R) \geq n$.

The hypotheses of the theorem, though somewhat cumbersome to state, are all quite natural ones holding in many cases, and moreover when they do hold they are usually fairly easy to verify. This is illustrated by the examples in the next section.

We observe that there is a corresponding result for the inverse dependence number of a complete filtered ring, holding under precisely analogous conditions; the main difference here is that the degree (in the free algebra) is replaced by the order, i.e. the minimum of the degrees of the nonzero terms, and the filtration (in terms of preassigned values on the generators) is defined accordingly. The detailed statement and proof may be left to the reader.

4. Applications. The main use of Theorem 3.1 is in the construction of counter-examples. It often happens that when a ring with certain pathological properties is needed, the choice of ring is quite obvious, though the conditions are rather difficult to verify. In these cases Theorem 3.1 can often be used to save calculations. E.g., a special case of Theorem 3.1 proved in [9] was used there to give a brief derivation of Leavitt's classification [12] of rings without invariant basis number. Next the inverse n -term weak algorithm was applied by A. J. Bowtell in [2] to construct a ring not embeddable in a skew field, but whose nonzero elements form a semigroup embeddable in a group (Mal'cev's problem). Another example of such a ring was given by Klein [11]: basically this is an algebra on n^2 generators x_{ij} ($n \geq 3$) and defining relations which express the fact that the $n \times n$ matrix $C=(x_{ij})$ satisfies $C^k=0$, where $k > n$. It is clear that R cannot be embedded in a

skew field (because $C^n \neq 0$), but to show that an embedding in a group exists required a lengthy calculation in [11]. Writing $C^r = (y_{ij}^{(r)})$, we can express the defining relations for R as

$$(4.1) \quad \begin{aligned} \sum y_{iv}^{(r)} y_{vj}^{(s)} &= y_{ij}^{(r+s)} & (r+s < k), \\ &= 0 & (r+s \geq k). \end{aligned}$$

If we assign values by writing $v(y_{ij}^{(r)}) = r$, it is possible to verify the conditions corresponding to Theorem 3.1 for the inverse dependence number (observe that the relations (4.1) are homogeneous); hence $\mu(R) \geq n \geq 3$. From this it follows easily (as in [2, Theorem 2.9, Corollary]) that R has an embedding in a group. We next give an example to show the independence of the conditions ACC_n ($n=1, 2, \dots$)⁽²⁾. Theorem 2.4 showed that a ring with n -term weak algorithm, where $n \geq 2$, satisfies ACC_n . The example which followed (of a semifir not satisfying ACC_1) showed that this need not hold for n -firs. On the other hand, a fir satisfies ACC_n for all n (by Proposition 4.3 of [10]) and one may ask whether in a semifir, ACC_{n-1} implies ACC_n . Certainly one would not expect this implication to hold for general rings, but even there it does not seem easy to construct a counterexample. We shall use Theorem 3.1 to construct a semifir satisfying ACC_{n-1} but not ACC_n (for any given $n \geq 2$).

To say that R satisfies ACC_n is to say that the $n \times n$ matrix ring R_n satisfies ACC_1 . Thus we require an infinite strictly ascending sequence of principal right ideals in R_n . We take R to be the K -algebra on the generators $a_{ij}^{(\nu)}, b_{ij}^{(\nu)}$ ($i, j=1, \dots, n$; $\nu=1, 2, \dots$) and defining relations

$$(4.2) \quad \sum_j a_{ij}^{(\nu)} b_{jk}^{(\nu)} = a_{ik}^{(\nu-1)} \quad (i, k = 1, \dots, n; \nu = 2, 3, \dots).$$

Let $R^{(N)}$ be the subring of R generated by the a 's and b 's with $\nu \leq N$, then $R^{(N)}$ is generated by

$$a_{ij}^{(N)}, b_{ij}^{(1)}, \dots, b_{ij}^{(N)} \quad (i, j = 1, \dots, n)$$

and is free on these generators. It follows (by [6, Theorem 4.3, Corollary 2]) that $R^{(N)}$ is a fir and since R is the union of the $R^{(N)}$, it is a semifir [6, Theorem 2.9]. Moreover, $(a_{ij}^{(N)})$ considered as $n \times n$ matrix, is not a zero-divisor in R_n but has no inverse. For if either of these properties were true they would already hold in some $R^{(M)}$ ($M \geq N$) and this is easily seen to be false. Consider now the conditions of Theorem 3.1. The fact that the reduced form in R (relative to the a 's) is actually a normal form follows easily from the fact that there is no interference in the reduction steps (cf. [7, Theorem III.9.3]). The condition N_μ is also verified without difficulty; hence $\lambda(R) \geq n$. It follows by Theorem 2.4, that for $n \geq 2$, R satisfies ACC_{n-1} , but the equations (4.2) show that R_n does not satisfy ACC_1 and so R

⁽²⁾ A similar example was found simultaneously and independently by G. M. Bergman.

does not satisfy ACC_n . Another application of Theorem 2.4 shows that $\lambda(R)$ cannot exceed n , so that in fact $\lambda(R) = n$. The result is summed up in

PROPOSITION 4.1. *For each $n > 1$, there exists a semifir R such that $\lambda(R) = n$ and so R satisfies ACC_{n-1} , but R does not satisfy ACC_n (and hence R is not a fir).*

As a further example we give a construction of a ring in which all projective modules on less than n generators are free, but there is an n -generator projective module which is not free (cf. [13]). We recall from [10] that a ring R with invariant basis number has a finitely generated projective module which is not free if and only if for some $n \geq 1$, there is an idempotent e in the $n \times n$ matrix ring R_n which is not similar to an idempotent of the form

$$e_r = \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}.$$

Fix $n \geq 1$ and let R be the K -algebra on the n^2 generators x_{ij} and relations

$$(4.3) \quad \sum_j x_{ij}x_{jk} = x_{ik}.$$

Clearly the matrix $E = (x_{ij})$ is idempotent. Moreover, the relations (4.3) are of the form (3.5). To prove the existence of the normal form we have again to check that there is no interference of reduction steps [7, Theorem III.9.3]. Such interference (relative to suffix 1) can only arise from terms like $x_{i1}x_{11}x_{1j}$. Now we have

$$\begin{aligned} x_{i1}x_{11}x_{1j} &\rightarrow x_{i1}(x_{1j} - \sum x_{1\mu}x_{\mu j}) \\ &\rightarrow x_{ij} - \sum x_{iv}x_{vj} - \sum x_{i\mu}x_{\mu j} + \sum x_{iv}x_{v\mu}x_{\mu j} \\ &= x_{ij} - 2 \sum x_{iv}x_{vj} + \sum x_{iv}x_{v\mu}x_{\mu j}, \end{aligned}$$

where all Greek suffixes are summed from 2 to n . If we perform these reduction steps in the opposite order, we clearly reach the same result; hence we have a normal form for the suffix 1, and likewise for each suffix $\mu = 2, \dots, n$. Now N_μ is verified without difficulty. Theorem 3.1 now shows that $\lambda(R) \geq n$, and so R is a strong GE_{n-1} -ring. In particular, by Theorem 2.2, Corollary, any submodule on less than n generators of a free module is free. However, as we shall now show, there is a projective module on n generators which is not free. To obtain such a module we need only find an idempotent $n \times n$ matrix over R which is not similar to e_r for any r ; the image of R^n under this idempotent will be the required module. In fact E is such an idempotent. For suppose that E is similar to e_r for some r , say

$$(4.4) \quad EA = Ae_r,$$

where $A \in GL_n(R)$. If we specialize $x_{ij} \rightarrow 0$, A goes over into a matrix \bar{A} which is again invertible and we obtain $\bar{A}e_r = 0$; hence $r = 0$. Thus (4.4) reads $EA = 0$ and it follows that $E = 0$, a contradiction. The result proved may be stated as

PROPOSITION 4.2. *For every $n \geq 1$, there exists a ring R such that any submodule on less than n generators of a free R -module is free, while there is a nonfree projective module on n generators. Moreover, for $n \geq 2$, R is an integral domain, and for $n \geq 3$, R is a unique factorization domain.*

The last part follows by Theorem 2.3, Corollary and Theorem 2.5.

REFERENCES

1. G. M. Bergman and P. M. Cohn, *Dependence in rings I: n -firs*, (to appear).
2. A. J. Bowtell, *On a question of Mal'cev*, *J. Algebra* **6** (1967), 126–139.
3. P. M. Cohn, *On a generalization of the Euclidean algorithm*, *Proc. Cambridge Philos. Soc.* **57** (1961), 18–30.
4. ———, *Factorization in non-commutative power series rings*, *Proc. Cambridge Philos. Soc.* **58** (1962), 452–464.
5. ———, *Rings with a weak algorithm*, *Trans. Amer. Math. Soc.* **109** (1963), 332–356.
6. ———, *Free ideal rings*, *J. Algebra* **1** (1964), 47–69.
7. ———, *Universal algebra*, Harper and Row, New York, 1965.
8. ———, *On the structure of the GL_2 of a ring*, *Publ. Math. Inst. Hautes Etudes Sci.*, No. 30, Paris, 1966, pp. 5–53.
9. ———, *Some remarks on the invariant basis property*, *Topology* **5** (1966), 215–228.
10. ———, *Torsion modules over free ideal rings*, *Proc. London Math. Soc.* (3) **17** (1967), 577–599.
11. A. A. Klein, *Rings nonembeddable in fields with multiplicative semigroups embeddable in groups*, *J. Algebra* **6** (1967), 101–125.
12. W. G. Leavitt, *The module type of a ring*, *Trans. Amer. Math. Soc.* **103** (1960), 113–130.
13. M. Raynaud, *Solution d'un problème universel relatif aux modules projectifs de type fini*, *C. R. Acad. Sci. Paris* **260** (1965), 4391–4394.

UNIVERSITY OF LONDON,
LONDON, ENGLAND
RUTGERS, THE STATE UNIVERSITY,
NEW BRUNSWICK, NEW JERSEY