

JOURNAL OF ALGEBRA I, 47-69 (1964)

## Free Ideal Rings

P. M. COHN

*Queen Mary College, University of London, London*

Received December 5, 1963

### I. INTRODUCTION

The Euclidean algorithm forms a convenient tool for deriving certain properties of commutative rings such as the unique factorization property or the elementary divisor theorem, but owing to the different forms which the norm function used for the algorithm can take, the class of rings to which it applies is not very clearly defined and from a theoretical point of view it is more satisfactory to establish these properties directly for the wider class of principal ideal domains. Now there is an analogue of the Euclidean algorithm for certain noncommutative rings; in particular, such a "weak" algorithm exists in free associative algebras over a field [5] and in free products of skew fields [4, 8]. Again the weak algorithm takes different forms in these rings (owing to the different ways of defining the norm function), but in each case it can be shown that in a ring with a weak algorithm all right ideals are free, as modules over the ring. The parallel with commutative rings suggests the problem of finding a class of rings which (i) includes the rings with a weak algorithm, (ii) reduces to principal ideal domains in the commutative case and which also has most of the properties derived by means of the weak algorithm.

An obvious solution is to take the class of rings in which all right ideals are free modules. An integral domain satisfying this condition and a further condition given in Section 2, is called a *free ideal ring*, or *fir*, for short. For some purposes it is more convenient to consider *locally free ideal rings* (*local firs*), in which only the finitely generated right ideals need be free. This class generalizes firs, while it is included in the class of weak Bezout rings defined in [7]. In all we have the following table, in which the left-hand column represents the commutative case and any move upwards (or to the right) leads to a wider class:

Bezout rings	locally free ideal rings
principal ideal domains	free ideal rings
Euclidean domains	rings with a weak algorithm

The main result proved here (Theorem 4.2) gives certain sufficient conditions under which the free product of a family of local firs exists and is again a local fir. These conditions show in particular that *the free product of any family of local firs (over a skew field) is again a local fir.*

A corresponding result, with an additional condition, is shown to hold for firs, and this leads to generalizations of theorems in refs. 4, 5 and 8. Since every principal ideal domain (commutative or not) is a fir, we find in particular that firs include (a) free products of fields<sup>1</sup> (over a given field), (b) free associative algebras over a commutative field, and (c) the group algebra of a free group over a commutative field. Case (a) was proved in ref. 4, while part of (b) was essentially treated in ref. 5; case (c) is believed to be new and it improves the known result, that the group algebra of a free group over a commutative field is hereditary (cf. Cartan-Eilenberg [2, chap. X. 5-6] and M. Auslander [1]).

The proof of the above results occupies Section 4. The exact definition and basic properties of firs and local firs are given in Section 2; besides, this section contains some results on the structure of finitely generated modules over (local) firs. It turns out that with each such module  $M$  an invariant  $r(M)$ , the *rank* of  $M$ , can be associated; this is  $-\infty$  if and only if  $M$  cannot be finitely defined; otherwise it is an integer (positive, negative or zero) which is essentially the excess of the number of generators over the number of independent defining relations in these generators. The proof of the main theorem uses an existence theorem for free products of associative rings which may be of independent interest. A ring  $R$  is said to be an *augmented  $K$ -ring* if  $K$  is a subring of  $R$  which is also a direct summand of  $R$ , as right  $K$ -module. With this definition we have the following theorem:

*If  $K$  is any ring, then the free product of any family of augmented  $K$ -rings, taken over  $K$ , exists.*

This overlaps (but is not included in) the results of ref. 3. In particular it leads to a shorter proof of the existence of free products over a field.

In conclusion we remark that the conjecture that every free product of fields is embeddable in a field [4] may now be replaced by the more general conjecture that every local fir is embeddable in a field. This may possibly be easier to verify than the original conjecture, since it allows an induction hypothesis to be made.

---

<sup>1</sup> We shall use the term "field" throughout in the sense of an associative but not necessarily commutative division ring. To stress this fact we occasionally use the prefix "skew."

## 2. MODULES OVER FIRS AND LOCAL FIRS

Throughout, all rings are understood to be associative, with a unit element, denoted by 1, which acts as identity on all modules. Moreover, a subring of a ring  $R$  is understood to contain the 1 of  $R$ . If  $M$  is any right  $R$ -module, then a subset  $X$  of  $M$  is  $R$ -independent, if the only relation

$$\sum x_i a_i = 0 \quad (x_i \in X, a_i \in R)$$

between different elements of  $X$  is the trivial one in which  $a_i = 0$  ( $i = 1, \dots, n$ ). Thus  $M$  has an independent generating set (also called a *basis*) if and only if it is a free  $R$ -module. Different bases of a free  $R$ -module need not contain the same number of elements (cf. Leavitt [11] for counter examples), but in any case, if  $M$  has an infinite basis, then all bases of  $M$  are infinite of the same cardinal [9]. We shall say that  $R$  is a ring with *invariant basis number* if all bases of a free  $R$ -module  $M$  have the same number of elements. This number is then called the *rank* of  $M$  and is denoted by  $r(M)$ . Thus the rank is only defined for free modules, but we shall see later how to extend it in certain cases.

DEFINITION 1. A *free ideal ring (fir)* is an integral domain  $R$  with invariant basis number, such that all right ideals of  $R$  are free  $R$ -modules.

It is not known whether an integral domain, in which all right ideals are free, necessarily has an invariant basis number. Thus the definition may be redundant, but essential use is made of the invariance of the basis number, and it may be noted in passing that any ring embeddable in a field must have invariant basis number.

Strictly speaking, the above definition refers to a right fir; a left fir is then a ring  $R$  whose opposite ring  $R^0$  is a right fir. Again it is not known whether every left fir is a right fir, but this seems likely to be true. In any case the symmetry will be established for the class of local firs to which we now turn.

DEFINITION 2. A *locally free ideal ring (local fir)* is an integral domain  $R$  with invariant basis number, in which all finitely generated right ideals are free.

A module is said to be *locally free* if all its finitely generated submodules are free. We note that a free module need not be locally free; a criterion for this to happen is given by

PROPOSITION 2.1. *Let  $R$  be any ring, then the free  $R$ -modules are locally free if and only if  $R$  is locally free, as right  $R$ -module.*

*Proof.* If all  $R$ -modules are locally free then  $R$  itself, being free, is also locally free. Conversely, assume that  $R$  is locally free, let  $F$  be a free  $R$ -module and  $N$  a finitely generated submodule of  $F$ . A finite generating set of  $N$  involves only finitely many generators from a basis of  $F$ , and we may map the remaining basis elements to zero without affecting  $N$ . Thus  $F$  may be taken to be finitely generated, by a set of  $r$  elements, say; we shall use induction on  $r$ . The submodule  $F'$  of  $F$  generated by the first  $r - 1$  elements of the given basis is free on  $r - 1$  free generators and is such that  $F/F' \cong R$ . Writing  $N' = N \cap F'$ , we have

$$\frac{N}{N'} \cong \frac{N + F'}{F'} \subseteq \frac{F}{F'}.$$

Since  $N$  is finitely generated, so is  $N/N'$  and hence  $(N + F')/F'$  is a finitely generated submodule of  $F/F'$ ; the submodules of  $F/F' \cong R$  are just the right ideals; therefore  $N/N'$  is free and we have

$$N = N' \oplus N'', \quad (1)$$

where  $N''$  is a free submodule of  $N$ . Now  $N' \cong N/N''$  is again finitely generated, and is a submodule of  $F'$ . By the induction hypothesis  $N'$  is free and hence by (1),  $N$  is free, as we wished to show.

It follows in particular that over a local fir, all free modules are locally free. Over a fir it can be shown more generally that every submodule of a free module is free. This follows, e.g., from Theorem 1.5.3 in ref. 2.

In any ring with invariant basis number, any free module  $F$  has a rank  $r(F)$ ; consider now a local fir  $R$ , and any finitely generated  $R$ -module  $M$ , say

$$M \cong F/N,$$

where  $F$  is free of finite rank. If  $N$  is finitely generated, it is also free, by Prop. 2.1, and we may put

$$r(M) = r(F) - r(N). \quad (2)$$

If  $N$  is not finitely generated we put  $r(M) = -\infty$ . If we have another presentation of  $M$ , say

$$M \cong F'/N',$$

where  $F'$  is again free of finite rank, then by Schanuel's theorem [12, p. 101]

$$F \oplus N' \cong F' \oplus N,$$

hence  $N'$  is finitely generated if and only if  $N$  is finitely generated, and when this is the case, then

$$r(F) - r(N) = r(F') - r(N').$$

This shows that for any module  $M$  which has a finite presentation, the number  $r(M)$  defined in (2) is finite and is independent of the presentation chosen, while for a module which can be finitely generated but not finitely presented,  $r(M)$  is necessarily  $-\infty$ . We call  $r(M)$  the *rank* of  $M$  and note that for free modules this agrees with the rank as previously defined. We also note the following immediate consequence of the definitions.

PROPOSITION 2.2. *Let  $M$  be any module over a local fir. If  $M$  has a finite generating set  $X$  of  $n$  elements, then*

$$r(M) \leq n,$$

*with equality if and only if  $M$  is free on  $X$ .*

All that has been said applies in particular to modules over a fir. We note however, that even over a fir  $R$ , submodules of finitely generated modules need not be finitely generated. They are so if and only if  $R$  is right Noetherian; for completeness we note the following characterization of Noetherian firs.

THEOREM 2.3. *For any fir  $R$  the following conditions are equivalent:*

- (i)  $R$  is a principal right ideal domain,
- (ii)  $R$  is right Noetherian,
- (iii)  $R$  satisfies the right multiple condition of Ore:

$$aR \cap bR \neq 0 \quad \text{for any} \quad a, b \in R, a, b \neq 0. \tag{3}$$

*Proof.* Clearly (i) implies (ii) in any ring, and Goldie has shown that for integral domains (ii)  $\Rightarrow$  (iii) (10) (cf. also ref. 6). Now assume (iii) and let  $\mathfrak{a}$  be any right ideal of  $R$ . Given  $a, b \in \mathfrak{a}$ ,  $a, b \neq 0$ , there exist  $a', b' \in R$  such that

$$ab' = ba' \neq 0 \tag{4}$$

by (3). But by hypothesis  $\mathfrak{a}$  is free; now (4) shows that no basis of  $\mathfrak{a}$  can contain more than one element, hence  $r(\mathfrak{a}) \leq 1$  and this means that  $\mathfrak{a}$  is principal. Thus  $R$  is a principal right ideal domain, i.e. (i) holds.

Since (3) holds trivially in any commutative integral domain, we have the

COROLLARY. *A commutative ring is a fir if and only if it is a principal ideal domain.*

Theorem 2.3 shows that over a local fir (or even a fir) which is not a principal ideal domain, neither submodules nor quotients of a finitely presented module  $M$  need be finitely presented; to obtain examples we need only take  $M = R$ . On the other hand, when  $M$  has a submodule  $M'$  such that both  $M'$  and  $M/M'$  are finitely presented, then so is  $M$ , by the following

PROPOSITION 2.4. *Given an exact sequence*

$$0 \rightarrow M' \rightarrow M \rightarrow M'' \rightarrow 0 \quad (5)$$

*of modules over a local fir, if  $M'$  and  $M''$  are finitely generated, then so is  $M$ , and*

$$r(M) = r(M') + r(M''). \quad (6)$$

*In particular it follows from (6) that under the given conditions,  $M$  is finitely presented if and only if both  $M'$  and  $M''$  are.*

*Proof.* Take resolutions of  $M'$ ,  $M''$  using finitely generated free modules  $F'$ ,  $F''$  and complete them to a commutative diagram

$$\begin{array}{ccccccc} & 0 & 0 & 0 & & & \\ & \downarrow & \downarrow & \downarrow & & & \\ 0 & \rightarrow & N' & \rightarrow & N & \rightarrow & N'' \rightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \rightarrow & F' & \rightarrow & F & \rightarrow & F'' \rightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \rightarrow & M' & \rightarrow & M & \rightarrow & M'' \rightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ & & 0 & & 0 & & 0 \end{array} \quad (7)$$

with exact rows and columns, where  $F = F' \oplus F''$  and hence

$$r(F) = r(F') + r(F'') \quad (8)$$

(cf. ref. 2, Prop. 1.2.5). Now assume that  $N'$  and  $N''$  are finitely generated, then in particular  $N''$  is free (Prop. 2.1), so the top row splits and  $N$  is also finitely generated free, and further

$$r(N) = r(N') + r(N''); \quad (9)$$

now (6) follows by subtracting (9) from (8). If  $N$  is finitely generated then so is  $N''$ , again it follows that  $N''$  is free, the top row splits and  $N'$  is also finitely generated (as homomorphic image of  $N$ ), so that this case has been

reduced to the previous one. The only remaining possibility is that  $N$  and at least one of  $N'$ ,  $N''$  cannot be finitely generated. Then  $r(M)$  and one (at least) of  $r(M')$ ,  $r(M'')$  are  $-\infty$ , and so (6) still holds in this case. This completes the proof.

In order to establish the left-right symmetry of the definition of a local fir we need to examine the different bases in a free module more closely. We recall that a square matrix over a ring  $R$  is said to be *unimodular*, if it has a (two-sided) inverse over  $R$ .

LEMMA 2.5. *Let  $F$  be a free module over a local fir  $R$ , with a basis  $v_1, \dots, v_r$ , and let  $u_1, \dots, u_n$  be a finite generating set of  $F$  (not necessarily a basis). Then  $n \geq r$  and there is a unimodular matrix  $P$  over  $R$  such that*

$$(u_1, \dots, u_n) P = (v_1, \dots, v_r, 0, \dots, 0). \tag{10}$$

*Proof.* By Prop. 2.2,  $r \leq n$ ; we shall use latin indices  $i, j, k$  for the range 1 to  $n$  and the greek indices  $\rho, \sigma$  for the ranges 1 to  $r$  and  $r + 1$  to  $n$  respectively. Since the  $u_i$  and the  $v_\rho$  are two generating sets of  $F$ , there exist  $p_{i\rho}, \hat{p}_{\rho i} \in R$  such that

$$v_\rho = \sum u_i p_{i\rho}, \tag{11}$$

$$u_i = \sum v_\rho \hat{p}_{\rho i}. \tag{12}$$

Write  $s = n - r$ , then the presentation of  $F$  in terms of the  $u_i$  has  $s$  independent defining relations, i.e., there exists  $n$ -tuples  $a_{i\sigma}$ , which are right  $R$ -independent, such that

$$\sum u_i a_{i\sigma} = 0, \tag{13}$$

and in every relation between the  $u_i$  the coefficients are linear combinations of the  $a_{i\sigma}$ . By (11) and (12),

$$u_j = \sum v_\rho \hat{p}_{\rho j} = \sum u_i p_{i\rho} \hat{p}_{\rho j},$$

i.e.,

$$u_i \left( \sum p_{i\rho} \hat{p}_{\rho j} - \delta_{ij} \right) = 0;$$

hence by (13), there exist elements  $b_{\sigma j} \in R$  such that

$$\sum p_{i\rho} \hat{p}_{\rho j} - \delta_{ij} = \sum a_{i\sigma} b_{\sigma j}. \tag{14}$$

If we put  $p_{i\sigma} = a_{i\sigma}$ ,  $\hat{p}_{\sigma j} = -b_{\sigma j}$ , then (14) may be written as

$$\sum_k p_{ik} \hat{p}_{kj} = \delta_{ij},$$

or, putting  $P = (p_{ij})$ ,  $\hat{P} = (\hat{p}_{ij})$ ,

$$P\hat{P} = I. \tag{15}$$

Hence  $P(\hat{P}P - I) = 0$  and it will follow that  $\hat{P}P = I$  if we can show that  $P$  is not a left zero-divisor. Thus assume that  $\sum p_{ij}c_j = 0$ , i.e.

$$\sum p_{i\rho}c_\rho + \sum a_{i\sigma}c_\sigma = 0. \tag{16}$$

Applying this relation to  $u_i$  and summing over  $i$  we obtain

$$\sum u_i p_{i\rho}c_\rho + \sum u_i a_{i\sigma}c_\sigma = 0,$$

i.e., by (11) and (13),

$$\sum v_\rho c_\rho = 0.$$

Since the  $v_\rho$  are  $R$ -independent, we have  $c_\rho = 0$  and (16) reduces to

$$\sum a_{i\sigma}c_\sigma = 0.$$

But the  $n$ -tuples  $a_{i\sigma}$  are also  $R$ -independent, hence  $c_\sigma = 0$  and so  $c_i = 0$  for  $i = 1, \dots, n$ . This shows that  $P$  is not a left zero-divisor, whence  $\hat{P}P = I$ , and together with (15) this states that  $P$  is unimodular. Moreover, by (11) and (13),

$$\sum u_i \hat{p}_{ij} = \begin{cases} v_\rho & \text{if } j = \rho \leq r, \\ 0 & \text{if } j = \sigma > r. \end{cases}$$

Thus  $(u_1, \dots, u_n)P = (v_1, \dots, v_r, 0, \dots, 0)$ , as we wished to show.

This lemma leads to a useful characterization of local firs:

**THEOREM 2.6.** *For any ring  $R$ , the following three conditions are equivalent:*

- (i)  $R$  is a local fir,
- (ii) given any elements  $a_1, \dots, a_n, b_1, \dots, b_n \in R$  such that

$$\sum a_i b_i = 0 \quad (b_i \text{ not all zero}), \tag{17}$$

there exists a unimodular matrix  $P = (p_{ij})$  such that  $\sum a_i p_{ij} = 0$  for at least one index  $j$ ,

- (iii) given  $a_1, \dots, a_n, b_1, \dots, b_n \in R$  such that

$$\sum a_i b_i = 0 \quad (a_i \text{ not all zero}), \tag{18}$$

there exists a unimodular matrix  $P = (p_{ij})$  such that  $\sum p_{ij} b_j = 0$  for at least one index  $i$ .



*Proof.* (i)  $\Rightarrow$  (ii). Given  $2n$  elements  $a_i, b_i$  satisfying (17), let  $\mathfrak{a}$  be the right ideal of  $R$  generated by the  $a_i$ , then  $\mathfrak{a}$  is free, and hence by Lemma 2.5, there is a unimodular matrix  $P = (p_{ij})$  which transforms the  $a_i$  into a basis of  $\mathfrak{a}$ , followed by zeros. Now (17) is a nontrivial relation between the  $a_i$ , therefore  $r(\mathfrak{a}) < n$  and at least one zero must occur, i.e.,  $\sum a_i p_{in} = 0$ .

(ii)  $\Rightarrow$  (iii). Given  $2n$  elements  $a_i, b_i$  satisfying (18), we may assume that none of the  $b_i$  vanishes (since otherwise the conclusion follows trivially) and use induction on  $n$ . By (ii) there is a unimodular matrix  $Q = (q_{ij})$  such that  $\sum a_i q_{ij} = 0$  for some  $j$ , say  $j = n$ . Put  $a'_j = \sum a_i q_{ij}$ ,  $b'_i = \sum q_{ij} b_j$ , where  $(q_{ij}) = Q^{-1}$ , then the  $a'_j$  do not all vanish and

$$\sum_1^{n-1} a'_\alpha b'_\alpha = 0;$$

by induction there exists a unimodular  $(n - 1) \times (n - 1)$  matrix  $S = (s_{\alpha\beta})$  such that  $\sum s_{\alpha\beta} b'_\beta = 0$  for some  $\alpha = 1, \dots, n - 1$ . Now

$$P = \begin{pmatrix} S & 0 \\ 0 & 1 \end{pmatrix} Q^{-1}$$

is a matrix with the required properties.

(iii)  $\Rightarrow$  (i). Let  $ab = 0, a \neq 0$ , then by (iii) for  $n = 1$ , there exists a unit  $u$  in  $R$  such that  $ub = 0$ ; hence  $b = 0$  and it follows that  $R$  is an integral domain. Next we show that  $R$  is locally free (as  $R$ -module); let  $\mathfrak{a}$  be a right ideal of  $R$  with a finite generating set  $a_1, \dots, a_n$  ( $n \geq 0$ ). We may assume without loss of generality, that  $a_i \neq 0$  ( $i = 1, \dots, n$ ) and we shall show by induction on  $n$ , that either  $\mathfrak{a}$  is free on  $a_1, \dots, a_n$  or  $\mathfrak{a}$  is free on fewer than  $n$  free generators. For  $n = 0$  this holds trivially, so let  $n > 0$ . If the  $a_i$  do not form a basis of  $\mathfrak{a}$ , then there is a relation  $\sum a_i b_i = 0$  in which the  $b_i$  are not all zero. Now the  $a_i$  are not all zero, so there is a unimodular matrix  $P = (p_{ij})$  such that  $\sum p_{ij} b_j = 0$  for some  $i$ , say  $i = 1$ . Write  $P^{-1} = (\hat{p}_{ij})$ ,  $a'_j = \sum a_i \hat{p}_{ij}$ ,  $b'_i = \sum p_{ij} b_j$ , then the elements  $a'_1, \dots, a'_n$  again generate  $\mathfrak{a}$  and since  $b'_1 = 0$ ,

$$\sum_2^n a'_i b'_i = \sum_1^n a'_i b'_i = 0. \tag{19}$$

Consider the ideal  $\mathfrak{c}$  say, generated by  $a'_2, \dots, a'_n$ . Since the  $b_i$  are not all zero, neither are the  $b'_i$  and (19) shows that  $a'_2, \dots, a'_n$  are  $R$ -dependent. By the induction hypothesis,  $\mathfrak{c}$  is free, with a basis  $c_1, \dots, c_r$  say, where  $r < n - 1$ . Now the elements  $a_1, c_1, \dots, c_r$  generate  $\mathfrak{a}$ ; noting that  $r + 1 < n$  and applying the induction hypothesis once more we conclude that either  $\mathfrak{a}$  is free on  $a_1, c_1, \dots, c_r$  or  $\mathfrak{a}$  is free on fewer than  $r + 1$  elements.

To show that  $R$  is a local fir it now only remains to verify that  $R$  has invariant basis number. If there exists a free right  $R$ -module with bases of  $m$  and  $n$  elements respectively, where  $m \neq n$ , then  $m$  and  $n$  are finite, by the remark at the beginning of this section, and the matrices of transformation between these bases are an  $m \times n$  matrix  $P$  and an  $n \times m$  matrix  $Q$  such that

$$PQ = I_m, \quad QP = I_n. \quad (20)$$

Conversely, a pair of matrices  $P, Q$  satisfying (20) leads to a free  $R$ -module with bases of  $m$  and  $n$  elements respectively. Thus we have to show that (20) with  $m \neq n$  is impossible. Let us assume then that (20) holds, with  $m < n$  say, and use induction on  $m$ . Since  $R$  is an integral domain, (20) cannot hold with  $m = 1$  (and  $m < n$ ), so we may take  $m > 1$ . Now the second equation (20) shows that if  $P = (p_{i\alpha}), Q = (q_{\alpha i})$ , then

$$\sum q_{\alpha i} p_{i1} = 0 \quad (\alpha \neq 1). \quad (21)$$

Since the  $q_{\alpha i}$  are not all zero, there exists a unimodular  $m \times m$  matrix  $C = (c_{ij})$  such that at least one of  $p'_{i1} = \sum c_{ij} p_{j1}$  is zero. Choose  $C$  such that the number of nonzero  $p'_{i1}$  is minimal; then the nonzero  $p'_{i1}$  are left  $R$ -independent, for if  $p'_{i1}$  is nonzero for  $i \leq r$  and zero for  $i > r$ , say, then any nontrivial relation

$$\sum a_i p'_{i1} = 0 \quad (a_i \in R \text{ not all zero})$$

would allow us to reduce the number of nonzero  $p'_{i1}$  by a unimodular transformation, applied to  $p'_{11}, \dots, p'_{r1}$ . Now write  $C^{-1} = (\epsilon_{ij}), q'_{\alpha i} = \sum q_{\alpha j} \epsilon_{ji}$ , then by (21),

$$\sum q'_{\alpha i} p'_{i1} = 0, \quad (\alpha \neq 1),$$

and by the independence of  $p'_{11}, \dots, p'_{r1}$  this means that  $q'_{\alpha i} = 0$  for  $\alpha > 1$  and  $i \leq r$ . Thus if we replace  $P, Q$  by  $P' = CP, Q' = QC^{-1}$  respectively, the relations (20) still hold, while  $q'_{\alpha 1} = 0$  for  $\alpha \neq 1$ . From the first relation (20) it now follows that the first column of  $P'$  consists of a nonzero element (in fact a unit) followed by zeros. Dropping the dashes from  $P', Q'$ , we thus have

$$P = \begin{pmatrix} p_{11} & p_{12} & \cdots & p_{1n} \\ 0 & & & \\ \vdots & & P_1 & \\ \vdots & & & \\ 0 & & & \end{pmatrix} \quad Q = \begin{pmatrix} q_{11} & q_{12} & \cdots & q_{1m} \\ 0 & & & \\ \vdots & & Q_1 & \\ \vdots & & & \\ 0 & & & \end{pmatrix}$$

Here  $P_1$  is an  $(m - 1) \times (n - 1)$  matrix and  $Q_1$  an  $(n - 1) \times (m - 1)$  matrix and since  $P, Q$  satisfy (20), so do  $P_1, Q_1$ . But this contradicts the induction hypothesis, therefore (20) with  $m \neq n$  is impossible, as we wished to show.

From the symmetry of the conditions (ii) and (iii) we derive the

**COROLLARY.** *A ring  $R$  is a local fir if and only if its opposite,  $R^0$  is a local fir.*

If  $M$  is a right  $R$ -module then its dual  $M^*$  is defined by the equation  $M^* = \text{Hom}(M, R)$ ; this is a left  $R$ -module in a natural way (cf., e.g., ref. 2, chap. II), i.e., a right module over the opposite ring  $R^0$ . When  $R$  is a local fir and  $M$  finitely generated,  $M^*$  is described by

**PROPOSITION 2.7.** *Let  $M$  be a finitely generated  $R$ -module, where  $R$  is a local fir, and let  $k$  be the maximal rank of a free direct summand of  $M$ :*

$$M = M_1 \oplus R^k, \tag{22}$$

where  $M_1$  does not have  $R$  as direct summand (and  $k \geq 0$ ). Then the dual of  $M$  is

$$M^* = R^k \quad (\text{as left } R\text{-module}). \tag{23}$$

For we have, by (22),

$$\text{Hom}(M, R) \cong \text{Hom}(M_1, R) \oplus \text{Hom}(R^k, R).$$

Here the first summand on the right is zero, for any homomorphism  $M_1 \rightarrow R$  has as image a finitely generated right ideal of  $R$ , which must be free, and therefore lifts to a direct summand of  $M_1$ . By hypothesis  $M_1$  has no free direct summand of rank greater than zero, so  $\text{Hom}(M_1, R) = 0$ . Further,  $\text{Hom}(R^k, R) \cong R^k$  and this establishes (23).

From this Proposition it follows that if  $M$  is a finitely presented  $R$ -module, with the resolution

$$0 \rightarrow R^m \rightarrow R^n \rightarrow M \rightarrow 0$$

then the exact cohomology sequence gives

$$0 \rightarrow M^* \rightarrow R^n \rightarrow R^m \rightarrow \text{Ext}^1(M, R) \rightarrow 0,$$

therefore

$$r(\text{Ext}^1(M, R)) = r(M^*) - r(M). \tag{24}$$

In particular this shows that as left  $R$ -module  $\text{Ext}^1(M, R)$  is again finitely presented.

We now consider the differences between firs and local firs in more detail. For this purpose we recall the following definition from ref. 7: A *weak Besout*

ring is an integral domain in which any two principal right ideals with a nonzero intersection have a sum and intersection which are again principal. In ref. 7 it was shown in effect that every fir is a weak Bezout ring (Theorem 6.2). The same proof shows actually that every local fir is a weak Bezout ring. Further, it was shown [7, Theorem 5.5, Cor. 1] that a weak Bezout ring is a unique factorization domain if and only if every nonunit  $\neq 0$  in  $R$  has a prime factorization. Thus to show that firs are unique factorization domains we have to prove the existence of prime factorizations. Whether this holds we do not know but we can establish it for rings which are left as well as right firs.

**THEOREM 2.8.** *If both  $R$  and its opposite are firs then  $R$  is a unique factorization domain.*

*Proof.* We first show that there is no infinite strictly ascending chain of principal right ideals

$$a_1R \subset a_2R \subset \cdots . \quad (25)$$

For, given such a chain, let  $(c_i)$  be a basis for the right ideal generated by  $a_1, a_2, \dots$ , then  $c_1 = \sum_1^n a_i u_i = a_n u$ , for a suitable  $u \in R$ , because  $a_1, \dots, a_n \in a_n R$ . We may assume that  $u$  is not a unit, increasing  $n$  by 1, if necessary. Now  $a_n = \sum c_i v_i$ , hence

$$c_1 = a_n u = \sum c_i v_i u .$$

Since the  $c_i$  are right  $R$ -independent,  $v_1 u = 1$ , and hence  $u v_1 = 1$ , because  $R$  is an integral domain. But this contradicts the fact that  $u$  is not a unit, hence no chain (25) exists. By symmetry it follows that no strictly ascending chain of principal left ideals exists, either. Now let  $a \in R$  be any nonunit ( $\neq 0$ ), then either  $a$  is prime or we can write  $a = b_1 c_1$ , where  $b_1, c_1$  are nonunits. If  $c_1$  is not prime, then  $c_1 = b_2 c_2$ , where  $b_2, c_2$  are nonunits; continuing in this way, we obtain an ascending chain of principal left ideals

$$Ra \subset Rc_1 \subset Rc_2 \subset \cdots ,$$

which must terminate, by what we have shown. This can only happen if  $c_n$  is prime for some  $n$ , and then  $a = b_1 b_2 \cdots b_n c_n$ ; in all we have proved that every nonunit  $\neq 0$  has a right factor which is prime. Thus every given nonunit  $a \neq 0$  is either prime or it can be written  $a = b_1 p_1$ , where  $p_1$  is prime.

If  $b_1$  is not a unit we have likewise  $b_1 = b_2 p_2$ , where  $p_2$  is prime, and continuing in this way, we obtain an ascending chain of principal right ideals  $aR \subset b_1 R \subset b_2 R \subset \cdots$  which again breaks off. This means that  $b_n$  is prime for some  $n$ , and so we obtain a prime factorization of  $a$ . Now the theorem follows from the results quoted from ref. 7.

In order to obtain examples of local firs which are not firs we first note a property of local firs:

**THEOREM 2.9.** *The property of being a local fir is of local character.*

This means that if a ring  $R$  has a directed family of subrings whose union is  $R$  and which are local firs (i.e.,  $R$  has a *local system* of subrings which are local firs), then  $R$  is itself a local fir. We remark that here it is material that a subring of  $R$  has the same unit element as  $R$ .

*Proof.* Let  $(R_\lambda)$  be a local system of subrings of  $R$  which are local firs; we have to show that  $R$  is a local fir. Given any relation  $\sum a_i b_i = 0$  in  $R$  in which the  $b_i$  are not all zero, we can choose a ring  $R_\lambda$  of the given system to contain all the  $a_i$  and  $b_i$ ; by Theorem 2.6, there exists then a unimodular matrix in  $R_\lambda$  which transforms the  $a_i$  to a set including zero, and hence, by another application of Theorem 2.6,  $R$  is a local fir.

Now let  $R$  be any fir, e.g., a free associative algebra over a field (cf. Section 4). By adjoining successive square roots of the generators of  $R$  we obtain a ring which is again a local fir, by Theorem 2.9, but it does not admit prime factorizations for all its nonunits; if it were a fir, then by the symmetry of the construction, its opposite would also be a fir, and it would be a unique factorization domain. This contradiction shows that it cannot be a fir.

### 3. THE FREE PRODUCT OF AUGMENTED RINGS

In order to show that the free product of firs is a fir we need a result on the existence of free products, which is derived in this section. Although the actual application to be made is also covered by the theorem in ref. 3, the approach used here is rather more direct and also introduces the concepts used in Section 4. We shall use the following criterion for the existence of free products established in [3, Theorem 3.4]:

*Let  $(R_\lambda)$  be a family of rings containing a common subring  $K$ . If there exists a right  $K$ -module  $V$  such that for each  $\lambda$ ,  $V$  is a right  $R_\lambda$ -module containing  $R_\lambda$  as submodule in such a way that  $R_\kappa \cap R_\lambda = K$  for  $\kappa \neq \lambda$ , then the free product of the  $R_\lambda$  over  $K$  exists.*

We recall from ref. 3 that a  $K$ -ring is essentially a ring  $R$  with a canonical homomorphism  $\theta : K \rightarrow R$ . We shall only be dealing with the case of a *strict*  $K$ -ring, i.e., the case where  $\theta$  is injective. In this case  $K$  is embedded in  $R$  and no confusion will arise if we denote the unit elements of  $K$  and  $R$  by the same symbol  $1$ . From the definition, any  $K$ -ring is a  $K$ -bimodule; now we define a  $K$ -ring to be *augmented* if there is a homomorphism of right  $K$ -modules

$$\epsilon : R \rightarrow K$$

such that  $\theta\epsilon = 1$ . Clearly this is equivalent to the condition that  $K$  be a direct summand of  $R$ , as right  $K$ -module:

$$R = K \oplus N, \quad (26)$$

where  $N = \ker \epsilon$  is called the *augmentation module*. In particular this shows that an augmented  $K$ -ring is necessarily strict. We remark that since both  $R$  and  $K$  are  $K$ -bimodules,  $N$  also has a bimodule structure, obtained from that of  $R/K$  by means of the isomorphism of right  $K$ -modules

$$N \cong R/K.$$

Here  $K$  acts on  $N$  from the right by right multiplication, while the action from the left may be described explicitly as follows: If  $\alpha \in K$ ,  $x \in N$  and  $\alpha x = \alpha_1 + x_1$  is the splitting according to (26) ( $\alpha_1 \in K$ ,  $x_1 \in N$ ), then the effect of  $\alpha$  on  $x$  is  $x_1$ .

**THEOREM 3.1.** *Let  $K$  be any ring, then the free product of any family  $(R_\lambda)$  of augmented  $K$ -rings exists (over  $K$ ) and is again an augmented  $K$ -ring.*

*Proof.* Each ring  $R_\lambda$  has a canonical decomposition (26):

$$R_\lambda = K \oplus N_\lambda. \quad (27)$$

where  $N_\lambda$  is a  $K$ -bimodule in the way described. For each finite sequence of suffixes

$$I = (i_1, \dots, i_n) \quad (i_1 \neq i_2 \neq \dots \neq i_n) \quad (28)$$

define a  $K$ -bimodule  $N_I$  by the equation

$$N_I = N_{i_1} \otimes \dots \otimes N_{i_n},$$

where all tensor products are taken over  $K$ . In particular if  $I = (i)$ , then  $N_I = N_i$ , while for the empty sequence  $\emptyset$  we put  $N_\emptyset = K$ . Now form the direct sum of all the  $N_I$ :

$$V = \sum \oplus N_I. \quad (29)$$

Then  $V$  is again a  $K$ -bimodule and in particular the action of  $K$  on the right is given by right multiplication. We consider  $V$  specifically as right  $K$ -module and for a fixed  $i$  we now define it as right  $R_i$ -module so that the restriction of  $R_i$  to  $K$  induces the given  $K$ -module structure.

With each sequence  $I$  of the form

$$I = (i_1, \dots, i_n) \quad (30)$$

where  $i_1 \neq \dots \neq i_n \neq i$  or  $n = 0$ , we associate the sequence

$$I^* = (i_1, \dots, i_n, i). \tag{31}$$

By the conditions imposed on (30), this is again of the form (28), and conversely, every sequence (28) is either of the form (30) or of the form (31), but not both. Now for any  $I$  satisfying (30), we have

$$\begin{aligned} N_I \otimes R_i &\cong (N_I \otimes K) \oplus (N_I \otimes N_i) \\ &\cong N_I \oplus N_{I^*}, \end{aligned}$$

and hence

$$V \cong \left( \sum' N_I \right) \otimes R_i, \tag{32}$$

where  $\sum'$  denotes the sum over all sequences  $I$  satisfying (30). Now (32) may be used to define a right  $R_i$ -module structure on  $V$ , of which the restriction to  $K$  is just right multiplication on  $V$ , and so coincides with the given right  $K$ -module structure. Moreover, taking  $I = \emptyset$  on the right of (32), we see that on  $R_i = K \oplus N_i$  the right  $R_i$ -module structure defined by (32) is just the usual one of right multiplication. Thus  $V$  is a right  $R_i$ -module with  $R_i$  itself as submodule, and by (29) it follows that for  $i \neq j$ ,  $R_i \cap R_j = K$ . We can now apply the theorem quoted from ref. 3 to conclude that the free product  $P$  of the  $R_i$  exists. Since all the  $R_i$  are augmented, we have a family of mappings from  $R_i$  to  $K$ ; by the universal mapping property they can be combined to a mapping  $P \rightarrow K$  and it is easily seen that this is a right inverse of the canonical injection  $K \rightarrow P$ . Therefore  $P$  is again augmented, and the proof is complete.

If  $k$  is a field then any  $k$ -ring  $\neq 0$  is necessarily strict, and is in fact augmented. Thus we obtain the

*COROLLARY. The free product of any family of  $k$ -rings ( $\neq 0$ ) over a field  $k$  exists.*

This result was also obtained in ref. 3 (Theorem 4.7, Cor.).

From the proof of Theorem 3.1 it is not hard to see that if  $P$  is the free product of the  $R_\lambda$ , each with the decomposition (27), then  $P$  is isomorphic to  $V$ , given by (29), as  $K$ -module or even as  $R_i$ -module (cf. also ref. 3). In this notation the filtration ( $H^n$ ) of  $P$  given in ref. 4 may be described by

$$H^n = \sum_n N_I,$$

where  $\sum_n$  indicates the sum over all sequences  $I$  of length at most  $n$ . We recall also that the *height*,  $h(a)$ , of an element  $a \in P$  was defined by the rule

$$h(a) = n \quad \text{if} \quad a \in H^n, \quad a \notin H^{n-1}.$$

Any element  $a \in H^n$  may be written in the form

$$a \equiv \sum a_I \pmod{H^{n-1}},$$

where  $a_I \in N_I$  and the sum is over all sequences  $I$  of length  $n$ . Here  $a_I$  is uniquely determined by  $a$  and is called the *homogeneous component of type  $I$*  of  $a$ ; in particular if  $h(a) < n$ , then  $a_I = 0$ . Thus in any congruence  $\pmod{H^{n-1}}$  between elements of  $H^n$  we may equate homogeneous components of a given type.

If  $a, b \in P$ , then we clearly have

$$h(ab) \leq h(a) + h(b). \quad (33)$$

We shall say that  $a, b$  *interact*, if the inequality in (33) is strict. Of course it need hardly be stressed that  $a, b$  may well interact without  $b, a$  interacting. Precise conditions for  $a, b$  to interact were given in [4, Theorem 2.1]; these conditions still apply in the present situation. In particular, two homogeneous elements  $a, b$  of types  $I = (i_1, \dots, i_n)$  and  $J = (j_1, \dots, j_m)$  respectively interact if and only if  $i_n = j_1$ ; when this is so, say  $i_n = j_1 = \lambda$ , then we shall say that  $a, b$  *interact in  $R_\lambda$* .

#### 4. THE FREE PRODUCT OF FIRS

The main task will be to establish a certain independence property of the free product of local firs, from which all our results will follow easily. In the proof a large number of summations over unrelated ranges will occur. We shall not indicate these ranges explicitly, but use the following convention: different latin suffixes will indicate (possibly) different ranges and summations are over all repeated suffixes, unless otherwise stated.

LEMMA 4.1. *Let  $K$  be a local fir and  $(R_\lambda)$  a family of local firs, where each  $R_\lambda$  is an augmented  $K$ -ring which is free as left  $K$ -module, while its augmentation module  $N_\lambda$  is free as right  $K$ -module. Denote by  $P$  the free product of the  $R_\lambda$  over  $K$ , with the filtration  $(H^n)$  described in Section III. Let  $a_k, b_k$  ( $k = 1, \dots, r$ ) be any elements of  $P$  such that  $h(a_k b_k) = n$  and*

$$\sum a_k b_k \equiv 0 \pmod{H^{n-1}}. \quad (34)$$

Further assume that the  $a_k$  are ordered by decreasing height, say  $h(a_i) = m$  for  $i \leq s$  and  $h(a_j) < m$  for  $j > s$ . Then either the  $a_i$  ( $i \leq s$ ) can be transformed unimodularly in  $K$  to a set including an element of height less than  $m$ , or the  $a_i$  ( $i \leq s$ ) which interact with  $b_i$  in a given factor  $R_\lambda$  can be transformed unimo-



dularly in  $R_\lambda$  to a set including an element of height less than  $m$ , or for each element  $a_i$  ( $i \leq s$ ) there exist elements  $x_{ji} \in P$  such that

$$h\left(a_i - \sum a_j x_{ji}\right) < m, \quad h(a_j x_{ji}) \leq m \quad (j > s).$$

*Proof.* By equating homogeneous components in (34), we may assume that all terms  $a_k b_k$  lie in the same component  $N_I \pmod{H^{n-1}}$ . We shall use induction on  $n$  and distinguish three cases.

(i)  $h(a_k) < n$  for all  $k$ . Then for each  $k$ , either  $h(b_k) \geq 2$  or  $h(b_k) = 1$  and  $a_k, b_k$  do not interact. Put  $I = (i_1, \dots, i_n)$ ,  $I' = (i_1, \dots, i_{n-1})$  and for simplicity assume that  $i_n = 1$ . Further, let  $(v_p)$  be a left  $K$ -basis for  $R_1$ , then

$$b_k = \sum x_{kp} v_p, \tag{35}$$

where  $x_{kp} \in P$ , such that  $a_k x_{kp} \in H^{n-2} + N_I$ , and  $a_k x_{kp}, v_p$  do not interact. Now

$$a_k b_k \in (H^{n-2} + N_{I'}) \otimes R_1 = H^{n-2} \otimes R_1 + N_I$$

and so

$$\sum a_k x_{kp} v_p \equiv 0 \pmod{H^{n-2} \otimes R_1}.$$

Since the  $v_p$  form a basis of  $R_1$ , we obtain for each  $p$ ,

$$\sum a_k x_{kp} \equiv 0 \pmod{H^{n-2}}. \tag{36}$$

Now  $a_k x_{kp} \in H^{n-1}$ , so if we retain only terms of height  $n - 1$  in (36), we can use induction on  $n$  to reach the conclusion, unless none of the congruences (36) contains a term  $a_1 x_{1p}$  of height  $n - 1$ . But this would mean that  $a_1 x_{1p} \in H^{n-2}$  for all  $p$ , and hence by (35),

$$a_1 b_1 \equiv \sum a_1 x_{1p} v_p \equiv 0 \pmod{H^{n-1}},$$

which contradicts the fact that  $h(a_1 b_1) = n$ .

(ii)  $h(a_k) = n$  for all  $k$ . Then  $b_k \in R_1$  and  $a_k \in H^{n-2} \otimes R_1 + N_I$ . Since each  $N_\lambda$  is free, as right  $K$ -module, it follows by induction on  $n$  that  $N_I$  is again free. Let  $(u_q)$  be a right  $K$ -basis of  $N_{I'}$ , then

$$a_k \equiv \sum u_q y_{qk} \pmod{H^{n-2} \otimes R_1}, \tag{37}$$

where  $y_{qk} \in R_1$  and  $u_q, y_{qk}$  do not interact. Substituting from (37) into (34) and putting  $c_q = \sum y_{qk} b_k$  for brevity, we obtain

$$\sum u_q c_q \equiv 0 \pmod{H^{n-2} \otimes R_1}. \tag{38}$$

Here  $c_q \in R_1$ , hence  $u_q c_q \in H^n$  and  $u_q, c_q$  do not interact. If there are any

terms of height  $n$  in (38), then when we retain only these terms, by case (i) there is a unimodular transformation in  $K$  of the  $u_q$  to a set including an element of height less than  $n - 1$ . But this contradicts the right  $K$ -independence of the  $u_q$ , hence  $u_q c_q \in H^{n-1}$  for all  $q$ . By (38), the sum of these terms lies in  $H^{n-2} \otimes R_1 = H^{n-2} + H^{n-2} \otimes N_1$ . But there can be no contribution to  $H^{n-2} \otimes N_1$ , because  $i_{n-1} \neq 1$ . Thus the congruence (38) is actually mod  $H^{n-2}$ , and if there are any terms of height  $n - 1$ , then by induction on  $n$  we can transform the  $u_q$  unimodularly in  $K$  to a set including an element of height less than  $n - 1$ . This leads to a contradiction as before, and therefore  $u_q c_q \in H^{n-2}$  for all  $q$ ; but this is possible only if  $c_q = 0$  for all  $q$ , i.e.

$$\sum y_{qk} b_k = 0.$$

Since  $R_1$  is a local fir and the  $b_k$  are not zero, we can transform the columns of the matrix  $(y_{qk})$  unimodularly in  $R_1$  to a set including zero (by Theorem 2.6). Applying the same transformation to the  $a_k$ , we obtain by (37) a set including an element of height less than  $n$  which is the desired conclusion.

(iii) In the remaining case,  $h(a_i) = n$  for  $i \leq s$  and  $h(a_j) < n$  for  $j > s$ . Let  $(v_p)$  again be a left  $K$ -basis for  $R_1$  and  $(u_q)$  a right  $K$ -basis for  $N_{I'}$ :

$$a_i \equiv \sum u_q y_{qi} \pmod{H^{n-2} \otimes R_1} \quad (i \leq s), \quad (39)$$

$$b_k = \sum x_{kp} v_p \quad (40)$$

as before, where  $x_{kp}$ ,  $v_p$  do not interact. If the columns  $(y_{qi})$  are right  $R_1$ -dependent, say

$$\sum y_{qi} c_i = 0 \quad \text{for all } q,$$

where the  $c_i$  are not all zero, then

$$\sum a_i c_i \equiv \sum u_q y_{qi} c_i \equiv 0 \pmod{H^{n-2} \otimes R_1};$$

by case (ii) we can transform the  $a_i$  unimodularly in  $R_1$  to a set including an element of height less than  $n$ . We may therefore assume that the columns  $(y_{qi})$  are right  $R_1$ -independent. Now the number of rows of  $(y_{qi})$  may well be infinite, but the number of congruences (39) is finite and each contains only a finite number of nonzero terms  $y_{qi}$ ; therefore the number of nonzero rows in  $(y_{qi})$  is finite and we may in the remainder of the proof use induction on the number of nonzero rows. If all rows are zero, then by (6),  $a_i \equiv 0 \pmod{H^{n-1}}$ , which contradicts the assumptions, so we may assume  $y_{qi} \neq 0$  for some  $q, i$ . From the assumptions about  $h(a_k)$  it follows that  $b_i \in R_1$  (for

$i \leq s$ ) while for  $j > s$ , either  $h(b_j) \geq 2$  or  $b_j \in R_1$  but  $a_j, b_j$  do not interact. Now for  $i \leq s$  we have  $x_{ip} \in K$  and so we may write

$$\sum y_{qi}x_{ip}v_p = \sum \eta_{qp}v_p \quad (\eta_{qp} \in K). \tag{41}$$

Inserting from (39), (40) and (41) into (34), we obtain

$$\sum u_q\eta_{qp}v_p + \sum a_jx_{jp}v_p \equiv 0 \pmod{H^{n-2} \otimes R_1},$$

and therefore (because the  $v_p$  form a basis of  $R_1$ ),

$$\sum u_q\eta_{qp} + \sum a_jx_{jp} \equiv 0 \pmod{H^{n-2}}. \tag{42}$$

If  $\eta_{qp} = 0$  for all  $q, p$ , then by (41),

$$\sum y_{qi}x_{ip}v_p = 0 \quad \text{for all } q,$$

and since the columns of  $(y_{qi})$  are right  $R_1$ -independent, it follows that  $\sum x_{ip}v_p = 0$ . But  $x_{ip} \in K$  and the  $v_p$  are left  $K$ -independent, so  $x_{ip} = 0$  for all  $i, p$ , whence by (40),  $b_i = 0$ , which contradicts the fact that  $h(a_i b_i) = n$ . Thus  $\eta_{qp} \neq 0$  for some  $q, p$ , say  $q = p = 1$ . If we apply the induction hypothesis for  $n$  to (42), we obtain elements  $c_j \in P$  such that

$$h\left(u_1 - \sum a_j c_j\right) < n - 1, \quad h(a_j c_j) \leq n - 1.$$

Now replace  $a_i$  by

$$a'_i = a_i - \sum a_j c_j y_{1i} \quad \text{and} \quad b_j \quad \text{by} \quad b'_j = b_j + \sum c_j y_{1j} b_i,$$

then we have the same situation as before, but with one fewer nonzero row  $(y_{qi})$  in (39), and so the result follows by the induction hypothesis.

For  $n = 0$  or  $1$  the result holds since  $K$  and each  $R_\lambda$  are local firs, and this completes the proof of the lemma.

We now apply the lemma to show that under the given conditions the free product of local firs is again a local fir.

**THEOREM 4.2.** *Let  $K$  be a local fir and  $(R_\lambda)$  a family of local firs, where each  $R_\lambda$  is an augmented  $K$ -ring which is free as left  $K$ -module while its augmentation module  $N_\lambda$  is free as right  $K$ -module. Then the free product of the  $R_\lambda$  over  $K$  is again a local fir.*

*Proof.* Let  $P$  be the free product of the  $R_\lambda$ ; we begin by showing that  $P$

is an integral domain. Omitting any factors  $R_\lambda$  which are equal to  $K$ , we may assume that  $R_\lambda \neq K$  for all  $\lambda$ ; hence  $N_\lambda \neq 0$  and since each  $N_\lambda$  is free, it follows easily (by induction on the length of  $I$ ) that  $N_I \neq 0$  for all sequences  $I$ . Now let  $a, b \in P$ ,  $a, b \neq 0$  and assume that  $ab = 0$ . By splitting each of  $a, b$  into its homogeneous components, we may assume that  $a \in N_I + H^{m-1}$  and  $b \in N_J + H^{n-1}$ , where  $I, J$  are of lengths  $m, n$  respectively. Suppose first that  $n > 1$  and write  $b = \sum x_p v_p$ , where  $(v_p)$  is a left  $K$ -basis for  $R_1$  and the  $x_p$  are homogeneous elements such that  $x_p, v_p$  do not interact. Then

$$\sum a x_p v_p = 0.$$

This lies in the direct summand  $(\sum N_G) \otimes R_1$  of  $P$ , where  $G$  runs over all sequences not ending in 1; it follows that  $a x_p = 0$  for all  $p$ , hence by induction on  $m + n$ , either  $a = 0$  or  $x_p = 0$  for all  $p$ , whence  $b = 0$ . Thus we may assume  $n = 1$ , say  $b \in R_1$ . If now  $a \in \sum N_G$ , the same reasoning holds as before; so we may take  $a = \sum u_q y_q$ , where the  $u_q$  are a right  $K$ -basis for  $N_{I'}$ ,  $I' = (i_1, \dots, i_{m-1})$ ,  $I = (i_1, \dots, i_m)$ , and  $y_q \in R_1$ . We thus have

$$\sum u_q y_q b = 0,$$

and hence  $y_q b = 0$  for all  $q$ . Since  $R_1$  is an integral domain, either  $b = 0$  or  $y_q = 0$  for all  $q$ , and hence  $a = 0$ . Thus  $P$  is indeed an integral domain.

To show that  $P$  is a local fir we shall verify condition (iii) of Theorem 2.6. Let

$$\sum a_k b_k = 0 \tag{43}$$

in  $P$ , where the  $a_k$  are not all zero. We begin by transforming the  $a_k$  and  $b_k$  unimodularly in  $P$  so that  $\max h(a_k b_k)$  has its least possible value,  $n$  say, and among all expressions with this value for  $\max h(a_k b_k)$ , take one for which  $\max h(a_i)$ , taken over all  $i$  with  $h(a_i b_i) = n$ , has its least possible value,  $m$  say. If after these transformations,  $b_k = 0$  for some  $k$ , then (iii) of Theorem 2.6 will be satisfied, so assume that  $b_k \neq 0$  for all  $k$ . Since the  $a_k$  were not all zero initially, the same holds after transformation, and so the  $a_k b_k$  are not all zero (because  $P$  is an integral domain) i.e.  $n > 0$ . Now write (43) as a congruence (mod  $H^{n-1}$ ). Then by Lemma 4.1, the  $a_i$  of maximal height  $m$  can be transformed unimodularly to a set including an element of height less than  $m$ . But this contradicts the construction and the result follows.

When the  $R_\lambda$  are all firs, we obtain

**THEOREM 4.3.** *Let  $K$  be a local fir and  $(R_\lambda)$  a family of firs, where each  $R_\lambda$  is an augmented  $K$ -ring which is free as left and as right  $K$ -module, while its augmentation module  $N_\lambda$  is a right ideal in  $R_\lambda$ . Then the free product of the  $R_\lambda$  is a fir.*

*Proof.* By Theorem 4.2, the free product  $P$  is certainly a local fir. Now well-order the sequences  $I$  by ascending length and put

$$M_\alpha = \sum_{I < \alpha} N_I, \quad \bar{M}_\alpha = \sum_{I \leq \alpha} N_I,$$

so that  $\bar{M}_\alpha/M_\alpha \cong N_I$  for some  $I$ ; this is of the form  $N_{I'} \otimes N_\lambda$  for some  $I', \lambda$ , and since  $N_{I'}$  is a free  $K$ -module,  $N_\lambda$  is a free  $R_\lambda$ -module. Let  $\mathfrak{a}$  be any right ideal of  $P$ , then

$$\frac{\mathfrak{a} \cap \bar{M}_\alpha}{\mathfrak{a} \cap M_\alpha} \cong \frac{(\mathfrak{a} \cap \bar{M}_\alpha) + M_\alpha}{M_\alpha} \cong \frac{\bar{M}_\alpha \cap (\mathfrak{a} + M_\alpha)}{M_\alpha}.$$

The last term on the right is a submodule of  $\bar{M}_\alpha/M_\alpha$ , and hence a free  $R_\lambda$ -module, so we have

$$\mathfrak{a} \cap \bar{M}_\alpha = (\mathfrak{a} \cap M_\alpha) \oplus \mathfrak{b}_\alpha,$$

$\mathfrak{b}_\alpha$  a free  $R_\lambda$ -module. Using induction on  $\alpha$ , let us assume that we have already a  $P$ -basis of  $\mathfrak{a} \cap M_\alpha$ , i.e., a right  $P$ -independent set  $B_\alpha$  in  $\mathfrak{a} \cap M_\alpha$  such that the right ideal of  $P$  generated by  $B_\alpha$  contains  $\mathfrak{a} \cap M_\alpha$ . Let  $B'$  be an  $R_\lambda$ -basis for  $\mathfrak{b}_\alpha$ , then  $B_\alpha \cup B'$  generates a right ideal including  $\mathfrak{a} \cap \bar{M}_\alpha$ , and it only remains to show that  $B_\alpha \cup B'$  is right  $P$ -independent. If this were not so, we would have a relation

$$\sum v_i a_i + \sum w_j b_j = 0, \tag{44}$$

where  $v_i \in B_\alpha$ ,  $w_j \in B'$  and the  $a_i, b_j \in P$  are not all zero. Let

$$n = \max \{h(v_i a_i), h(w_j b_j)\}$$

and rewrite (44) as a congruence (mod  $H^{n-1}$ ). Equating homogeneous components, we may assume that only terms  $v_i a_i$ , or only terms  $w_j b_j$  occur. The former contradicts the independence of  $B_\alpha$ , so we are left with

$$\sum w_j b_j \equiv 0 \pmod{H^{n-1}}.$$

By Lemma 4.1, the  $w_j$  may be transformed unimodularly in  $R_\lambda$  to a set including an element of height less than  $h(w_j)$ , which contradicts the fact they were chosen to be an  $R_\lambda$ -independent set. Thus  $B_\alpha \cup B'$  is a right  $P$ -basis for  $\mathfrak{a} \cap \bar{M}_\alpha$ . By induction on  $\alpha$  we obtain a  $P$ -basis for  $\mathfrak{a}$ , and this shows  $\mathfrak{a}$  to be free. This completes the proof.

When  $K$  is taken to be a field, most of the conditions of Theorem 4.2 hold automatically and we have

**COROLLARY 1.** *The free product of any family of local firs over a field is*

again a local fir. If  $(R_\lambda)$  is a family of firs which are augmented  $k$ -rings, where  $k$  is a field, such that the augmentation module in  $R_\lambda$  is a right ideal, then the free product of the  $R_\lambda$  is a fir.

Since a field is a particular fir, we see that the free product of any family of fields over a given field is a local fir. In refs. 4 and 8 it was shown that in such a free product all right ideals are free and it follows that the free product of fields (over a given field) is actually a fir.

Now let  $A$  be a free associative algebra on a set  $X$  over a commutative field  $F$ . Then  $A$  may be constructed as the free product of the family of polynomial rings  $F[x]$ , ( $x \in X$ ) over  $F$ . Since  $F[x]$  is a fir and  $F$  is complemented by an ideal, we obtain

**COROLLARY 2.** *The free associative algebra on a set  $X$  over a commutative field  $F$  is a fir.*

Next let  $G$  be the free group on a set  $X$  and  $G_F$  the group algebra of  $G$  over  $F$ . Then  $G_F$  is the free product over  $F$  of the group algebras of the infinite cyclic groups on the elements of  $X$ , so we need only verify that the group algebra of the infinite cyclic group over  $F$  is a fir and that  $F$  is complemented by an ideal. This group algebra is of the form  $F[x, x^{-1}]$ ; clearly  $F$  is complemented by an ideal (the augmentation ideal) and the ring itself is the ring of quotients of  $F[x]$  with respect to the set  $(x^{-n})$ , and is therefore a principal ideal domain (cf. ref. 13, p. 223). Hence  $F[x, x^{-1}]$  is a fir and we find

**COROLLARY 3.** *The group algebra of a free group (over a commutative field) is a fir.*

#### REFERENCES

1. AUSLANDER, M. On the dimension of modules and algebras III. *Nagoya Math. J.* **9** (1955), 67-77.
2. CARTAN, H. AND EILENBERG, S. "Homological Algebra." Princeton Univ. Press, 1956.
3. COHN, P. M. On the free product of associative rings. *Math. Z.* **71** (1959), 380-398.
4. COHN, P. M. On the free product of associative rings II. *Math. Z.* **73** (1960), 433-456.
5. COHN, P. M. On a generalization of the Euclidean algorithm. *Proc. Cambridge Phil. Soc.* **57** (1961), 18-30.
6. COHN, P. M. On the embedding of rings in skew fields. *Proc. London Math. Soc.* (3) **11** (1961), 511-530.
7. COHN, P. M. Non-commutative unique factorization domains. *Trans. Am. Math. Soc.* **109** (1963), 313-331.
8. COHN, P. M. Rings with a weak algorithm. *Trans. Am. Math. Soc.* **109** (1963), 332-356.
9. FUJIWARA, T. Note on the isomorphism problem for free algebraic systems. *Proc. Japan. Acad.* **31** (1955), 135-136.

10. GOLDIE, A. W. The structure of prime rings under ascending chain conditions. *Proc. London Math. Soc.* (3) **11** (1958), 589-608.
11. LEAVITT, W. G. Two word rings. *Proc. Am. Math. Soc.* **7** (1956), 867-870.
12. MACLANE, S. "Homology." Springer, Berlin, 1963.
13. ZARISKI, O. AND SAMUEL, P. "Commutative Algebra," Vol. I. Van Nostrand, Princeton, 1958.