Rings With a Weak Algorithm

P. M. Cohn

Transactions of the American Mathematical Society, Vol. 109, No. 2 (Nov., 1963), 332-356.

Stable URL:
http://links.jstor.org/sici?sici=0002-9947%28196311%29109%3A2%3C332%3ARWAWA%3E2.0.CO%3B2-Q

Transactions of the American Mathematical Society is currently published by American Mathematical Society.

RINGS WITH A WEAK ALGORITHM(1)

BY
P. M. COHN

1. **Introduction.** Commutative principal ideal domains form a somewhat special class of rings, which, however, possess many pleasant properties. Often we can make the task of deriving these properties even easier by limiting ourselves to Euclidean domains. If we have a valuated (commutative) ring and ask that it shall be a Euclidean domain with respect to this valuation, the ring is almost uniquely determined: it must be a polynomial ring $F[x]$ in a single indeterminate over a field F.

All these ideas can be generalized in a straightforward manner to the noncommutative case: the principal ideal domains again form a well-behaved though rather narrow class (cf. Jacobson [9, Chapter 3]), and the valuated rings with a Euclidean algorithm are just the skew polynomial rings $k[x;S,D]$ over a skew field k with an automorphism S and an S-derivation D(2). One obtains a slightly larger class by taking, instead of principal ideal domains, *Bezout rings*, i.e., integral domains in which any finitely generated (left or right) ideal is principal but this probably amounts to not much more than allowing locally principal ideal domains. A significantly wider class of rings is obtained by taking all integral domains in which any two principal right ideals with a nonzero intersection have a sum and intersection which are again principal. These are the *weak Bezout rings* introduced in [6], where it is shown that a weak Bezout ring in which prime factorizations exist, is a unique factorization domain, and other decomposition theorems hold (corresponding to the primary decomposition of an ideal in a Noetherian ring). Further it is shown there that the weak Bezout rings include free associative algebras in any number of free generators over a field.

It is possible to weaken the definition of the Euclidean algorithm in a similar way so as to obtain rings with a *weak algorithm* (cf. §2 for the definition). This was first introduced in [4] where it was applied to prove (in effect) that in any ring R with a weak algorithm, all right ideals were free R-modules. We now continue the study of rings with a weak algorithm and in particular show that they are weak Bezout rings, so that the results of [6] become applicable (§4). This

Received by the editors November 10, 1962.

(1) This work was supported by the U. S. Air Force through the Air Force Office of Scientific Research of the Air Research and Development Command under Contract No. SAR/G/AF/OSR 61-29.

(2) More generally, if S is allowed to be an endomorphism, all rings with a right-Euclidean algorithm are obtained. Cf. Jacobson [8], and independently, Cohn [4].

is done by means of the usual Euclidean algorithm, which is developed rather fully, using noncommutative continuants (§3). In §2 we recall some facts about the weak algorithm which were proved in [4] and show that for any bimodule M over a skew field k, the tensor k-ring on M has a weak algorithm. If we require k to lie in the centre of the ring, we just obtain the free associative algebras. In this special case some further applications of the weak algorithm can be made (§5); in particular it is shown that two elements of a free associative algebra which commute, must be algebraically dependent over the ground field.

In conclusion (§6) we establish a form of the weak algorithm for the free product of (any number of) skew fields over a given skew field k. This does not fall under the heading of §2, because the algorithm is not with respect to a true valuation; nevertheless we are able to use it to prove that (i) free products of skew fields are weak Bezout rings, and (ii) all right ideals are free modules. This generalizes some results obtained in [3].

2. **Definition of the weak algorithm.** Throughout this paper 'ring' means 'associative ring with a unit-element 1 which is different from 0', the subrings of R are understood to contain the 1 of R and the images of homomorphisms are understood to be subrings (so that 1 maps to 1 in any homomorphism). The term 'field' will be used in the sense of 'skew field', i.e., 'not necessarily commutative division ring'. Further, in any integral domain R, i.e., a ring without proper zero-divisors, the set of nonzero elements is denoted by R^*.

Let R be a filtered ring, more precisely, a ring with a positive increasing filtration

$$0 \subseteq R_0 \subseteq R_1 \subseteq \cdots \qquad (\bigcup R_n = R, \quad R_i R_j \subseteq R_{i+j}),$$

and define, for any $x \in R$, its *value* $v(x)$ by the equation

$$v(x) = \min\{n \mid x \in R_n\},$$

where formally, $v(0) = -\infty$; as is easily verified, v is a pseudovaluation on R (cf. [4]). We now have the following basic definitions(3):

(i) A subset X of R is *right R-dependent*, if $X = \{0\}$ or if $X = \{x_1, \cdots, x_r\}$ and there exist $a_1, \cdots, a_r \in R$ such that

$$v(x_1) + v(a_1) = \cdots = v(x_r) + v(a_r) > v(\sum x_i a_i).$$

(ii) A subset X of R is *right R-independent* if it contains no right R-dependent subset.

(iii) Given a subset X of R, an element $y \in R$ is *right R-dependent* on X if $y = 0$ or if there exist $x_1, \cdots, x_r \in X$ and $a_1, \cdots, a_r \in R$ such that

$$v(y - \sum x_i a_i) < v(y), \qquad v(x_i) + v(a_i) \leqq v(y) \qquad (i = 1, \cdots, r).$$

(3) The definitions given here reduce to those given in [4] for the case where v is a valuation. This will always be so under the special conditions imposed later on.

The notion of *left R-dependence* is defined analogously; we shall be mostly concerned with right R-dependence and we shall usually omit the word 'right'.

It should be noted that an R-dependent set is necessarily finite, and that a subset of R may be neither R-dependent nor R-independent. To say that the subset X of R is R-independent is to say that for any sum $\sum xa_x$ ($x \in X$, $a_x \in R$) we have

$$v(\sum xa_x) = \max\{v(x) + v(a_x) \mid x \in X\}. \tag{2.1}$$

For the left-hand side can at most equal the right-hand side, and if it were less, the terms for which $v(x) + v(a_x)$ attains its maximum would give a right R-dependence.

DEFINITION 1. A filtered ring R is said to possess a *right algorithm*, if the function v is a valuation, i.e., if

$$v(ab) = v(a) + v(b), \tag{2.2}$$

and if of any two nonzero elements of R, any one of maximal value is right R-dependent on the other.

DEFINITION 2. A filtered ring R is said to possess a *weak right algorithm*, if in any right R-dependent set, any element of maximal value is right R-dependent on the rest.

We note that in a ring with a weak right algorithm, the function v necessarily satisfies (2.2). For if not, then for some $a, b \in R$,

$$v(ab) < v(a) + v(b). \tag{2.3}$$

This means that the set $\{a\}$ is R-dependent, and hence a must be R-dependent on the empty set, i.e., $a = 0$. But for $a = 0$, (2.3) is clearly false if we interpret operations with $-\infty$ in the conventional way. Hence v is a valuation on R; in particular it follows that R is an integral domain.

The preceding remark shows that a ring with a right algorithm is necessarily a ring with a weak right algorithm. Conversely, a filtered ring with a weak right algorithm is a ring with a right algorithm (relative to the given filtration) if and only if it satisfies Ore's right multiple condition

$$aR \cap bR \neq 0 \qquad (a, b \in R^*) \tag{2.4}$$

(cf. Cohn [4, Theorem 3.1]).

It is clear how a ring with a (weak) left algorithm would be defined. Now we recall Theorem 3.2 of [4] which states that a ring has a weak left algorithm if and only if it has a weak right algorithm. We can therefore omit the attribute 'right' and simply speak of *rings with a weak algorithm*. Of course the right algorithm by no means implies the left algorithm (cf. the examples in [4]), although it does imply the weak left algorithm, by what has been said.

We recall the description of rings with a right algorithm given in [4, Theorem 2.1](4):

Let R be a filtered ring with a right algorithm. Then the elements of non-positive value form a field k and R is either k or the ring of skew polynomials $k[x;S,D]$, where S is an endomorphism of k and D an S-derivation. Thus R consists of all polynomials in x with right coefficients in k, subject to the commutation rule

$$\alpha x = x\alpha^S + \alpha^D \qquad (\alpha \in k). \tag{2.5}$$

Conversely, the ring $k[x;S,D]$ with any (non-negative) valuation for which $v(x) > 0$, has a right algorithm.

Similarly, the rings with a weak algorithm were described as follows [4, Theorems 3.4–3.5]:

Let R be a filtered ring with a weak algorithm. Then the elements of non-positive value form a field k, and if $X = \{x_\lambda\}_{\lambda \in \Lambda}$ is a right R-independent generating set for a right ideal complementing k in R (which always exists), then every element of R can be expressed in just one way as a sum

$$\sum x_I \alpha_I \qquad (\alpha_I \in k, \text{ almost all } \alpha_I \text{ are } 0), \tag{2.6}$$

where $I = (i_1, \cdots, i_r)$ runs over all ordered finite subsets of Λ and

$$x_I = x_{i_1} \cdots x_{i_r}.$$

Conversely, a filtered ring R containing a field k and a set X such that every element of R is unique of the form (2.6) *has a weak algorithm, provided that*

(i) $v(x) \leqq 0$ *implies* $x \in k$,

(ii) X *is right R-independent.*

In any filtered ring R the set R_0 of elements of nonpositive value forms a subring, provided that $1 \in R_0$. In that case we shall refer to R as a filtered R_0-ring, or if R_0 is contained in the centre of R, as a filtered R_0-algebra. Thus the above description shows that rings with a weak algorithm are filtered k-rings for some field k. Further, as was noted in [4, Theorem 3.6], the free associative algebra on a set X over a commutative field F may be characterized as a filtered F-algebra with a weak algorithm. As a more general example we have the tensor ring on a k-bimodule, where k is any skew field. To define this concept, we recall that in a k-ring the elements of k are regarded as unary operators, so that a *k-ring homomorphism* is a homomorphism between k-rings leaving the elements of k fixed.

---

(4) In [4] R was explicitly assumed to be valuated, whereas here the assumption that (2.2) holds is absorbed in the definition of the algorithm. Clearly this does not affect the truth of the result.

PROPOSITION 2.1. *Let k be a field and M a k-bimodule. Then there exists a k-ring T_M and a k-bimodule homomorphism*

$$\lambda : M \to T_M,$$

such that for any k-bimodule homomorphism $\phi : M \to A$, where A is a k-ring, there is a unique k-ring homomorphism $\phi' : T_M \to A$ such that $\lambda\phi' = \phi$. Further, T_M is unique up to isomorphism.

The existence and uniqueness of T_M follow as a particular case of the universal mapping property. T_M may be constructed explicitly by putting

$$T_M = \sum \oplus T^i, \qquad T^i = M \otimes M \otimes \cdots \otimes M, \ i \text{ factors}$$

where all the tensor products are taken over k, and the module T_M is made into a ring by defining a mapping

$$T^i \otimes T^j \to T^{i+j}: (x_1 \otimes \cdots \otimes x_i)(y_1 \otimes \cdots \otimes y_j) = x_1 \otimes \cdots \otimes x_i \otimes y_1 \otimes \cdots \otimes y_j,$$

and extending these mappings by linearity to a mapping of $T \times T$ into T. The resulting ring T_M is called the *tensor ring* on M; the above construction shows that the canonical mapping $\lambda : M \to T_M$ is 1-1 and we may therefore identify M with the subspace T^1 of T_M.

The ring T_M may be filtered by putting $(T_M)_n = \sum_{i \leqq n} T^i$; with this definition T_M becomes a k-ring with a weak algorithm. To show this we need only choose a basis X of M as right k-space. Then it is clear that every element of T_M is unique of the form (2.6); further, (i) holds by definition and (ii) follows since

$$v(\sum x_I \alpha_I) = \max \{v(x_I) \mid \alpha_I \neq 0\}.$$

Consider now a general filtered k-ring R with a weak algorithm. Let X be an R-independent generating set for a right ideal complementary to k. Then by the R-independence of X,

$$v(\sum x_I \alpha_I) = \max \{v(x_I \alpha_I)\},$$

and since v is a valuation,

$$v(x_{i_1} \cdots x_{i_r} \alpha) = v(x_{i_1}) + \cdots + v(x_{i_r}).$$

Thus v is completely determined by its values on X. Further, the multiplication in R is determined by k, X and equations analogous to (2.5) for αx_λ ($x_\lambda \in X$). These must have the form

$$\alpha x_\lambda = \sum x_I \rho_{I\lambda}(\alpha) \qquad (\rho_{I\lambda}(\alpha) = 0 \text{ for } v(x_I) > v(x_\lambda)). \tag{2.7}$$

This allows rather more general rings than tensor rings on k-bimodules. In the first place, we may take the bimodule M itself to have a filtration,

$$M_0 \subseteq M_1 \subseteq \cdots \qquad (\bigcup M_n = M, \quad M_n k + k M_n \subseteq M_n),$$

where we shall further assume for simplicity that $M_0 \cong k$. Then we may construct a tensor ring for this bimodule by applying the universal mapping property for mappings compatible with the filtration. This tensor ring has a natural filtration and relative to this filtration it has a weak algorithm, but even this is not the most general ring in this class, for if e.g. $v(x_1) = 2$, $v(x_2) = v(x_3) = 1$, then we may have an equation of the form

$$\alpha x_1 = x_1\alpha + x_2x_3,$$

which cannot occur in a tensor ring T_M. Thus there remains the problem of completely determining the structure of rings with a weak algorithm, or from another point of view, the problem of giving an intrinsic characterization of tensor rings on a bimodule.

An important property of rings with a weak algorithm is that all right (or left) ideals are free as modules over the ring. If we can show that any two bases of a free right module have the same cardinal, or even that in a free module on two free generators every basis consists of two elements, then it will follow (from [6], Theorem 6.2 and the remark following it) that the ring is a weak Bezout ring. We shall not take this route but verify directly (in §4 below) that every ring with a weak algorithm is a weak Bezout ring.

3. **The continuant polynomials.** Let $t_1, t_2, \cdots$ be a set of noncommuting indeterminates. We define a sequence of polynomials in the t's (with integer coefficients) by induction on n as follows:

$$f_0 = 1, \quad f_1(t_1) = t_1,$$
$$f_n(t_1, \cdots, t_n) = f_{n-1}(t_1, \cdots, t_{n-1})t_n + f_{n-2}(t_1, \cdots, t_{n-2}). \tag{3.1}$$

If the variables are allowed to commute, the expression for f_n reduces to the continuant (cf. Aitken [1, p. 126])

$$\begin{vmatrix} t_1 & 1 & & & & 0 & \\ -1 & t_2 & 1 & & & & \\ & -1 & t_3 & 1 & & & \\ & & \cdots\cdots & & & & \\ & & & \cdots\cdots & & & \\ 0 & & & & -1 & t_{n-1} & 1 \\ & & & & & -1 & t_n \end{vmatrix},$$

and we shall therefore refer to f_n as the nth *continuant polynomials*. The following lemma generalizes the well-known relations between successive convergents to a continued fraction (cf., e.g., Hardy and Wright [7, Chapter X]; also Wedderburn [10]).

LEMMA 3.1. *The continuant polynomials f_n satisfy the identities*:
(i) $f_n(t_1,\cdots,t_n)f_{n-1}(t_{n-1},\cdots,t_1) = f_{n-1}(t_1,\cdots,t_{n-1})f_n(t_n,\cdots,t_1)$,
(ii) $f_{n+1}(t_1,\cdots,t_{n+1})f_{n-1}(t_n,\cdots,t_2) - f_n(t_1,\cdots,t_n)f_n(t_{n+1},\cdots,t_2) = (-1)^{n-1}$.

The proof is immediate by induction on n, using the recursion formulae (3.1). As in the commutative case, (ii) shows that if we substitute any elements of an arbitrary ring for $t_1,\cdots,t_{n+1}$, two successive f's can have no common (left or right) factor apart from units.

The continuant polynomials may be regarded as elements of the free associative algebra (over the integers) on $t_1,t_2,\cdots$. This ring has an involution (anti-automorphism of order two) which maps each t_i to itself. We denote this involution by J and call it the *reversal operator*. In the sequel we shall also require the following properties of f_n:

LEMMA 3.2. (i) $f_n(t_1,\cdots,t_n)^J = f_n(t_n,\cdots,t_1)$,
(ii) *if the variables $t_1,\cdots,t_n$ commute, then*

$$f_n(t_1,\cdots,t_n) = f_n(t_n,\cdots,t_1),$$

(iii) *if R is any ring with a valuation v (assuming only non-negative values), then for any elements $a_1,\cdots,a_n$ such that $v(a_i) > 0$ for all i except possibly $i = 1$ or $i = n$,*

$$v(f_n(a_1,\cdots,a_n)) = v(f_n(a_n,\cdots,a_1)).$$

Proof. (i) amounts to showing that

$$f_1(t_1,\cdots,t_n) = t_1f_{n-1}(t_2,\cdots,t_n) + f_{n-2}(t_3,\cdots,t_n),$$

and this follows by induction on n. Now (ii) follows because J reduces to the identity when the variables commute. To prove (iii) we first take the case $n = 2$, $v(a_1) = v(a_2) = 0$. Then the value of $a_1a_2 + 1$ can only be 0 or $-\infty$, according as the expression is different from or equal to zero, and correspondingly for $a_2a_1 + 1$. Moreover([5]), if $a_1a_2 + 1 = 0$, then $a_2 = (-a_1)^{-1}$ and so $a_2a_1 + 1 = 0$; the converse also holds, so that $v(a_1a_2 + 1) = v(a_2a_1 + 1)$ in this case. If $n = 1$, the assertion holds trivially; so assume now that $n > 2$ or $v(a_1) + v(a_2) > 0$. Then every term in $f_n(a_1,\cdots,a_n)$ apart from $a_1a_2\cdots a_n$ itself has lower value than $a_1a_2\cdots a_n$. Hence

$$v(f_n(a_1,\cdots,a_n)) = v(a_1\cdots a_n) = v(a_1) + \cdots + v(a_n),$$

and the result follows by symmetry.

LEMMA 3.3. *Let s be any noncommuting indeterminate([6]) with inverse s^{-1}. Then*

([5]) Because in a valuated ring there are no proper zero-divisors, and hence one-sided inverses are necessarily two-sided.

([6]) The polynomials in s, $s^{-1},t_1,t_2,\cdots$ may be considered purely formally or e.g., as certain elements in the group ring (over the integers) of the free group on $s,t_1,t_2,\cdots$.

(i) *if n is odd,*

$$f_n(t_1s,s^{-1}t_2,\cdots,s^{-1}t_{n-1},t_ns) = f_n(t_1,\cdots,t_n)s, \tag{3.2}$$

$$f_n(st_1,t_2s^{-1},\cdots,t_{n-1}s^{-1},st_n) = sf_n(t_1,\cdots,t_n). \tag{3.3}$$

(ii) *If n is even,*

$$f_n(t_1s,s^{-1}t_2,\cdots,t_{n-1}s,s^{-1}t_n) = f_n(t_1,\cdots,t_n), \tag{3.4}$$

$$f_n(st_1,t_2s^{-1},\cdots,st_{n-1},t_ns^{-1}) = sf_n(t_1,\cdots,t_n)s^{-1}. \tag{3.5}$$

(iii) *For any n,*

$$f_n(t_1,\cdots,t_n) = f_{n+1}(t_1,\cdots,t_{n-1},t_n-1,1). \tag{3.6}$$

Proof. We prove (i) and (ii) by simultaneous induction on n. If n is odd and greater than 1, we have

$$\begin{aligned} f_n(t_1s,\cdots,t_ns) &= f_{n-1}(t_1s,\cdots,s^{-1}t_{n-1})t_ns + f_{n-2}(t_1s,\cdots,t_{n-2}s) \\ &= f_{n-1}(t_1,\cdots,t_{n-1})t_ns + f_{n-2}(t_1,\cdots,t_{n-2})s \\ &= f_n(t_1,\cdots,t_n)s, \end{aligned}$$

where we have used the definition twice and the induction hypothesis once. This establishes (3.2) and by symmetry (or by applying J) (3.3). Next, if n is even and greater than 0,

$$\begin{aligned} f_n(t_1s,\cdots,s^{-1}t_n) &= f_{n-1}(t_1s,\cdots,t_{n-1}s)s^{-1}t_n + f_{n-2}(t_1s,\cdots,s^{-1}t_{n-2}) \\ &= f_{n-1}(t_1,\cdots,t_{n-1})t_n + f_{n-2}(t_1,\cdots,t_{n-2}) \\ &= f_n(t_1,\cdots,t_n); \end{aligned}$$

in the same way we can establish (3.5). Now (i) and (ii) clearly hold for $n = 1$ and 0, respectively, and therefore they hold generally.

To prove (iii) we have

$$\begin{aligned} f_{n+1}(t_1,\cdots,t_n-1,1) &= f_n(t_1,\cdots,t_n-1) + f_{n-1}(t_1,\cdots,t_{n-1}) \\ &= f_{n-1}(t_1,\cdots,t_{n-1})(t_n-1) + f_{n-2}(t_1,\cdots,t_{n-2}) + f_{n-1}(t_1,\cdots,t_{n-1}) \\ &= f_{n-1}(t_1,\cdots,t_{n-1})t_n + f_{n-2}(t_1,\cdots,t_{n-2}) \\ &= f_n(t_1,\cdots,t_n). \end{aligned}$$

This completes the proof.

We note that (i) and (ii) may also be proved by observing that $f_n(t_1,\cdots,t_n)$ is a sum of terms of which the first is $t_1t_2\cdots t_n$ and the others are obtained from this by omitting one or more factors of the form $t_{i-1}t_i$, in all possible ways. Thus e.g., $f_2 = t_1t_2 + 1$, $f_3 = t_1t_2t_3 + t_1 + t_3$, $f_4 = t_1t_2t_3t_4 + t_1t_2 + t_3t_4 + t_1t_4 + 1$.

4. **The Euclidean algorithm.** Let R be a ring with a weak algorithm. We shall now develop an analogue of the Euclidean algorithm in R, which will be used to show that R is a weak Bezout ring.

Given two elements $a, b \in R$ with a nonzero common right multiple in R, say,

$$ab' = ba' \neq 0, \tag{4.1}$$

we may regard this relation as a right R-dependence between a and b. We assert that there exist $q_1, r_1 \in R$ such that

$$a = bq_1 + r_1, \qquad v(r_1) < v(b). \tag{4.2}$$

For if q_1 is chosen so that $v(a - bq_1)$ is minimal and we had $v(a - bq_1) \geqq v(b)$, then because $(a - bq_1)b' = b(a' - q_1b')$, the weak algorithm in R shows that $a - bq_1$ is right R-dependent on b, i.e., there exists $c \in R$ such that

$$v(a - b(q_1 + c)) < v(a - bq_1),$$

which contradicts the choice of q_1. Writing $r_1 = a - bq_1$, we thus obtain (4.2); we note incidentally that q_1 and r_1 are uniquely determined in (4.2), for if we also had $a = bq + r (v(r) < v(b))$, then

$$b(q - q_1) = r_1 - r, \tag{4.3}$$

and if $q \neq q_1$, then $v(b) \leqq v(b(q - q_1)) = v(r_1 - r) < v(b)$, which is a contradiction. Therefore $q = q_1$ and by (4.3), $r = r_1$.

Substituting from (4.2) into (4.1) we obtain

$$r_1b' = (a - bq_1)b' = b(a' - q_1b').$$

If we put $r_1' = a' - q_1b'$, this may be written

$$r_1b' = br_1'. \tag{4.4}$$

By (4.4) and (4.2), $v(b) + v(r_1') = v(r_1) + v(b') < v(b) + v(b')$, hence $v(r_1') < v(b')$, so that there is complete left-right symmetry (as we know there must be, by Theorem 3.3 of [4]). It may happen that $r_1 = 0$, but by (4.4) this is so only if $r_1' = 0$. Excluding this case, we can apply the same reasoning to (4.4) and thus obtain the chain of equations of the Euclidean algorithm. More precisely, we obtain two such chains, one for left- and one for right-division:

$$\begin{array}{llll} a = bq_1 + r_1 & a' = q_1b' + r_1' & r_1b' = br_1', \\ b = r_1q_2 + r_2 & b' = q_2r_1' + r_2' & r_2r_1' = r_1r_2', \\ r_1 = r_2q_3 + r_3 & r_1' = q_3r_2' + r_3' & r_3r_2' = r_2r_3', \\ \cdots & \cdots & \cdots \ . \end{array} \tag{4.5}$$

Note that whereas the remainders r_i, r_i' on the two sides are in general distinct, the quotients q_i are the same. The values of the remainders decrease strictly.

$$v(b) > v(r_1) > \cdots, \qquad v(b') > v(r_1') > \cdots. \tag{4.6}$$

Hence the remainders must vanish eventually. Let n be the least integer such that $r_{n+1} = 0$. Since $r_{n+1}r_n' = r_n r_{n+1}'$, it follows that $r_{n+1}' = 0$; if we had $r_k' = 0$ for some $k \leqq n$, then by symmetry, $r_k = 0$, which contradicts the definition of n. Hence r_{n+1}' is the first vanishing remainder of the right-hand division and the last two rows of (4.5) read

$$\begin{aligned} r_{n-2} &= r_{n-1}q_n + r_n & r_{n-2}' &= q_n r_{n-1}' + r_n' & r_n r_{n-1}' &= r_{n-1}r_n', \\ r_{n-1} &= r_n q_{n+1} & r_{n-1}' &= q_{n+1}r_n' & r_{n+1} &= r_{n+1}' = 0. \end{aligned} \tag{4.5)'}$$

From (4.5), (4.5)′ and the inequalities (4.6) we see that

$$v(q_i) > 0 \quad (i = 2,3, \cdots, n+1), \tag{4.7}$$

while $v(q_1) > 0$ if and only if $v(b) < v(a)$.

Using the continuant polynomials f_n, we may express the equations (4.5) and (4.5)′ as follows:

$$a = r_n f_{n+1}(q_{n+1}, \cdots, q_1), \qquad b = r_n f_n(q_{n+1}, \cdots, q_2), \tag{4.8}$$

$$a' = f_{n+1}(q_1, \cdots, q_{n+1})r_n', \qquad b' = f_n(q_2, \cdots, q_{n+1})r_n'. \tag{4.9}$$

It is now an easy matter to prove that R is a weak Bezout ring:

THEOREM 4.1. *A ring with a weak algorithm is a weak Bezout ring, i.e., any two principal right ideals with nonzero intersection have an intersection and sum which are again principal.*

Proof. Let $aR \cap bR \neq 0$, then by the above reasoning there exist r_n, r_n', $q_1, q_2, \cdots, q_{n+1} \in R$, all different from zero except possibly q_1, such that (4.8) and (4.9) hold. We assert that

$$aR \cap bR = mR, \qquad aR + bR = dR,$$

where $m = af_n(q_2, \cdots, q_{n+1})$, $d = r_n$. For by Lemma 3.1 (i),

$$m = af_n(q_2, \cdots, q_{n+1}) = bf_{n+1}(q_1, \cdots, q_{n+1}),$$

which shows that $m \in aR \cap bR$. Conversely, if $m_1 \in aR \cap bR$, say $m_1 = ab_1 = ba_1$, then by applying the algorithm to this equation, we find analogously to (4.9),

$$b_1 = f_n(q_2, \cdots, q_{n+1})r_n^*,$$

with the same quotients q_i, since these were determined by a, b alone. Hence

m_1 is a right multiple of m, which shows that $aR \cap bR = mR$. Next, r_n clearly is a left factor of a and b, by (4.8), while the equation

$$af_{n-1}(q_2, \cdots, q_n) - bf_n(q_1, \cdots, q_n) = (-1)^n r_n,$$

which follows from Lemma 3.1 (ii), shows that $r_n \in aR + bR$. This means that $aR + bR = r_nR$, as asserted, and the theorem follows.

COROLLARY 1. *Any ring with a right algorithm is a right Bezout ring.*

For the hypothesis means that R satisfies the Ore condition (2.4), and the conclusion therefore follows from Theorem 5.2 of [6].

In a ring with a weak algorithm, any element which is neither zero nor a unit may be expressed as a product of primes. For in any factorization of a, the number of nonunit factors is bounded by $v(a)$, and to obtain a prime factorization we need only take a factorization into nonunits with a maximal number of factors. Applying [6, Theorem 5.5, Corollary 1], we therefore obtain(7)

COROLLARY 2. *A ring with a weak algorithm is a unique factorization domain*(8).

It follows that the other decomposition theorems established in [6, Theorems 5.7–5.8], giving complete decompositions of an element into indecomposable and right indecomposable elements, respectively, also hold for rings with a weak algorithm. The proof of Theorem 4.1 actually gives more information than this; we recall that a commutative UFD is characterized by the fact that this multiplicative semigroup, taken modulo the group of units, is free commutative. In the same way we can give a description of the defining relations in a ring with a weak algorithm.

COROLLARY 3. *Let R be a ring with a weak algorithm. Then the multiplicative semigroup of R is generated (modulo the group of units) by its prime elements and a set of defining relations is given by the equations*

$$f_{n+1}(a_1, \cdots, a_{n+1})f_n(a_n, \cdots, a_1) = f_n(a_1, \cdots, a_n)f_{n+1}(a_{n+1}, \cdots, a_1), \tag{4.10}$$

where $n = 1, 2, \cdots$ and $a_1, \cdots, a_{n+1}$ run over all elements of R.

Of course these relations are redundant, i.e., the f_n do not necessarily represent primes in R, and not all of the relations (4.10) are needed. As an example of (4.10), we note the simplest case, $n = 1$, which is of the form

$$(xy + 1)x = x(yx + 1).$$

As an application of the Euclidean algorithm we shall now describe the general

(7) For noncommutative Euclidean domains this was obtained by Wedderburn [10]. Cf. Jacobson [9] and the references given there.

(8) This term is used here in the sense defined in [6].

solution of a linear equation in two unknowns with coprime coefficients. Here two elements are said to be *left coprime* if they have a common nonzero right multiple but no common left factor apart from units. Thus in a ring R with a weak algorithm, the elements a, b are left coprime if and only if neither is zero and $aR + bR = R$. The definition of right coprime elements is analogous.

THEOREM 4.2. *Let R be a filtered k-ring with a weak algorithm and let a, b be two elements of R not both in k, which are left coprime. Then there exist elements $a', b', c', d' \in R$ such that*

$$ab' - ba' = 0, \qquad v(a') = v(a), \qquad v(b') = v(b), \tag{4.11}$$

and

$$ad' - bc' = 1, \qquad v(c') < v(a), \qquad v(d') < v(b). \tag{4.12}$$

The elements c', d' are uniquely determined by a, b while a', b' are determined up to a common right factor from k^*. Further, the equation

$$a\xi - b\eta = g \tag{4.13}$$

has a solution for any $g \in R$, the general solution being

$$\xi = d'g + b'h, \qquad \eta = c'g + a'h, \tag{4.14}$$

where h is an arbitrary element of R.

Proof. By the Euclidean algorithm we have

$$a = r_n f_{n+1}(q_{n+1}, \cdots, q_1), \qquad b = r_n f_n(q_{n+1}, \cdots, q_2),$$

where $r_n \in k^*$, because a and b are left coprime. If we put

$$\begin{aligned} a' &= f_{n+1}(q_1, \cdots, q_{n+1}), & b' &= f_n(q_2, \cdots, q_{n+1}), \\ c' &= (-1)^{n-1} f_n(q_1, \cdots, q_n) r_n^{-1}, & d' &= (-1)^{n-1} f_{n-1}(q_2, \cdots, q_n) r_n^{-1}, \end{aligned}$$

then the equations in (4.11) and (4.12) hold, as well as the value conditions, because $v(q_{n+1}) > 0$ (cf. Lemma 3.2 (iii)). Further $ab' = ba'$ is a least common right multiple of a and b and so the solution of (4.11) is unique up to right multiplication by units, i.e., elements of k^*. Now the solution (4.12) is also unique, for otherwise we should by subtraction obtain a common right multiple $ab_0 = ba_0$ which is of lower value than ab', clearly an impossibility. Next consider any solution of (4.13); we have

$$a(\xi - d'g) = b(\eta - c'g),$$

hence $\xi - d'g = b'h$, $\eta - c'g = a'h$ for some $h \in R$, which shows the solution to be of the form (4.14). Conversely, every pair ξ, η of the form (4.14) satisfies (4.13) as is easily seen, and so the proof is complete.

To apply the theorem we may use the

PROPOSITION 4.3. *Two elements a, b of a ring R with a weak algorithm are left coprime if they are different from zero and there exist $\lambda \in k^*$, $u, v \in R$ such that*

$$av - bu = \lambda.$$

Proof. If $u = 0$, then $av\lambda^{-1} = 1$, so a is a unit and the result holds trivially. If $u \neq 0$, then

$$bu\lambda^{-1}a = (av - \lambda)\lambda^{-1}a = a(v\lambda^{-1}a - 1),$$

thus $aR \cap bR \neq 0$ and hence $aR + bR = dR$ for some $d \in R$. Since d must be a left factor of λ, it is a unit and $aR + bR = R$, as we had to show.

Let R be any ring with a weak algorithm. Two elements a, a' of R are said to be *related*, in symbols $a \overline{\wedge} a'$, if there exist elements $z_1, \cdots, z_n \in R$ such that

$$a = f_n(z_1, \cdots, z_n), \qquad a' = f_n(z_n, \cdots, z_1).$$

If we put

$$b = f_{n-1}(z_1, \cdots, z_{n-1}), \qquad b' = f_{n-1}(z_{n-1}, \cdots, z_1),$$
$$c' = (-1)^n f_{n-1}(z_n, \cdots, z_2), \qquad d' = (-1)^n f_{n-2}(z_{n-1}, \cdots, z_2),$$

then we have

$$ab' = ba', \qquad ad' - bc' = 1,$$

and it follows that a and a' are similar (cf. [(6, Propositions 2.1 and 5.3]). The converse does not quite hold: any two associated elements are similar, but not necessarily related. However, if two elements are similar, one of them is related to an associate of the other. For the proof we need a lemma on related elements.

LEMMA. *Let a, a' be related elements in a ring R with a weak algorithm, and let u be a unit in R. Then* (i) $au \overline{\wedge} a'u$, (ii) $ua \overline{\wedge} ua'$, (iii) $u^{-1}au \overline{\wedge} a'$.

Proof. Let

$$a = f_n(z_1, \cdots, z_n), \qquad a' = f_n(z_n, \cdots, z_1), \tag{4.15}$$

and suppose first that n is odd. Then by Lemma 3.3,

$$f_n(z_1u, u^{-1}z_2, \cdots, z_nu) = au,$$
$$f_n(z_nu, u^{-1}z_{n-1}, \cdots, z_1u) = a'u,$$

hence $au \overline{\wedge} a'u$ in this case. If n is even, we may rewrite a, a' as

$$a = f_{n+1}(z_1, \cdots, z_n - 1, 1), \qquad a' = f_{n+1}(1, z_n - 1, \cdots, z_1)$$

and apply the same argument. This proves (i) and now (ii) follows by symmetry.

To prove (iii) we first assume that n is even in (4.15). Then we have again by Lemma 3.3,

$$f_n(u^{-1}z_1, z_2u, \cdots, u^{-1}z_{n-1}, z_nu) = u^{-1}au,$$
$$f_n(z_nu, u^{-1}z_{n-1}, \cdots, z_2u, u^{-1}z_1) = a';$$

if n is odd we can again change its parity and so establish (iii) in all cases.

PROPOSITION 4.4. *In a ring with a weak algorithm, two elements a, a' are similar if and only if a is related to an associate of a'.*

Proof. We have seen that related elements are similar; hence an element is also similar to any associate of a related element. Conversely, if a and a' are similar, then there is a coprime relation([9])

$$ab' = ba'. \tag{4.16}$$

By the Euclidean algorithm we can determine $q_1, \cdots, q_{n+1}$, r_n, $r_n' \in R$ such that (4.8) and (4.9) hold. Since (4.16) is coprime, r_n and r_n' must be units and $r_n^{-1}a \overline{\wedge} a'r_n'^{-1}$. By the lemma it follows that $a \overline{\wedge} r_n a' r_n'^{-1}$, as we wished to show.

It is clear that the notion of relatedness is reflexive and symmetric. Whether it is also transitive is not known, but in practice it plays a subordinate role to the notion of similarity, which of course is reflexive, symmetric and transitive. A more interesting question is the following: it may happen that an element is related to infinitely many distinct elements of R. E.g., if k is the ground field, then $a \overline{\wedge} \lambda^{-1}a\lambda$ for all $\lambda \in k^*$, and if k is not contained in the centre of R, these elements may include infinitely many distinct ones. However, the elements $\lambda^{-1}a\lambda$ are also associated to a and this raises the following question:

In a ring with a weak algorithm, or more generally, in a weak Bezout ring, can a similarity class of elements consist of infinitely many classes of associated elements?

5. **Free associative algebras.** All the results obtained for rings with a weak algorithm naturally apply to free associative algebras. In this section we obtain some further results for these algebras, which depend on their special nature. The main result is

THEOREM 5.1. *Let A be a free associative algebra over a commutative field F. If $a, b, b' \in A$, where $a \neq 0$ and ([10]) $v(b) > 0$, and*

$$ab' = ba, \tag{5.1}$$

then there is a polynomial $\phi(t) \in F[t]$ in one variable and an element $c \in A$, such that

$$\phi(b) = ac, \qquad \phi(b') = ca. \tag{5.2}$$

([9]) I.e., a relation (4.16) in which a, b are left coprime and a', b' right coprime (cf. [6]).

([10]) By $v(b)$ we mean the degree of b in the free generators of A.

If ϕ is taken to be the monic polynomial of least degree satisfying (5.2), *then ϕ is uniquely determined and if ϕ splits over F,*

$$\phi(t) = \prod_{i=1}^{n} (t - \alpha_i), \tag{5.3}$$

then for any $\lambda \in F$, the following three conditions are equivalent:

(i) *a and $b - \lambda$ have a nontrivial common left factor,*

(ii) *a and $b' - \lambda$ have a nontrivial common right factor,*

(iii) *λ equals one of the α_i.*

Proof. From (5.1) we have, by induction on n,

$$ab'^n = b^n a,$$

and hence by linearity,

$$af(b') = f(b)a, \tag{5.4}$$

for any polynomial $f(t) \in F[t]$. By the weak algorithm in A,

$$f(b) = aq_f + r_f, \qquad \text{where } v(r_f) < v(a). \tag{5.5}$$

Now a, b, b' belong to a subalgebra of A which is free on a finite generating set. We need only restrict attention to those free generators which occur in a, b and b'. We may therefore assume from the outset that A is finitely generated. In particular, the space of elements of value $< v(a)$ is then finite-dimensional. Since $v(b) > 0$, the subalgebra $F[b]$ generated by b is infinite-dimensional over F, and by (5.5) the mapping $f \to r_f$ is linear. It is therefore not 1-1, and taking any nonzero element $f(b)$ in the kernel, we have

$$f(b) = aq.$$

Inserting this in (5.4), we obtain $af(b') = aqa$, whence

$$f(b') = qa.$$

This proves the first part. Let ϕ be monic and of least degree, subject to the conditions $\phi(b) = ac$, $\phi(b') = ca$ (for some $c \in A$). If also $\psi(b) = ad$, $\psi(b') = da$, where ψ has the same degree as ϕ and is also monic, then $\phi - \psi$ is a polynomial of lower degree satisfying (5.2), and hence vanishes identically. Now assume (5.3) holds and suppose that a and $b - \alpha_1$ have no common left factor. Since

$$(b - \alpha_1)a = a(b' - \alpha_1),$$

it follows that a and $b - \alpha_1$ are left coprime, so there exist $u, v \in A$ such that

$$av - (b - \alpha_1)u = 1. \tag{5.6}$$

Put([11]) $\phi_1(t) = \prod_{i\neq 1}(t-\alpha_i)$, then by (5.6),

$$\begin{aligned}\phi_1(b) &= \phi_1(b)av - \phi_1(b)(b-\alpha_1)u \\ &= a\phi_1(b')v - \phi(b)u \\ &= a(\phi_1(b')v - cu),\end{aligned}$$

where we have used (5.4), (5.3) and then (5.2). Since ϕ_1 has lower degree than ϕ, this contradicts the definition of ϕ. Thus a and $b-\alpha_1$ have a common left factor, and similarly with α_1 replaced by α_i $(i=2,\cdots,r)$. Conversely, if a and $b-\lambda$ have a common factor, so have $\phi(b)=ac$ and $b-\lambda$([12]); it follows that $\lambda=\alpha_i$ for some i. This proves that (i)$\Leftrightarrow$(iii) and by symmetry we find that (ii)$\Leftrightarrow$(iii).

COROLLARY 1. *If F is algebraically closed and $a,b,b'\in A$ are such that a is prime and*

$$ab' = ba,$$

then there exist $c\in A$ and $\lambda\in F$ such that

$$b = ac+\lambda, \qquad b' = ca+\lambda.$$

If $v(b)=0$, this holds trivially; otherwise, by the theorem, for some $\lambda\in F$, a and $b-\lambda$ have a common left factor, which must be a itself, because a is prime. Thus $b-\lambda=ac$ and hence also $b'-\lambda=ca$.

COROLLARY 2. *If F is algebraically closed and $a,b,b'\in A$ are such that*

$$ab' = ba, \qquad 0<v(b)<v(a),$$

then a is not prime.

For if a were prime, then by Corollary 1, $b=ac+\lambda$, which is impossible by the condition on the degrees.

As an illustration of Theorem 5.1, consider the relation

$$ad - bc = \lambda \tag{5.7}$$

in a free associative algebra A over F, where $\lambda\in F$, and we further assume that $a\neq 0$, $c\notin F$, to exclude trivialities. Multiplying (5.7) by c on the left and a on the right, we obtain $ca\cdot da - cb\cdot ca = \lambda ca$, or

$$ca(da-\lambda) = cb\cdot ca,$$

which is of the form (5.1), with a,b,b' replaced by ca, cb, $da-\lambda$, respectively. It is easily seen that the polynomial ϕ is in this case $t(t+\lambda)$, unless $\lambda=0$ and $b\in aR$, in which case $\phi\equiv t$.

([11]) Note that the α_i need not be distinct.

([12]) The factors $b-\alpha_i$ all commute with one another, so their order is immaterial.

The information provided by Theorem 5.1 is not as explicit as one might wish. Thus, if a, b, b' satisfying (5.1) are homogeneous in the free generators of A, then it can be shown that there exist $u, v \in A$ and an integer r such that([13])

$$a = (uv)^r u, \qquad b = uv, \qquad b' = vu.$$

An analogous assertion for nonhomogeneous elements would be

$$a = f(uv)u, \qquad b = uv, \qquad b' = vu, \tag{5.8}$$

for some polynomial f, or weaker still,

$$a = f(uv)u, \qquad b = g(uv), \qquad b' = g(vu), \tag{5.8$'$}$$

for certain polynomials f and g. But such a representation need not exist, as the following example shows: A is free associative on x and y, and

$$a = xy^2x + xy + yx + x^2 + 1, \qquad b = xy^2 + x + y, \qquad b' = y^2x + x + y.$$

Clearly $ab' = ba$, but no representation of the form (5.8) or (5.8)$'$ exists. To see this we need only consider the more general form (5.8)$'$. If either u or v were a unit, it would belong to F and so b and b' would be equal, which is not the case. Hence both u and v have positive degree and since $v(b) = 3$, g must be of degree 1; but the explicit form of b and b' shows this to be impossible.

We note incidentally, that in this example a is not prime if F is algebraically closed. This is not a priori obvious, but it follows easily from Corollary 2. By going through the proof, we find that

$$b^2 + 1 = a(y^2 + 1),$$

and hence

$$a = (xy + ix + 1)(yx - ix + 1) = (xy - ix + 1)(yx + ix + 1), \tag{5.9}$$

$$\begin{aligned} b \pm i &= (xy \pm ix + 1)(y \mp i), \\ b' \pm i &= (y \mp i)(yx \pm ix + 1), \end{aligned} \tag{5.10}$$

where $i = \sqrt{-1}$. Clearly the two factorizations (5.9) of a are into prime factors, and in fact $xy + ix + 1 = f_2(x, y + i)$ is related to $yx + ix + 1$. It may be verified that a is prime over the rational (or real) numbers.

Finally we ask when two elements of A commute. A plausible guess is that two elements of a free associative algebra commute if and only if they are polynomials in a suitably chosen element of A. We are not quite able to prove this, but as a partial result in this direction we have

THEOREM 5.2. *Let A be a free associative algebra over F and let $a, b \in A$ be such that $ab = ba$. Then a and b are algebraically dependent over F, i.e., there is a nonzero polynomial $f(x, y)$ with coefficients in F such that*

$$f(a, b) = 0. \tag{5.11}$$

([13]) This follows e.g. from [5, Theorem 4.1, Corollary 2].

Proof. The result is clearly true if a or b is in F, so assume $a, b \notin F$. Adjoin an indeterminate t to F, then

$$(a - t)b = b(t - a),$$

hence by Theorem 5.1, there is a polynomial ϕ over $F(t)$, not identically zero and such that

$$\phi(b) = (a - t)c,$$

where c has coefficients rational in t. Clearing of fractions in t, we may write this as

$$f(t, b) = (a - t)(c_0 + tc_1 + \cdots + t^n c_n), \tag{5.12}$$

where f has coefficients in F and $c_i \in A$. Since $ab = ba$, we may put $t = a$ in (5.12); then the right-hand side becomes zero and (5.11) follows.

The following result is also of interest in this context.

THEOREM 5.3. *Let A be a free associative algebra over F and let a be any element of A which is not in F. Then the centralizer of a in A is a commutative algebra.*

Proof. Denote by X a free generating set of A, then A may be embedded in the power series ring $\hat{A}$ in the elements of X over F. Now the centralizer C of a in $\hat{A}$ is a power series ring in a single indeterminate over F (cf. [5, Theorem 4.4]) and hence is commutative. The centralizer of a in A is clearly $C \cap A$; this is again commutative and the result is established.

COROLLARY. *If A is a free associative algebra over F, then any element of A not in F belongs to a unique maximal commutative subalgebra, namely, its centralizer, and any two distinct maximal commutative subalgebras of A meet in F.*

For by Theorem 5.3, the centralizer of an element not in F is commutative and it is clearly maximal commutative. Conversely, any maximal commutative subalgebra contains elements not in F and is therefore the centralizer of any one of these elements. It follows that the centralizer of an element not in F is the unique maximal commutative subalgebra containing it, i.e., the first assertion of the corollary, and the second assertion follows immediately from this.

6. **The algorithm in free products of fields.** Let $(R_\lambda)_{\lambda \in \Lambda}$ be any family of k-rings, where k is a given (skew) field. We denote the free product of this family over k (which always exists, by [2, Theorem 4.7, Corollary]), by P. In the case of two factors which are fields, we have previously shown [3, Lemma 3.4] that there is an analogue of the weak algorithm and have used this to prove that in this case all finitely generated (left or right) ideals are free modules [3, Theorem 3.5]. We shall now extend this algorithm to the free product of any family of fields; this more general situation actually allows some simplifications to be made

in the proof. We then apply the result to show that all right (or left) ideals of P are free P-modules and that P is a weak Bezout ring with prime factorization, from which it follows that P is a UFD.

We begin by introducing some notation([14]). As usual we regard each factor R_λ as a subring of P. If we put $H = \sum R_\lambda$, we have the filtration

$$k = H^0 \subseteq H^1 \subseteq H^2 \subseteq \cdots.$$

An element $a \in P$ is said to have the *height* n, $h(a) = n$, if $a \in H^n$, $a \notin H^{n-1}$. Such an element can be expressed in the form

$$a = \sum a_{1\lambda_1} a_{2\lambda_2} \cdots a_{n\lambda_n} + a',$$

where $a_{i\lambda_i} \in R_{\lambda_i}$, $a' \in H^{n-1}$, and where $\lambda_1 \neq \lambda_2 \neq \cdots \neq \lambda_n$. If we write $\bar{R}_\lambda = R_\lambda/k$, as k-bimodule, we have the direct sum

$$H^n/H^{n-1} \cong \sum \oplus \bar{R}_{\lambda_1} \otimes \cdots \otimes \bar{R}_{\lambda_n} \qquad (n \geqq 1), \tag{6.1}$$

where the summation is over all n-tuples $(\lambda_1, \cdots, \lambda_n)$ such that

$$\lambda_1 \neq \lambda_2 \neq \cdots \neq \lambda_n.$$

If we combine the isomorphism (6.1) with the natural mapping of H^n onto H/H^{n-1}, we obtain a homomorphism of H^n onto the right-hand side of (6.1), with kernel H^{n-1}. We denote this homomorphism by η_n. Now consider the partial sum on the right of (6.1), taken over those terms for which $\lambda_n = \nu$, for some fixed ν. The inverse image of this sum under η_n is denoted by H^n_ν, and any element of height n in H^n_ν is said to be *half pure*, more precisely *right pure* of type $(\cdot, \nu)$. Similarly the inverse image under η_n of the terms in (6.1) for which $\lambda_1 = \mu$ is denoted by ${}_\mu H^n$ and the elements of height n in ${}_\mu H^n$ are called *half pure* or *left pure* of type $(\mu, \cdot)$. Finally we put ${}_\mu H^n_\nu = {}_\mu H^n \cap H^n_\nu$ and call the elements of height n in ${}_\mu H^n_\nu$ *pure* of type (μ, ν). In the special case where P has only two factors, the direct sum in (6.1) has only two terms and any half pure element is automatically pure (cf. [3]).

To take account of purity, we now refine the notion of height. For any element $a \in P$, we define the *left height* $h_l(a)$ and the *right height* $h_r(a)$ as follows:

$$h_l(a) = \begin{cases} h(a) - \frac{1}{2} & \text{if } a \text{ is left pure of positive height,} \\ h(a) & \text{otherwise.} \end{cases}$$

$$h_r(a) = \begin{cases} h(a) - \frac{1}{2} & \text{if } a \text{ is right pure of positive height,} \\ h(a) & \text{otherwise.} \end{cases}$$

We recall that an element of P is said to be (left, right) *reducible* if it is (left, right) associated to an element of lower height, otherwise (left, right) *irreducible*. Then the result of Theorem 2.4 of [3] may be stated thus ([15]):

([14]) This differs in some minor respects from that used in [3].

([15]) The proof in [3] is only stated for the case of two factors, but it is easily seen to carry over to any number of factors.

Let P be the free product of k-rings without proper zero-divisors, then for any $a, b \in P$ such that either a is right irreducible or b is left irreducible,

$$h(ab) = h_r(a) + h_l(b) + \varepsilon(a, b), \tag{6.2}$$

where

$$\varepsilon(a,b) = \begin{cases} 1 & \text{if } a, b \text{ are right and left pure, respectively, of different types,} \\ \frac{1}{2} & \text{if } a \text{ is right pure or } b \text{ left pure but not both,} \\ 0 & \text{otherwise.} \end{cases}$$

We can now formulate the notion of P-dependence in analogy with the definitions of §2. In what follows P denotes the free product of the family $(R_\lambda)_{\lambda \in \Lambda}$ of k-rings without proper zero-divisors; however, we shall use the definition here only in the case where all the factors are fields.

(i) A subset X of P is *right P-dependent* if $X = \{0\}$ or if $X = \{x_1, \cdots, x_r\}$ and there exist $a_1, \cdots, a_r \in P$ such that

$$h(x_1 a_1) = \cdots = h(x_r a_r) > h(\sum x_i a_i).$$

(ii) A subset X of P is *right P-independent* if it contains no right P-dependent subset.

(iii) Given a subset X of P, an element $y \in P$ is *right P-dependent on X*, if y is right reducible or 0 or if there exist $x_1, \cdots, x_r \in X$, $a_1, \cdots, a_r \in P$ and a unit $u \in P$ such that

$$h_r(yu - \sum x_i a_i) < h_r(y), \qquad h_r(x_i a_i) \leqq h_r(y) \qquad (i = 1, \cdots, r).$$

Left P-dependence is defined similarly. With these definitions the main result may now be stated:

THEOREM 6.1. *Let P be the free product of a family $(K_\lambda)_{\lambda \in \Lambda}$ of fields over a given field k. Then in any right P-dependent set of right irreducible elements of P, any element of maximal right height is right P-dependent on the rest.*

A corresponding assertion holds with 'right' replaced by 'left' throughout.

The proof which we shall give of this result is modelled on that given in [3, Lemma 3.4] for the case of two factors. At the same time we correct an inaccuracy in [3]. First we restate the independence property of the tensor product and a decomposition formula for the elements of P which was obtained in [3]. To avoid confusion with the notion of P-dependence introduced above we shall refer to dependence in a space over k as k-dependence.

Given $a_1, \cdots, a_r \in H_\mu^m$ and $b_1, \cdots, b_r \in {}_\nu H^n$ $(\mu \neq \nu)$, if the a's are right k-independent (mod H^{m-1}) and

$$\sum a_i b_i \equiv 0 \pmod{H^{m+n-1}}, \tag{6.3}$$

then $b_i \in H^{n-1}$ $(i = 1, \cdots, r)$. This is merely a restatement of the independence property; it depends on k being a field, but the K_λ may be arbitrary k-rings. If we are again given $a_1, \cdots, a_r \in H^m_\mu$, where the a's are right k-independent $(\mathrm{mod}\, H^{m-1})$, but only know that $b_1, \cdots, b_r \in H^n$ and (6.3) holds, then $b_i \in {}_\mu H^n$ $(i = 1, \cdots, r)$. For if we write $b_i = \sum b_{iv}$, where $b_{iv} \in {}_v H^n$, then the preceding argument shows that $b_{iv} \in H^{n-1}$ for $v \neq \mu$; hence $b_i = b_{i\mu} + b_i'$, where $b_i' \in H^{n-1}$; thus $b_i \in {}_\mu H^n$.

We also require the extension to any number of factors of Lemma 3.2 of [3]. This is the following

LEMMA 6.2. *Let P be the free product of a family (R_λ) of k-rings. Given an element $a \in P$, of positive height n, an integer r in the range $1 \leqq r \leqq n$ and elements $a_h \in H^r$ which are right k-independent* $(\mathrm{mod}\, H^{r-1})$, *then there is an expression*

$$a \equiv \sum a_h x_h + \sum_{u \neq v} a_{i\mu} x_{iv} \qquad (\mathrm{mod}\, H^{r-1}), \tag{6.4}$$

where $a_{i\mu} \in H^r_\mu$, $x_{iv} \in {}_v H^{n-r}$, $x_h \in H^{n-r}$. Moreover, the a_h, $a_{i\mu}$ are right k-independent $(\mathrm{mod}\, H^{r-1})$ *and the x_{iv} of given height s $(\leqq n - r)$ are left k-independent* $(\mathrm{mod}\, H^{s-1})$; *in particular all the x_{iv} are left k-independent.*

The proof is precisely as for [3, Lemma 3.2] and is therefore omitted.

We now come to the proof of Theorem 6.1. Clearly the assertion is left-right symmetric; we shall assume $a_1, \cdots, a_r$, $b_1, \cdots, b_r \in P$ to be given nonzero elements such that b_ρ is left irreducible, $h_l(b_1) \geqq h_l(b_\rho)$, $h(a_\rho b_\rho) = N$ for $\rho = 1, \cdots, r$ and

$$\sum a_\rho b_\rho = 0 \qquad (\mathrm{mod}\, H^{N-1}). \tag{6.5}$$

We have to find elements $c_\rho \in P$ $(\rho = 2, \cdots, r)$ and a unit u such that

$$h_l(ub_1 - \sum c_\rho b_\rho) < h_l(b_1), \qquad h_l(c_\rho b_\rho) \leqq h_l(b_1). \tag{6.6}$$

If $a_1 \in k$, we can satisfy (6.6) with $u = a_1$, $c_\rho = -a_\rho$. We may therefore assume that $h(a_1) > 0$. In particular, in view of the left irreducibility of b_1 this implies that $N > 0$. For if $N = 0$, then $a_1 b_1 \in k$, i.e., b_1 is a unit and $h(a_1) > 0$, hence $h(b_1) > 0$, which contradicts the fact that b_1 is left irreducible. We now put $h(a_1) = m$, $h(b_1) = n$, $h(a_\rho) = m_\rho$, $h(b_\rho) = n_\rho$ $(\rho = 2, \cdots, r)$ and distinguish two cases.

(i) $N \neq m + n$. By (6.2), $N = m + n - 1$ and a_1, b_1 are half pure, of types $(\cdot, 1)$ and $(1, \cdot)$, say. By Lemma 6.2 we have a decomposition for a_1:

$$a_1 = \sum a_i' x_i + a_1^*, \tag{6.7}$$

where $a_i' \in H^{m-1}$, $a_1^* \in H^{m-2}$, $x_i \in K_1$ and further, the a_i' are right pure of type $\neq (\cdot, 1)$ and right k-independent $(\mathrm{mod}\, H^{m-2})$ and $x_i \notin k$.

Now $m+n-1=N \leqq m_\rho + n_\rho$ and $n_\rho \leqq n$, hence

$$m-1 \leqq m_\rho + n_\rho - n \leqq m_\rho \qquad (\rho = 2, \cdots, r).$$

So we may apply Lemma 6.2 to $a_1, \cdots, a_r$ in turn, and obtain the decompositions

$$a_\rho = \sum a_i' y_{i\rho} + \sum u_j z_{j\rho} + a_\rho^*, \tag{6.8}$$

where the u_j are right pure of height $m-1=N-n$ and such that a_i', u_j are right k-independent $(\mathrm{mod}\, H^{N-n-1})$, $a_\rho^* \in H^{N-n-1}$ and the $y_{i\rho}, z_{j\rho}$ have height $m_\rho - N + n$. Further, if a_ρ is right pure, of type $(\cdot, \lambda)$, say, then $y_{i\rho}, z_{j\rho}$ may also be taken to be right pure of type $(\cdot, \lambda)$.

It follows that the elements $y_{i\rho}b_\rho$, $z_{j\rho}b_\rho$ have height at most $m_\rho - N + n + n_\rho$ when $m_\rho + n_\rho = N$ and at most $m_\rho - N + n + n_\rho - 1$ when $m_\rho + n_\rho - 1 = N$, hence in either case,

$$y_{i\rho}b_\rho \equiv z_{j\rho}b_\rho \equiv 0 \qquad (\mathrm{mod}\, H^n). \tag{6.9}$$

Now $h(a_\rho^* b_\rho) \leqq m-2+n_\rho \leqq m-2+n = N-1$, so substituting in (6.5), we find

$$\sum a_i'(x_i b_1 + \sum y_{i\rho} b_\rho) + \sum u_j z_{j\rho} b_\rho \equiv 0 \quad (\mathrm{mod}\, H^{N-1}). \tag{6.10}$$

By hypothesis each a_i' is right pure of type $\neq (\cdot, 1)$; let a_1' be of type $(\cdot, 2)$ say, then by the independence property we obtain from (6.10)

$$x_1 b_1 + \sum y_{1\rho} b_\rho \equiv 0 \qquad (\mathrm{mod}_2 H^n). \tag{6.11}$$

Here the term $x_1 b_1$ is of type $(1, \cdot)$, while the other terms can each be expressed as a sum of left pure terms of the same form. When $y_{1\rho}$ has positive height, this is clear; otherwise we must have $m_\rho = m-1$ and since $n_\rho \leqq n$, $m_\rho + n_\rho \leqq \leqq m+n-1 = N$. Since $m_\rho + n_\rho \geqq N-1$, we have either $n_\rho = n$ or $n_\rho = n-1$. If $n_\rho = n$, then b_ρ is left pure, by the maximality of $h_l(b_1)$; if $n_\rho = n-1$, then $m_\rho + n_\rho = N-1$ and again b_ρ is left pure. If we now equate the terms of height n and type $(1, \cdot)$ in (6.11), we obtain

$$x_1 b_1 + \sum y_\rho' b_\rho \equiv 0 \qquad (\mathrm{mod}\, H^{n-1}), \tag{6.12}$$

and we can now satisfy (6.6) by putting $u = x_1$, $c_\rho = -y_\rho'$.

(ii) $N = m+n$. Since $m_\rho + n_\rho \geqq N = m+n$ and $n_\rho \leqq n$, we have $m_\rho \geqq m$. Lemma 6.2 again gives a decomposition

$$a_1 = \sum a_i', \tag{6.7)'}$$

where a_i' is right pure of height m, and similarly for $\rho = 2, \cdots, r$,

$$a_\rho = \sum a_i' y_{i\rho} + \sum u_j z_{j\rho} + a_\rho^*, \tag{6.8)'}$$

where u_j is right pure of height $m = N-n$ and such that the a_i', u_j are right

k-independent (mod H^{m-1}), $a_\rho^* \in H^{m-1}$, $y_{i\rho}$, $z_{j\rho} \in H^{m_\rho - m}$. Further, if a_ρ is right pure of type $(\cdot, \lambda)$, then $y_{i\rho}$, $z_{j\rho}$ are right pure of type $(\cdot, \lambda)$.

As before we see that (6.9) holds and $h(a_\rho^* b_\rho) \leqq N-1$, so substituting into (6.5), we find

$$(6.10)' \qquad \Sigma a_i'(b_1 + \Sigma y_{i\rho} b_\rho) + \Sigma u_j z_{j\rho} b_\rho \equiv 0 \quad (\text{mod } H^{N-1}).$$

Now by the maximality of $h_l(b_1)$, *either* every b_ρ of height n is left pure, *or* b_1 is not left pure. Assume the former holds, and that b_1 is of type $(1, \cdot)$, say.

Since $N = m + n$ and b_1 is left pure of type $(1, \cdot)$, a_1 cannot be right pure of type $(\cdot, 1)$ (by (6.2)), hence in (6.7)′ there occurs an a_i' of type $\neq (\cdot, 1)$. Taking such an a_i', of type $(\cdot, 2)$, say, and equating its coefficient in (6.10)′ to zero, we obtain

$$(6.11)' \qquad b_1 + \Sigma y_{1\rho} b_\rho \equiv 0 \quad (\text{mod}_2 H^n).$$

Each term $y_{1\rho} b_\rho$ may be expressed as a sum of terms of the same form which are left pure; for if $m_\rho = m$, then $n_\rho = n$ and b_ρ is then left pure by hypothesis. Thus we may again equate the terms of height n and type $(1, \cdot)$ in (6.11)′ and obtain

$$(6.12)' \qquad b_1 + \Sigma y_\rho' b_\rho \equiv 0 \quad (\text{mod } H^{n-1}),$$

from which (6.6), with $u = 1$ and $c_\rho = -y_\rho'$ follows without difficulty.

Next suppose that b_1 is not left pure; we still obtain (6.11)′, where now $(\cdot, 2)$ is any type occurring in a_1. This may be written as

$$b_1 = \Sigma - y_{i\rho} b_\rho + b_1^*,$$

where by (6.11)′, $h_l(b_1^*) < h_l(b_1)$; thus (6.6) again follows and the theorem is completely proved.

As a first application we show that right ideals in P are free P-modules.

THEOREM 6.3. *Let P be the free product of a family $(K_\lambda)_{\lambda \in \Lambda}$ of fields over a field k. Then any right ideal of P is a free P-module, with a right P-independent free generating set.*

Proof ([16]). Let I be a right ideal of P; we put $B_{-1/2} = \emptyset$ and for any half integer $n \geqq 0$ define B_n inductively as a right P-independent subset of I consisting of $B_{n-1/2}$ and right irreducible elements of right height n, and maximal subject to these conditions. The union $B = \bigcup B_n$ is still P-independent and it follows that the right ideal I' of P generated by B is free on B, as a right P-module. Since $B \subseteq I$, we have $I' \subseteq I$ and the theorem follows if we show that $I' = I$. Assume that $I' \neq I$ and let $a \in I$, $a \notin I'$ be such that $h_r(a)$ is minimal, say $h_r(a) = n$. Then a is right irreducible and since $a \notin B$, $B_n \cup \{a\}$ contains a right P-dependent subset, which must involve a. By Theorem 6.1, a is right P-dependent on B_n, i.e., there exist $b_i \in B_n$, $c_i \in P$ and a unit $u \in P$ such that

([16]) This is modelled on the proof of Theorem 3.3 of [4].

$$au = \sum b_i c_i + a', \quad \text{where } h_r(a') < h_r(a). \tag{6.13}$$

Now $a' = au - \sum b_i c_i \in I$, and by the minimality of $h_r(a)$, $a' \in I'$, hence (6.13) shows that $au \in I'$, and so $a \in I'$. This contradiction proves the theorem.

Next we develop the Euclidean algorithm in P. The result is as in §4, but a little more care is required in the proof, since the units do not all lie in the ground field.

LEMMA 6.4. *Let P be the free product of the family $(K_\lambda)_{\lambda \in \Lambda}$ of fields over a field k, and let $a, b, a', b' \in P$ be such that*

$$ab' = ba' \neq 0. \tag{6.14}$$

Then there exist elements $d, d', q_1, q_2, \cdots, q_{n+1} \in P$ such that (possibly after interchanging a with b and a' with b'),

$$a = df_{n+1}(q_{n+1}, \cdots, q_1), \qquad b = df_n(q_{n+1}, \cdots, q_2),$$
$$a' = f_{n+1}(q_1, \cdots, q_{n+1})d', \qquad b' = f_n(q_2, \cdots, q_{n+1})d',$$

where the f's are the continuant polynomials.

Proof. For any element $c \in P$ we define the *reduced right height* $\bar{h}_r(c)$ of c as $h_r(c_0)$, where c_0 is a right irreducible element right associated with c. This defines $\bar{h}_r(c)$ uniquely as a non-negative half integer (or $-\infty$) which vanishes if and only if c is a unit. Without loss of generality we may assume that $\bar{h}_r(a) \geqq \bar{h}_r(b)$ (by interchanging a with b and a' with b', if necessary). Now choose $q_1 \in P$ such that $\bar{h}_r(a - bq_1)$ has its least value and put

$$r_1 = a - bq_1, \qquad r_1' = a' - q_1 b'.$$

Then we clearly have

$$r_1 b' = b r_1'.$$

We assert that $\bar{h}_r(r_1) < \bar{h}_r(b)$; for if not, let $b = b_0 u$, $r_1 = r_{10} v$, where u, v are units and b_0, r_{10} right irreducible. Then $h_r(b_0) \leqq h_r(r_{10})$ and

$$r_{10} v b' = b_0 u r_1'.$$

Hence, by Theorem 6.1, $r_{10} w = b_0 p + s$, where w is a unit and $h_r(s) < h_r(r_{10})$. A fortiori, $\bar{h}_r(s) < h_r(r_{10})$ $(= \bar{h}_r(r_1))$, and

$$\begin{aligned} a &= bq_1 + r_1 \\ &= bq_1 + (b_0 p + s)w^{-1}v \\ &= b(q_1 + u^{-1} p w^{-1} v) + s w^{-1} v, \end{aligned}$$

but $\bar{h}_r(sw^{-1}v) = \bar{h}_r(s) < \bar{h}_r(r_1)$, in contradiction with the choice of q_1. Thus we have the equations

$$a = bq_1 + r_1, \qquad a' = q_1 b' + r_1', \qquad r_1 b' = b r_1',$$

where $\bar{h}_r(r_1) < \bar{h}_r(b)$. If $r_1 \neq 0$, we can continue the process and thus obtain a chain of equations as in (4.5), (4.5)′, such that

$$\bar{h}_r(a) \geqq \bar{h}_r(b) > \bar{h}_r(r_1) > \bar{h}_r(r_2) > \cdots > \bar{h}_r(r_n).$$

After a finite number of steps this chain breaks off, since $\bar{h}_r(c) \geqq 0$ for $c \neq 0$. Let n be the least integer such that $r_{n+1} = 0$, then as in §4 we have $r'_{n+1} = 0$, $r'_n \neq 0$, and the lemma follows if we put $d = r_n$, $d' = r'_n$.

We note that the quotients and remainders are no longer uniquely determined; in particular, if we had started by determining q_1 and r'_1 from a' and b' we might well have obtained different values. But this is immaterial for our purpose.

COROLLARY 1. *The free product of a family of fields over a field k is a weak Bezout ring.*

This follows in the same way as Theorem 4.1.

In [3, Theorem 3.1], it was shown that in a free product of two fields, the number of nonunits in any factorization of an element a (of positive height) cannot exceed the height of a. This theorem extends without any difficulty to the case of an arbitrary number of factors, and we therefore obtain

COROLLARY 2. *The free product of any family of fields over a field k is a unique factorization domain.*

In a similar way the other results of §4 (Theorem 4.1, Corollary 3, Theorem 4.2 and Propositions 4.3–4.4) may be established for the free product of fields.

REFERENCES

1. A. C. Aitken, *Determinants and matrices*, 3rd ed., Oliver and Boyd, Edinburgh, 1944.

2. P. M. Cohn, *On the free product of associative rings*, Math. Z. **71** (1959), 380–398.

3. ———, *On the free product of associative rings*. II, Math. Z. **73** (1960), 433–456.

4. ———, *On a generalization of the Euclidean algorithm*, Proc. Cambridge Philos. Soc. **57** (1961), 18–30.

5. ———, *Factorization in non-commutative power series rings*, Proc. Cambridge Philos. Soc. **58** (1962), 452–464.

6. ———, *Noncommutative unique factorization domains*, Trans. Amer. Math. Soc. **109** (1963), 313–331.

7. G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, 2nd ed., Clarendon, Oxford, 1945.

8. N. Jacobson, *A note on non-commutative polynomials*, Ann. of Math. (2) **35** (1934), 209–210.

9. ———, *Theory of rings*, Amer. Math. Soc., Providence, R. I., 1943.

10. J. M. H. Wedderburn, *Non-commutative domains of integrity*, J. Reine Angew. Math. **167** (1932), 129–141.

YALE UNIVERSITY,
NEW HAVEN, CONNECTICUT
UNIVERSITY OF MANCHESTER,
MANCHESTER, ENGLAND
QUEEN MARY COLLEGE, UNIVERSITY OF LONDON,
LONDON, ENGLAND