NONCOMMUTATIVE UNIQUE FACTORIZATION DOMAINS(1)

BY
P. M. COHN

1. **Introduction.** By a (commutative) unique factorization domain (UFD) one usually understands an integral domain R (with a unit-element) satisfying the following three conditions (cf. e.g. Zariski-Samuel [16]):

A1. *Every element of R which is neither zero nor a unit is a product of primes.*

A2. *Any two prime factorizations of a given element have the same number of factors.*

A3. *The primes occurring in any factorization of a are completely determined by a, except for their order and for multiplication by units.*

If R^* denotes the semigroup of nonzero elements of R and U is the group of units, then the classes of associated elements form a semigroup R^*/U, and A1–3 are equivalent to

B. *The semigroup R^*/U is free commutative.*

One may generalize the notion of UFD to noncommutative rings by taking either A–13 or B as starting point. It is obvious how to do this in case B, although the class of rings obtained is rather narrow and does not even include all the commutative UFD's. This is indicated briefly in §7, where examples are also given of noncommutative rings satisfying the definition.

However, our principal aim is to give a definition of a noncommutative UFD which includes the commutative case. Here it is better to start from A1–3; in order to find the precise form which such a definition should take we consider the simplest case, that of noncommutative principal ideal domains. For these rings one obtains a unique factorization theorem simply by reinterpreting the Jordan-Hölder theorem for right R-modules on one generator (cf. Jacobson [10] and the references given there). This leads to the notion of *similarity*, two elements a, b of R being similar if $R/aR \cong R/bR$, as R-modules. Now A1–3 can be taken over in the noncommutative case, except that in A3, corresponding primes are required to be similar, rather than associated. This is carried out in §2, together with some immediate consequences of the definitions.

Another very natural way of defining commutative UFD's is in terms of the

Received by the editors October 15, 1962.

(1) This research was supported by a National Science Foundation Grant No. NSF G-19137.

lattice of principal ideals. This leads to the consideration of HCF-rings (Jaffard [11]); their relation to UFD's is examined in §3. The main result here is a refinement theorem of the Schreier type (Theorem 3.2), from which the unique factorization property may be deduced for any elements which have a prime decomposition. The proof hinges on the fact that the principal right ideals form a modular lattice. While this follows from the existence of the HCF in the commutative case, in general it has to be assumed explicitly. However, there is one case in which the principal right ideals automatically form a modular lattice, namely, when they are a sublattice of the lattice of all right ideals. An integral domain with this property is called a *right Bezout ring* and its properties and relations to HCF-rings and UFD's are studied in §4.

For the applications it is of importance to consider a wider class, the *weak Bezout rings*; these are integral domains, in which the principal right ideals containing a given nonzero principal right ideal form a sublattice of the lattice of all right ideals. These rings form in many ways a more interesting class than the right Bezout rings. In the first place, it is shown that the definition is left-right symmetric (Proposition 5.1). Secondly, although a weak Bezout ring need not be a right HCF-ring, the refinement theorem still holds (Theorem 5.5), and for weak Bezout rings which are UFD's, several decomposition theorems hold (Theorems 5.7–5.8), analogous to the primary decomposition of an ideal in a commutative Noetherian ring. This generalizes and simplifies some results obtained by Ore for skew polynomial rings over fields [14]. And thirdly it may be shown that weak Bezout rings include many important classes of rings, in particular, (1) free associative algebras over a field, (2) tensor rings over k-bimodules, and (3) free products of skew fields over k, where k is a given skew field. Case (1) is established in §6, while (2) and (3) will be dealt with in another communication [6].

2. **Definition of a UFD.** Throughout, all rings will be associative, with a unit-element, denoted by 1. By an *integral domain* we understand a ring (not necessarily commutative) in which $1 \neq 0$, and without zero-divisors(2). Thus in an integral domain R, the nonzero elements form a semigroup under multiplication which will be denoted by R^*. We recall that in an integral domain any element with a right (or left) inverse is necessarily a unit.

Two elements a, b of a ring R are said to be *associated*, if $b = uav$, where u, v are units in R. A *prime* in R is a nonunit which is not a product of two nonunits. Clearly, if a is prime, or a unit, or zero, then so is any element associated to a.

Two elements a, b of R are said to be *right similar*, if $R/aR \cong R/bR$, as right R-modules (Jacobson [10, p. 33]). From the definition it is clear that right similarity is a reflexive, symmetric and transitive relation. The notion of left similarity may be defined in an analogous fashion; however, in an integral domain this is equivalent to right similarity, as follows from a more general result of Fitting [7]. We

(2) By convention we do not reckon zero among the zero-divisors.

shall prove this directly by means of a lemma, which will be needed again later. We recall that an $n \times n$ matrix over a ring R is called *unimodular*, if it is a unit in R_n.

LEMMA. *Two elements a, b of an integral domain R may be taken as the first row of a unimodular matrix over R if and only if a and b have an LCRM and an HCLF*([3]), *the latter being a unit. More precisely, if $aR \cap bR = mR$, say, and*

$$ab' = ba' = m, \tag{2.1}$$

$$ad' - bc' = 1, \tag{2.2}$$

then there exist $c, d \in R$ such that the matrix

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \tag{2.3}$$

is unimodular, with the inverse

$$A' = \begin{pmatrix} d' & -b' \\ -c' & a' \end{pmatrix}. \tag{2.4}$$

Proof. Suppose that (2.1) and (2.2) hold, where m is an LCRM of a and b. Then by (2.2), $ad'a - bc'a = a$, i.e., $a(d'a - 1) = bc'a$, hence, there exists $c \in R$ such that

$$d'a - 1 = b'c, \qquad c'a = a'c; \tag{2.5}$$

similarly, $ad'b - bc'b = b$, i.e., $ad'b = b(c'b + 1)$, which gives

$$d'b = b'd, \qquad c'b + 1 = a'd \tag{2.6}$$

for some $d \in R$. If we define A, A' as in (2.3) and (2.4), then (2.5) and (2.6) just state that $A'A = I$, and to show that $AA' = I$ we need only verify that A' is not a left zero-divisor. Thus, assume that

$$A'\begin{pmatrix} x \\ y \end{pmatrix} = 0,$$

i.e., $d'x = b'y$, $c'x = a'y$. By (2.2) we have

$$x = ad'x - bc'x = ab'y - ba'y = 0,$$

hence, $x = 0$ and $a'y = b'y = 0$. Suppose that $y \neq 0$, then $a' = b' = 0$ and hence, by (2.5–2.6), $d'a = 1$, $c'b = -1$. It follows that $ad' = 1$, $bc' = -1$ and so $ad' - bc' = 2$, which contradicts (2.2). Hence, $y = 0$ and this shows A' to be inverse to A.

([3]) Any ring may be preordered by the relation "a is a right factor of b", and the terms 'least common right multiple (LCRM)' and 'highest common left factor (HCLF)' are interpreted in the sense of this preordering. The terms 'LCLM' and 'HCRF' are defined analogously in terms of the preordering by left divisibility.

Conversely, if A, given by (2.3), is unimodular, with inverse A' given by (2.4), then $ad'-bc'=1$, hence, $aR+bR=R$. Now let $ab'=ba'=m$ and let $n\in aR\cap bR$, say $n=ab_1=ba_1$. Put $da_1-cb_1=k$, then

$$A\begin{pmatrix}-b_1\\ a_1\end{pmatrix}=\begin{pmatrix}0\\ k\end{pmatrix},$$

hence,

$$\begin{pmatrix}-b_1\\ a_1\end{pmatrix}=A'\begin{pmatrix}0\\ k\end{pmatrix}=\begin{pmatrix}-b'k\\ a'k\end{pmatrix};$$

which shows that $n=mk$.

We now have the following condition for a and b to be right similar (cf. Jacobson [10, p. 33] for the case of principal ideal domains).

PROPOSITION 2.1. *Two nonzero elements a, a' in an integral domain R are right similar if and only if there exist b, b', c', $d'\in R$ such that*

$$ad'-bc'=1 \tag{2.7}$$

and

$$ab'=ba' \tag{2.8}$$

is an LCRM of a and b.

The proof in [10] still applies; we reproduce it for completeness. Thus assume that $R/aR\cong R/a'R$ and in the isomorphism, let

$$1+a'R\to b+aR. \tag{2.9}$$

Since $1a'=a'+a'R$, we must have $ba'\in aR$, hence,

$$ba'=ab' \tag{2.10}$$

for some $b'\in R$. Moreover, since $a'R$ is the precise annihilator of $1+a'R$,

$$ba_1=ab_1 \text{ implies } a_1\in a'R, \tag{2.11}$$

which means that ba' is an LCRM of a and b. Further, $b+aR$ generates R/aR, so there exist c', $d'\in R$ such that (2.7) holds. Conversely, if (2.7), (2.10) and (2.11) hold, then the mapping (2.9) defines a homomorphism (by (2.10)), which is 1-1 by (2.11) and onto by (2.7).

COROLLARY 1 (FITTING [7]). *Two elements in an integral domain are right similar if and only if they are left similar.*

This is trivial if one of the elements is zero. Otherwise, by combining the proposition with the lemma preceding it, we see that a, a' are right similar if and

only if there exist b, c, d, b', c', d' such that the matrices A, A' given by (2.3) and (2.4) are mutually inverse. But this is a left-right symmetric condition and so the corollary follows.

As we shall be dealing exclusively with integral domains in the sequel, we may omit the reference to left or right and simply speak of similar elements.

COROLLARY 2. *An element of an integral domain is similar to any of its associates.*

For if $a' = uav$, where u, v are units, then a is an LCRM of u^{-1} and a, and we have $u^{-1} \cdot uav = av$ and $a \cdot 0 + u^{-1} \cdot u = 1$.

An element a of an integral domain R is a unit if and only if R/aR is the zero-module, a is prime if and only if R/aR has no cyclic submodules other than 0 or itself and $a = 0$ if and only if every nonzero element of R/aR has zero annihilator. It follows that if a is a unit, prime or zero, then so is any element similar to a. The first two assertions are special cases of Proposition 2.2 below.

Let $a, b \in R$ and consider any factorizations of a and b:

$$a = u_1 u_2 \cdots u_r, \tag{2.12}$$

$$b = v_1 v_2 \cdots v_s. \tag{2.13}$$

These factorizations are said to be *isomorphic*, if $r = s$ and there is a permutation π of $(1, \cdots, r)$ such that u_i is similar to $v_{i\pi}$.

PROPOSITION 2.2. *Let a, b be nonzero elements of an integral domain R which are similar. Then any factorization of a gives rise to an isomorphic factorization of b.*

For a factorization of a may be regarded as a chain of cyclic submodules from R to aR, and by the isomorphism $R/aR \cong R/bR$ this gives a chain from R to bR, in which corresponding factors are isomorphic.

We can now state the basic

DEFINITION. A *unique factorization domain* (UFD for short) is an integral domain R such that every nonunit of R^* has a factorization into primes and any two prime factorizations of a given element are isomorphic.

Our first task is to show that this reduces to A1–3 in the commutative case.

THEOREM 2.3. *A commutative integral domain is a UFD if and only if it satisfies* A1–3 *of* §1.

This amounts to showing that in a commutative integral domain R,

$$R/aR \cong R/bR \tag{2.14}$$

holds if and only if a and b are associated. If a and b are associated, then $aR = bR$

and (2.14) clearly holds in this case. Conversely, assume (2.14), then $b + aR$ maps to 0 in the isomorphism and hence, $b \in aR$. Thus $bR \subseteq aR$, and by symmetry $aR \subseteq bR$, and so $aR = bR$, from which the result follows.

As an example of a noncommutative UFD we mention noncommutative principal ideal domains (Jacobson [10, Chapter 3]). This includes in particular the skew polynomial rings([4]) studied by Ore [14] and the ring of integral quaternions. Other examples will be given later (§6).

The existence condition A1 may be separated from the uniqueness conditions A2–3 for rings in which a refinement theorem of the Schreier type([5]) holds. Given two factorizations of the same element a, say (2.12) and (2.13), where now $b = a$, we say that (2.13) is a *refinement* of (2.12) if it is obtained from (2.12) by replacing each u_i by some factorization of itself. A factorization is said to be *proper* if no factor is a unit. Clearly, if two factorizations of a are isomorphic, then by absorbing the units (into their neighbours) we obtain two proper factorizations of a which are still isomorphic. Now we note that in a UFD R, any two factorizations of an element of R^* have isomorphic refinements. We need only decompose each nonunit occuring in the two factorizations into primes; the refinements so obtained are then isomorphic, provided we insert an appropriate number of unit factors so as to get the same number of factors in the two factorizations. As a converse we have

THEOREM 2.4. *Let R be an integral domain such that any two factorizations of an element of R^* have isomorphic refinements. Then any two prime factorizations of a given element of R^* are isomorphic, and if a is an element of R^* possessing a prime factorization, then any proper factorization of a has a refinement with prime factors. In particular, if every nonunit of R^* has at least one prime factorization, then R is a UFD.*

Proof. Let

$$a = p_1 p_2 \cdots p_r, \tag{2.15}$$

$$a = q_1 q_2 \cdots q_s, \tag{2.16}$$

be two prime factorizations of a. By hypothesis these have isomorphic refinements. But in any factorization of p_i or q_j, all but one of the factors must be units. Since all units are similar among themselves, but not similar to any prime, we may disregard them. Hence $r = s$ and for some permutation π, p_i is similar to an associate of $q_{i\pi}$; now by Proposition 2.1, Corollary 2, p_i is similar to $q_{i\pi}$. Further, if a has a prime factorization with r factors, then no factorization of a can have

---

([4]) More precisely, the skew polynomial rings defined by an automorphism of the underlying field. In the general case (of an endomorphism) one has a right principal domain. But it follows from later results (Theorem 5.5, Corollary 1) that this is still a UFD.

([5]) Cf. Schreier [15].

more than r nonunit factors, from which it follows that any proper factorization of a has a refinement with prime factors. The last assertion is an immediate consequence of this fact.

3. **HCF-rings.** Commutative UFD's may be characterized in yet another way Let R be any commutative integral domain and K its field of fractions, then the fractional principal ideals form a partially ordered group G. If G is actually lattice-ordered, R is said to be an HCF-ring (Jaffard [11, p. 78]); this is equivalent to the condition that any two nonzero elements of R have an HCF. Clearly, R is a UFD if and only if G is a free abelian group. Now we have

THEOREM 3.1. *A (commutative) HCF-ring R is a UFD if and only if every nonunit in R^* has a prime factorization.*

This is just the well-known result that an abelian l-group is free abelian if and only if every bounded chain is finite (cf. Bourbaki [2, §1, No. 13, Théorème 2]).

If we want to extend this result to the noncommutative case, we have to take account of the fact that in a noncommutative integral domain R, the principal right ideals in general do not even form a semigroup(6). However, they still form a (partially) ordered set, with respect to inclusion, and so we make the following

DEFINITION. An integral domain R is said to be a *right HCF-ring* if the set of all principal right ideals of R is a modular lattice with respect to the ordering by inclusion.

In case R is commutative this clearly reduces to the definition of HCF-ring given earlier. Since in any modular lattice the Schreier refinement theorem holds (Birkhoff [1, Chapter V, Theorem 5, Corollary, p. 72]), we obtain

THEOREM 3.2. (REFINEMENT THEOREM FOR RIGHT HCF-RINGS). *In a right HCF-ring R, any two factorizations of an element in R have isomorphic refinements.*

Applying Theorem 2.4, we obtain the

COROLLARY. *A right HCF-ring R is a UFD if and only if every nonunit in R^* has a prime factorization.*

If in this corollary we take R to be commutative, we obtain an independent proof of Theorem 3.1. It is easy to give examples of right HCF-rings which are not UFD's (cf. §4). We shall also meet examples (in §5) of UFD's which are not right HCF-rings.

In conclusion we note that a right HCF-ring can always be embedded in a skew field. More precisely, we have

THEOREM 3.3. *Any right HCF-ring R has a skew field K of right quotients, i.e., there is a field K containing R such that all the elements of K are of the form ab^{-1}, where $a \in R$, $b \in R^*$.*

(6) We cannot speak of a group since R need not be embeddable in a skew field.

Proof. By definition, R is an integral domain, so we need only show that R satisfies the right multiple condition of Ore [13]:

$$aR \cap bR \neq 0 \qquad \text{for all } a, b \in R^*. \tag{3.3}$$

By hypothesis there exist $m, d \in R$ such that $aR \cap bR = mR$, $aR \cup bR = dR$, hence, by modularity,

$$aR/mR \cong dR/bR. \tag{3.4}$$

Let $m = ab'$, $b = db_0$, then (3.4) may be rewritten as

$$R/b'R \cong R/b_0R,$$

because $a, d \neq 0$. Hence, b' is right similar to b_0, which is not zero. Therefore, $b' \neq 0$ and so $m \neq 0$, i.e., $aR \cap bR \neq 0$ and (3.3) follows.

4. **Bezout rings.** An integral domain R is said to be a *right Bezout ring*, if for any two principal right ideals, their sum and intersection are again principal. *Left Bezout rings* are defined similarly, and a ring which is both left and right Bezout is called a *Bezout ring*.

As an example of a right Bezout ring which is not a Bezout ring we take a field F with an endomorphism σ which is not an automorphism of F, and define the associated ring $F[x;\sigma]$ of skew polynomials in an indeterminate x by the commutation formula

$$ax = xa^\sigma \qquad (a \in F)$$

(cf. Ore [14]). Every right ideal of this ring is principal, hence, it is a right Bezout ring; but if $a \notin F^\sigma$, then the left ideal generated by x and xa is not principal.

We note in passing that Bezout rings form the precise class of integral domains over which every rectangular matrix admits a triangular reduction (cf. Kaplansky [12, Theorem 3.4]; in the terminology used there, a Bezout ring is an Hermite ring without zero-divisors).

It is clear that in a right Bezout ring the principal right ideals form a lattice; in fact, by definition they form a sublattice of the lattice of all right ideals. Since this lattice is modular, we have

THEOREM 4.1. *A right Bezout ring is a right HCF-ring.*

By Theorem 3.2 we deduce the

COROLLARY. *The refinement theorem holds for right Bezout rings.*

Theorem 4.1 shows, in particular, that a commutative Bezout ring is an HCF-ring. Now in the commutative case the existence of an HCF of any two elements

is already enough to ensure the existence of an LCM, because every semi-lattice-ordered group is necessarily a lattice-ordered group. Whether the definition of a right Bezout ring can be weakened in the same way is not known, but for two-sided Bezout rings this is so. We have([7])

THEOREM 4.2. *An integral domain R is a Bezout ring if and only if the sum of any two principal right ideals or any two principal left ideals is again principal.*

Proof. The necessity is clear; for the sufficiency it is enough to prove, by symmetry, that the intersection of any two principal right ideals is again principal. Thus given $a, b \in R$, we have to show the existence of $m \in R$ such that $aR \cap bR = mR$; we may assume that $a, b \neq 0$, without loss of generality. We begin by proving that Ore's right multiple condition (3.3) holds. By hypothesis we have $aR + bR = dR$, say

$$a = da_0,\ b = db_0 \text{ and } a_0v - b_0u = 1. \tag{4.1}$$

Either u or v is nonzero, say $u \neq 0$, then multiplying the last equation in (4.1) by a_0 on the right, we find $a_0(va_0 - 1) = b_0ua_0 \neq 0$, and multiplying by d on the left we see that $aR \cap bR \neq 0$; by symmetry we also have $Ra \cap Rb \neq 0$. Thus given $a, b \in R^*$, there exist $a', b' \in R$ such that

$$ab' = ba' \neq 0.$$

Let $Ra' + Rb' = Rd'$, then dividing a', b' by d' on the right, we obtain a common right multiple of a, b:

$$m = ab_1 = ba_1 \text{ say, where } ya_1 - xb_1 = 1 \text{ for some } x, y \in R. \tag{4.2}$$

We assert that

$$mR = aR \cap bR. \tag{4.3}$$

Clearly $mR \subseteq aR \cap bR$ by (4.2); conversely, let $n \in aR \cap bR$, say

$$n = ab_2 = ba_2.$$

If $b_1R + b_2R = b^*R$, then there exist $c_1, c_2, p, q \in R$ such that

$$b_1 = b^*c_1,\quad b_2 = b^*c_2,\quad b_1q - b_2p = b^*. \tag{4.4}$$

Hence,

$$ab^* = a(b_1q - b_2p) = mq - np = b(a_1q - a_2p);$$

using this to transform (4.2), we get

$$ba_1 = ab_1 = ab^*c_1 = b(a_1q - a_2p)c_1,$$

([7]) This result has also been obtained (independently) by S. A. Amitsur.

whence

$$a_1 = (a_1q - a_2p)c_1. \tag{4.5}$$

Inserting from (4.4) and (4.5) into (4.2) we find

$$(y(a_1q - a_2p) - xb^*)c_1 = 1.$$

Hence, c_1 is a unit and putting $z = c_1^{-1}c_2$, we have from (4.4), $b_2 = b_1z$, whence $n = mz$. Hence, $n \in mR$, as we wished to prove.

COROLLARY 1([8]). *A commutative integral domain in which the sum of any two principal ideals is principal, is a Bezout ring.*

It may also be noted that the property of being a Bezout ring is "of local character." We recall that if P is any property of rings, then a ring R is said to be *locally* P, if it has a *local system* of subrings satisfying P, that is a family (R_λ) $(\lambda \in \Lambda)$ of subrings having P, such that

(i) (R_λ) is directed by inclusion: given R_λ, R_μ there exists R_ν in the family such that $R_\nu \supseteq R_\lambda \cup R_\mu$,

(ii) $\bigcup R_\lambda = R$.

If a ring has P whenever it has P locally, then P is said to be a property of *local character*.

COROLLARY 2. *The property of being a Bezout ring is of local character.*

For let R be a ring with a local system (R_λ) of Bezout subrings. Then no element of R can be a zero-divisor. Given $a, b \in R$, there exists a Bezout subring R_0 containing a, b and hence we can find d, a_0, b_0, u, $v \in R_0$ such that

$$a = da_0, \quad b = db_0, \quad a_0v - b_0u = 1. \tag{4.6}$$

It follows from (4.6) that $aR + bR = dR$; similarly $Ra + Rb = Rd'$, for some d' and the result follows.

In the proof of this corollary we made essential use of Theorem 4.2; thus it is not obvious at this stage that the property of being a right Bezout ring has local character, but we shall see later (§5) that this is so.

Since a principal ideal domain is clearly a Bezout ring, we obtain

COROLLARY 3. *A locally principal ideal domain is a Bezout ring.*

We remark that in fact every locally principal ideal domain is an elementary divisor ring in the sense of Kaplansky [12]. Whether every Bezout ring is a locally principal ideal domain (or at least an elementary divisor ring) remains open, although Theorem 4.2 suggests that the answer is affirmative.

As an example of an HCF-ring which is not a UFD, consider the semigroup

([8]) This answers a question raised by Gillman and Henriksen [8] who give an example (in [9]) to show that this corollary does not remain true when zero-divisors are admitted.

ring over a field F of the additive semigroup of positive rationals. This is a locally principal ideal domain and hence a Bezout ring. Therefore it is an HCF-ring and the refinement theorem (Theorem 3.2) applies. However, it is not a UFD, since it contains no primes, as is easily seen.

5. **Weak Bezout rings.** The Bezout rings defined in §4 do not differ very much from principal ideal domains, also they fail to take account of such important UFD's as the polynomial rings in several indeterminates over a field. Further, in the noncommutative case, the distinction arises between left and right Bezout rings. We now introduce a class of rings which in the commutative case reduces to Bezout rings (and so gives nothing new there) but in the noncommutative case it is considerably wider, in that it includes, e.g., free associative algebras over a field (§6). Moreover, the definition, although expressed in terms of right ideals, is left-right symmetric. We begin by proving

PROPOSITION 5.1. *In any integral domain the following two conditions are equivalent*:

(i) *Any two principal right ideals with nonzero intersection have a sum and intersection which are again principal.*

(ii) *Any two principal left ideals with nonzero intersection have a sum and intersection which are again principal.*

Proof. By symmetry it is enough to show that (i) implies (ii). Let $a_1, b_1 \in R$ be such that $Ra_1 \cap Rb_1 \neq 0$, say

$$ab_1 = ba_1 \neq 0. \tag{5.1}$$

By hypothesis a and b have an HCLF; dividing out by this we may assume that

$$aR + bR = R; \tag{5.2}$$

further, a and b have an LCRM, say

$$aR \cap bR = mR. \tag{5.3}$$

Hence, $ab_1 = mk$ for some $k \in R$, and if we put $m = ab' = ba'$, then

$$b_1 = b'k, \quad a_1 = a'k.$$

Now by the lemma of §2, there exist $c, d, c', d' \in R$ such that

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \qquad A^{-1} = \begin{pmatrix} d' & -b' \\ -c' & a' \end{pmatrix}.$$

Hence a', b' satisfy

$$Ra' + Rb' = R, \qquad Ra' \cap Rb' = Rab'.$$

Multiplying by k on the right, we obtain

$$Ra_1 + Rb_1 = Rk, \qquad Ra_1 \cap Rb_1 = Rab_1.$$

Thus (ii) holds, and the result is established.

An integral domain satisfying the conditions (i) or (ii) of Proposition 5.1 is called a *weak Bezout ring*. Clearly this includes both left and right Bezout rings; more precisely, we have

THEOREM 5.2. *For any ring R the following three conditions are equivalent:*

1. *R is a right Bezout ring.*
2. *R is a weak Bezout ring which is also a right HCF-ring.*
3. *R is a weak Bezout ring which satisfies Ore's right multiple condition.*

Proof. 1. $\Rightarrow$ 2. follows by Theorem 4.1, 2. $\Rightarrow$ 3. follows by Theorem 3.3, and finally 3. $\Rightarrow$ 1. is immediate from the definitions.

In particular, a weak Bezout ring is Bezout if and only if it is left and right Bezout; thus the example given at the beginning of §4 is a weak Bezout ring (by Theorem 5.2) but not a Bezout ring. We also see from Theorem 5.2 that a weak Bezout ring need not be a right (or left) HCF-ring, but even when it is not, it may still be a UFD. Thus in §6 we shall meet examples of weak Bezout rings which are UFD's, but not HCF-rings; as a matter of fact, in the example given (free associative algebras) an HCLF, HCRF, LCRM and LCLM of any two elements exists, but the rings fail to be HCF-rings, because the lattice of principal right ideals is not modular.

In a weak Bezout ring there is a simple criterion for similarity which is left-right symmetric. In any ring R, the products ab' and ba' are said to be *right coprime*, if a', b' have no common right factor apart from units, and *left coprime* if a, b have no common left factor apart from units. They are called *coprime* if they are both left and right coprime. Now we have

PROPOSITION 5.3. *In a weak Bezout ring R, two elements a, a' are similar if and only if there exist b, $b' \in R^*$ such that*

$$ab' = ba', \tag{5.4}$$

where the two sides of (5.4) *are coprime.*

Proof. If a, a' are similar, then by Proposition 2.1 we have a relation (5.4), where a, b are left coprime by (2.7) and a', b' are right coprime because (5.4) is an LCRM of a and b. Conversely, if (5.4) holds and the two sides are coprime, then $aR + bR = R$ and $aR \cap bR = ab'R$, and so a and a' are similar, again by Proposition 2.1.

Before studying the relation with UFD's we note the local character of weak Bezout rings.

THEOREM 5.4. *The property of being a weak Bezout ring is of local character.*

Proof. Let R be locally weak Bezout and let (R_λ) be a local system of weak Bezout subrings. Given $a, b \in R$ such that $aR \cap bR \neq 0$, we have

$$ab' = ba' \neq 0, \tag{5.5}$$

say. Let R_0 be a weak Bezout subring of R containing a, b, a', b'. Then there exist $d, a_0, b_0, u', v' \in R_0$ such that

$$a = da_0, \qquad b = db_0, \qquad a_0v' - b_0u' = 1. \tag{5.6}$$

Further, we may assume that a', b' have no common right factor in R_0 apart from units (by dividing out in (5.5), if necessary). Then there exist $u, v \in R_0$ such that

$$va' - ub' = 1. \tag{5.7}$$

From (5.6) we have $aR + bR = dR$; we complete the proof by showing that $aR \cap bR = mR$, where $m = ab' = ba'$. Thus $mR \subseteq aR \cap bR$ follows from (5.5); conversely, if $n = ab_1 = ba_1$, let R_1 be a weak Bezout subring of R containing R_0, a_1 and b_1. Then in R_1, a and b have an LCRM $ab_2 = ba_2$ say, and m must be a right multiple of this, i.e., $a' = a_2z$, $b' = b_2z$ for some $z \in R_1$. Inserting this in (5.7) we obtain

$$(va_2 - ub_2)z = 1.$$

Hence z is a unit and so m is an LCRM of a, b in R_1. It follows that n is a right multiple of m and since n was any element of $aR \cap bR$, this proves that $aR \cap bR = mR$; hence, R is a weak Bezout ring.

COROLLARY. *The property of being a right Bezout ring is of local character.*

For by Theorem 5.2, R is right Bezout if and only if it is weak Bezout and satisfies Ore's right multiple condition, and both these conditions have local character.

In §3 the property of being a UFD was established by means of the refinement theorem (Theorem 3.2) which was proved there for right HCF-rings. This result cannot be applied here because a weak Bezout ring is in general neither a left nor a right HCF-ring. Nevertheless, the refinement theorem still holds; in fact, if we examine the proof of Theorem 3.2 we see that it does not use the full force of the hypothesis that the principal right ideals form a lattice.

THEOREM 5.5 (REFINEMENT THEOREM FOR WEAK BEZOUT RINGS). *In a weak Bezout ring any two factorizations of a nonzero element have isomorphic refinements.*

Proof. Let R be a weak Bezout ring and $a \in R^*$, then the principal right ideals containing aR form a modular lattice and so by the Schreier refinement theorem for modular lattices any two factorizations have right isomorphic refinements. By Proposition 5.3 these are actually isomorphic.

As for Theorem 3.2 we have

COROLLARY 1. *A weak Bezout ring R is a UFD if and only if every nonunit in R has a prime factorization.*

We note that Theorem 5.5 and its corollary apply in particular to right Bezout rings, giving a generalization of the corollary to Theorem 4.4.

We now turn to consider the analogues of the primary decomposition of an ideal in a (commutative) Noetherian ring. If we confine our attention to principal right ideals we actually obtain two analogues which in the case of skew polynomial rings were considered by Ore [14].

An element a of a ring R is said to be (*left, right*) *decomposable* if it has two proper factorizations

$$a = bc' = cb',$$

which are (left, right) coprime. Clearly any decomposable element is both right and left decomposable; hence, an element which is either right or left indecomposable is indecomposable. In a weak Bezout ring these definitions may be rephrased as follows:

(i) $a \in R$ is right decomposable if and only if there exist $b, c \in R$ such that $aR = bR \cap cR$, where $aR \neq bR, cR$.

(ii) $a \in R$ is decomposable if and only if there exist $b, c \in R$ such that $aR = bR \cap cR$ and $bR + cR = R$, where $aR \neq bR, cR$.

Our first object is to show that decomposability is preserved under passage to similar elements. This is most easily done by expressing the decomposability of a as a condition on R/aR. Let us call an R-module *strictly cyclic*, if it has one generator and one defining relation (which is not redundant). Thus a strictly cyclic module (over an integral domain) is one of the form R/aR, where $a \neq 0$ (but a may be a unit).

PROPOSITION 5.6. *Let R be a weak Bezout ring; then an element a of R is right decomposable if and only if R/aR is an irredundant subdirect sum of two strictly cyclic R-modules, and a is decomposable if and only if R/aR is a direct sum of two nonzero strictly cyclic R-modules. In particular, if a is (left, right) decomposable so is any element similar to a.*

Proof. Let a be right decomposable, say $aR = bR \cap cR$, where $aR \neq bR, cR$. Then there is a monomorphism

$$R/aR \to R/bR \oplus R/cR; \tag{5.8}$$

the result of composing this with the projection onto either of the summands is onto, but neither is 1:1, hence R/aR is an irredundant subdirect sum of R/bR and R/cR. Conversely, given any irredundant subdirect sum representation of R/aR, let R/bR, R/cR be the kernels of the projections, then $bR \cap cR = aR$ and $aR \neq bR$, cR.

Next let a be decomposable, then we have

$$R/aR = (bR + cR)/aR \cong bR/aR \oplus cR/aR,$$

where the last sum is direct because $bR \cap cR = aR$, and neither summand is zero. The converse is clear.

Let R be a weak Bezout ring and $a \in R^*$, then by a *complete decomposition* of aR we mean an irredundant representation

$$aR = b_1R \cap \cdots \cap b_nR, \tag{5.9}$$

where each b_i is right indecomposable. Similarly, a *complete direct decomposition* of aR is an irredundant representation (5.9), where each b_i is indecomposable and such that

$$b_iR \neq R, \qquad b_iR + \left(\bigcap_{j\neq i} b_jR\right) = R \qquad (i = 1, \cdots, n).$$

For these two types of decomposition we have the following uniqueness theorems.

THEOREM 5.7. *Let R be a weak Bezout ring which is also a UFD. Then for every element a of R^*, aR has a complete decomposition*

$$aR = b_1R \cap \cdots \cap b_nR, \tag{5.10}$$

and if a second complete decomposition of aR is given,

$$aR = c_1R \cap \cdots \cap c_mR, \tag{5.11}$$

then $m = n$ and the c_iR may be exchanged against the b_jR, i.e., after suitably renumbering the c's, we have, for $i = 1, \cdots, n$,

$$aR = b_1R \cap \cdots \cap b_iR \cap c_{i+1}R \cap \cdots \cap c_nR.$$

Proof. The principal right ideals of R which contain aR form a modular lattice which has finite length, by hypothesis. The theorem is therefore just a restatement of the Kuroš-Ore theorem (Birkhoff [1, p. 93]).

THEOREM 5.8. *Let R be a weak Bezout ring which is also a UFD. Then for every element a of R^*, aR has a complete direct decomposition* (5.10) *and if a second complete direct decomposition* (5.11) *is given, then $m = n$ and the b's and c's are similar in pairs.*

This follows in the same way as Theorem 5.7 from the Krull-Schmidt theorem for modular lattices of finite length (Ore's theorem; cf. Birkhoff [1, p. 94].

6. **Examples of weak Bezout rings.** As obvious examples of weak Bezout rings we have principal ideal domains, commutative or not, and more generally, left or right Bezout rings. In order to obtain a wider class we first note the following characterization of commutative principal ideal domains.

PROPOSITION 6.1. *A commutative integral domain R is a principal ideal domain if and only if every ideal of R is a free R-module.*

For in a commutative principal ideal domain every ideal is a free R-module, on 0 generators or 1, according as it is or is not 0. Conversely, if every ideal of R is free, let I be an ideal of R and suppose that I is not principal. Then I has a basis with more than one element, say $a_0 \neq a_1$; now $a_0a_1 - a_1a_0 = 0$ is a non-trivial relation between these elements, which contradicts the basis property. Hence every ideal of R is principal and the result follows.

Proposition 6.1 suggests considering in the noncommutative case, integral domains R whose right ideals are all free R-modules. Whether every such ring is a weak Bezout ring we do not know, but we can assert this with a supplementary condition.

THEOREM 6.2(9). *An integral domain R is a weak Bezout ring provided the following two conditions are satisfied*:

(i) *All right ideals of R are free R-modules.*

(ii) *Any two free bases of a free right R-module have the same cardinal.*

Proof. In any integral domain R we have, for any $a, b \in R$, the following exact sequence of right R-modules:

$$0 \to aR \cap bR \xrightarrow{\lambda} aR \oplus bR \xrightarrow{\mu} aR + bR \to 0. \tag{6.1}$$

The mappings λ and μ are given as follows: if $m = ax = by \in aR \cap bR$, then $m\lambda = (ax, by)$ and $(ax, by)\mu = ax - by$. With these definitions the exactness of (6.1) is immediate. By hypothesis (i) all the terms of this sequence are free R-modules, therefore the sequence splits. Now (ii) states that the cardinal of any basis of a free R-module M is an invariant of M, which we denote by $r(M)$. In view of the splitting of (6.1) we have

$$r(aR \cap bR) + r(aR + bR) = r(aR \oplus bR). \tag{6.2}$$

Now assume that $a, b \in R^*$ and $aR \cap bR \neq 0$. Then the right-hand side of (6.2) has the value 2 and each term on the left-hand side is a positive integer. This can only happen if both terms are 1, which means that $aR \cap bR$ and $aR + bR$ are principal. Hence, R is a weak Bezout ring.

By Theorem 5.4 we have the

(9) Some special cases of this result appear to be well known. I should like to acknowledge a stimulating conversation with Alex Rosenberg, in which he drew my attention to the above result and pointed out its applicability to free associative algebras.

COROLLARY. *Any integral domain satisfying the conditions* (i)–(ii) *of Theorem* 6.2 *locally is a weak Bezout ring.*

In the proof of Theorem 6.2 we have not used the full force of (ii) but merely the following special case:

(ii)′ *If M is a free R-module on two free generators, then every basis of M contains exactly two elements.*

We note without proof that this is true in every weak Bezout ring. It is tempting to conjecture that the property of being a weak Bezout ring is actually equivalent to (i) holding locally, and that either implies (ii).

Let R be a free associative algebra on a free generating set X over a commutative field F. Then it is known that R has no zero-divisors and satisfies (i) of Theorem 6.2 (cf. Cohn [3]). Moreover, if M is any free R-module, with basis B, denote by R_1 the augmentation ideal in R (i.e., the ideal generated by X), then $R/R_1 \cong F$ and M/MR_1 is a vector space over F of dimension equal to the cardinal of B. This shows that (ii) holds and we obtain the

COROLLARY. *Any free associative algebra over a field is a weak Bezout ring.*

In any free associative algebra we have a degree-function which is nonpositive precisely for the elements of the ground field, and in particular it is positive for nonunits $\neq 0$. It follows that the number of nonunits in any factorization of a nonzero element a is bounded by the degree of a, and we therefore have

THEOREM 6.3. *Any free associative algebra is a UFD.*

This result may also be derived from the existence of a generalized Euclidean algorithm in free associative algebras, and it holds more generally for the tensor ring of a k-bimodule and any free product of skew fields over k, where k is a given skew field (cf. Cohn [6]).

Together with Theorem 5.4, the corollary to Theorem 6.2 shows that any locally free associative algebra is a weak Bezout ring. If, e.g., we take the free associative algebra on X and adjoin, for every positive integer n, an nth root of each generator, we obtain a weak Bezout ring which is neither a UFD nor a Bezout ring (provided X has more than one element).

7. **Rigid UFD's.** Let R be any integral domain and U its group of units. If the semigroup R^*/U is free, we call R a *rigid UFD*. This is analogous to definition B in §1, but it is not a true generalization, since commutative UFD's are not generally rigid. First we show that a rigid UFD is indeed a UFD in the sense of §3.

THEOREM 7.1. *Let R be a rigid UFD. Then any two (left, right) similar elements are associated, every nonunit in R^* has a prime factorization and if an element has two prime factorizations,*

$$a = p_1 \cdots p_r = q_1 \cdots q_s,$$

then $s = r$ and p_i is similar (and hence associated) to q_i. Conversely, any integral domain with these properties is a rigid UFD.

Proof. Suppose that R is a rigid UFD and denote the natural homomorphism of R^* onto R^*/U by $a \to \bar{a}$. Then we have to show that each $\bar{a}$ has a unique representation in terms of the minimal generating set([10]) of R^*/U. But this is just the assertion that R^*/U is a free semigroup. To show that similar elements are associated, let $R/aR \cong R/bR$; by Proposition 2.1 there exist $e, f \in R^*$ and $x, y \in R$ such that $ay - ex = 1$ and $af = eb$ is an LCRM of a and e. Since R^*/U is free we have $a = ez$ or $e = az$ for some $z \in R$ and correspondingly $b = zf$ or $f = zb$ (cf., e.g., Cohn [4]). If $a = ez$, $b = zf$, then $1 = ay - ex = e(zy - x)$, hence e is a unit and since eb is an LCRM of a and e, f must also be a unit, i.e., a is associated to b. If $e = az$, $f = zb$, then $1 = ay - ex = a(y - zx)$ and a is a unit; hence so is b. Thus in any case a and b are associated. The converse is obvious.

A commutative UFD can be rigid only if its semigroup R^*/U is infinite cyclic. The conditions for this to happen are given in

THEOREM 7.2. *A commutative UFD is rigid if and only if it is a discrete (rank 1) valuation ring.*

Proof. Let R be a rigid UFD which is commutative and let p be an element whose residue class generates R^*/U. Then every element of R^* is of the form $p^n u$ ($n \geqq 0$, u a unit), and it follows that R is a discrete (rank 1) valuation ring. The converse is clear.

As an example of a noncommutative rigid UFD we mention free power series rings in any number (> 1) of noncommuting indeterminates (cf. Cohn [5]). By adjoining successive roots of the indeterminates it is possible to construct rings in which any two factorizations of a nonzero element have a common refinement, but which are not UFD.

REFERENCES

1. G. Birkhoff, *Lattice theory*, rev. ed., Amer. Math. Soc., Providence, R.I., 1948.

2. N. Bourbaki, *Éléments de mathématique: Algèbre*, Chapter VII, Actualités Sci. Ind., No. 1132, Hermann, Paris, 1951.

3. P. M. Cohn, *On a generalization of the Euclidean algorithm*, Proc. Cambridge Philos. Soc. **57** (1961), 18–30.

4. ———, *On subsemigroups of free semigroups*, Proc. Amer. Math. Soc. **13** (1962), 347–351.

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

6. ———, *Rings with a weak algorithm*, Trans. Amer. Math. Soc., (to appear).

7. H. Fitting, *Über den Zusammenhang zwischen dem Begriff der Gleichartigkeit zweier Ideale und dem Äquivalenzbegriff der Elementarteilertheorie*, Math. Ann. **112** (1936), 572–582.

([10]) The free generating set of a free semigroup is uniquely determined as the least generating set.

8. L. Gillman and M. Henriksen, *Some remarks about elementary divisor rings*, Trans. Amer. Math. Soc. **82** (1956), 362–365.

9. ———, *Rings of continuous functions in which every finitely generated ideal is principal*, Trans. Amer. Math. Soc. **82** (1956), 366–391.

10. N. Jacobson, *Theory of rings*, Amer. Math. Soc., Providence, R.I., 1943.

11. P. Jaffard, *Les systèmes d'idéaux*, Dunod, Paris, 1960.

12. I. Kaplansky, *Elementary divisors and modules*, Trans. Amer. Math. Soc. **66** (1949), 464–491.

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

14. ———, *Theory of non-commutative polynomials*, Ann. of Math. (2) **34** (1933), 480–508.

15. O. Schreier, *Über den Jordan-Hölderschen Satz*, Abh. Math. Sem. Univ. Hamburg **6** (1928), 300–302.

16. O. Zariski and P. Samuel, *Commutative algebra*, Vol. I, Van Nostrand, Princeton, N.J., 1958.

UNIVERSITY OF CALIFORNIA,
BERKELEY, CALIFORNIA
UNIVERSITY OF MANCHESTER,
MANCHESTER, ENGLAND
QUEEN MARY COLLEGE, UNIVERSITY OF LONDON,
LONDON, ENGLAND