RIGHT LCM DOMAINS[1]

RAYMOND A. BEAUREGARD

ABSTRACT. A right LCM domain is a not necessarily commutative integral domain with unity in which the intersection of any two principal right ideals is again principal. The principal result deals with right LCM domains that satisfy an additional mild hypothesis; for such rings (which include right HCF domains and weak Bezout domains) it is shown that each prime factorization of an element is unique up to order of factors and projective factors. Projectivity is an equivalence relation that reduces to the relation of "being associates" in commutative rings and reduces to similarity in weak Bezout domains.

All rings considered are (not necessarily commutative) integral domains with unity. If R is such a ring, R^* denotes the monoid of nonzero elements of R. Among the interesting properties of integral domains are the conditions that guarantee uniqueness of the prime decompositions of a given element. (A prime is understood to be a nonzero nonunit with no proper divisors.) In commutative rings the uniqueness referred to is uniqueness up to order of factors and associate factors. It is common knowledge that, in this case, uniqueness is guaranteed by the existence of LCM's for each pair of nonzero elements. This is, of course, equivalent to existence of GCD's for such elements, although in the noncommutative case this is not true. Our main concern is the extension of such results to the noncommutative case.

In going over to the noncommutative case uniqueness must be weakened. It is well known [2] that the prime factorization of a given element is unique up to order of factors and similarity in a weak Bezout domain, that is, in a ring in which the sum and intersection of any two principal right (or left) ideals is again principal whenever the intersection is nonzero. Now a weak Bezout domain can be characterized as a ring in which right (and left) LCM's exist for each pair of nonzero elements that has a nonzero common right (left) multiple, and left (and right) GCD's exist for such elements and are

linear combinations of them. In attempting to weaken this condition we are led to a consideration of rings in which the intersection of any two principal right ideals is principal (right LCM domains). In this paper we study the properties of such rings; among these is the unique factorization property given in Theorem 2. We begin with integral domains in general.

For two elements a, $b \in R^*$ the greatest common left divisor (GCLD), denoted by $(a, b)_l$, and the least common right multiple (LCRM), denoted by $[a, b]_r$, are defined in the obvious way. Thus, $d = (a, b)_l$ iff dR is the smallest principal right ideal of R containing both aR and bR, and $m = [a, b]_r$ iff mR is the largest nonzero principal right ideal of R contained in aR and bR. If $d = (a, b)_l$ then $dR = aR + bR$ provided that $aR + bR$ is already principal; in general we write $dR = aR \vee bR$. On the other hand, we always have $m = [a, b]_r$ iff $mR = aR \cap bR$. Similar definitions and remarks are analogous for the GCRD and LCLM of two elements of R^*.

LEMMA 1. *Let* $ab' = ba' \in R^*$. *If* $[a, b]_r$ *exists then so does* $(a', b')_r$ *and*

(1) $ab' = ba' = [a, b]_r(a', b')_r.$

Similarly if $[a', b']_l$ *exists then so does* $(a, b)_l$ *and*

(1′) $ab' = ba' = (a, b)_l[a', b']_l.$

PROOF. Let $m = [a, b]_r$ so that $mR = aR \cap bR$ and m has the form $m = ab_1 = ba_1$. Then $ab' = ab_1d$ for some d and, therefore, $b' = b_1d$, $a' = a_1d$. Thus d is a common right divisor of a' and b'. Let c be any other such divisor, say, $b' = b_2c$, $a' = a_2c$. We wish to show c is a right divisor of d. Now $ab_2 = ba_2$ which yields $ab_2 = ab_1r$ for some r. Hence $b_2 = b_1r$, $b_1d(= b') = b_1rc$ which yields $d = rc$ as desired. Therefore $d = (a', b')_r$ and (1) holds by the choice of d. The proof of (1′) is similar.

Before proceeding further we shall consider an example to illustrate the lack of left-right symmetry of some of the concepts considered thus far. Let S be a local PRI domain with pS the ideal of nonunits of S such that $\cap p^nS = aS \neq 0$ (see [1, p. 252]). Since aS is a two sided ideal we may define a monomorphism σ on S by $sa = as^\sigma$ ($s \in S$). Note that $a = a^\sigma$. Also $t = p^\sigma$ is a unit because $a = pa_1$ for some $a_1 \in aS$, say $a_1 = au$; substituting the last two equations into $pa = at$ we obtain $pa = paut$ from which it follows that $ut = 1$ and t is a unit.

Let $R = S[x, \sigma] = \{\sum x^ib_i \mid b_i \in S\}$ be the ring of skew polynomials in which multiplication is determined by the formula $bx = xb^\sigma$. Since $px = xt$ it follows that $x = pxt^{-1} = p^2xt^{-2} = \cdots$ and $x \in \cap p^nR$. There-

fore $xR+aR\subset\bigcap p^n R$. On the other hand, if $g\in\bigcap p^n R$ then writing $g=b_0+xg_0$ where b_0 is the constant term of g we have $b_0=g-xg_0$ $\in\bigcap p^n S=aS$ and so b_0 has the form $b_0=ar_0$. Thus $g=ar_0+xg_0$. We conclude $xR+aR=\bigcap p^n R$. Next we observe that $xR+aR$ is not a principal right ideal. For if $dR=xR+aR$ then $d\in S$; in fact, $d\in S\backslash aS$ since $d\in aS$ would yield $xR\subset aR$, say $x=af$ where f has the form $f=xr$ ($r\in S$), and so $x=xar$ and upon cancelling x we would obtain the contradiction that a is a unit; thus d must have the form $d=p^k u$ where $u\in S\backslash pS$ and this contradicts the fact that $xR+aR=\bigcap p^n R$. We conclude that $xR+aR$ is not a principal right ideal. Finally we check that $xR\cap aR=axR$. For if $xf=ag\in xR\cap aR$ then evidently $\deg(g)>0$ so that $g=xg_0$. Therefore $xf=axg_0\in axR$ and $xR\cap aR\subset axR$. The reverse inclusion is obvious since $ax=xa$.

In the present example we have $[a,x]_r=ax=xa$ but from what we have shown $(a,x)_l$ does not exist. According to Lemma 1, $[a,x]_l$ also fails to exist and $(a,x)_r$ does exist.

We shall call R a *right LCM domain* iff R is a ring in which the intersection of any two principal right ideals is principal. *Left LCM domains* are similarly defined, and if R is both a right and a left LCM domain we call R an *LCM domain*. Obviously every weak Bezout domain is an LCM domain. The most immediate example of an LCM domain that is not a weak Bezout domain is the ring of polynomials in more than one commuting indeterminate over a field.

If $a\in R$ we denote by $[aR,R]$ ($[Ra,R]$) the poset[2] of principal right (left) ideals of R containing aR (Ra). By Lemma 1 we see that the posets $[aR,R]$ and $[Ra,R]$ ($a\in R^*$) are lattices under inclusion if R is an LCM domain. In contrast, a weak Bezout domain can be characterized as a ring in which $a\in R^*$ implies the poset $[aR,R]$ (or $[Ra,R]$) is a sublattice of the lattice of all right (left) ideals of R.

A right (left) HCF ring has been defined in [2] to be a ring in which the poset of principal right (left) ideals of R is a modular lattice under inclusion. In order to compare these with right LCM domains we generalize the definition and call R a *right weak HCF domain* iff $a\in R^*$ implies $[aR,R]$ is a modular lattice under inclusion. *Left weak HCF domains* and (two sided) *weak HCF domains* are defined in the obvious way. Evidently any weak Bezout domain is a weak HCF domain. To relate LCM rings to HCF rings we use the following lemma.

LEMMA 2. *In an LCM domain R the following two conditions are equivalent*:

---

[2] Partially ordered set.

(2) $[x, yz]_r = [x, y]_r$, $(x, yz)_l = (x, y)_l$ *implies z is a unit,*[3]
(2') $[y', zx']_l = [y', x']_l$, $(y', zx')_r = (y', x')_r$ *implies z is a unit.*

PROOF. If $xy' = yzx' \neq 0$ then using (1) and (1') we have

$$xy' = (x, y)_l[zx', y']_l = [x, y]_r(zx', y')_r = (x, yz)_l[x', y']_l = [x, yz]_r(x', y')_r$$

from which the equivalence of (2) and (2') follows.

THEOREM 1. *If R is a right (left) HCF domain then R is a right (left) LCM domain satisfying* (2) ((2')). *Conversely, if R is an LCM domain satisfying* (2) ((2')) *then R is a right (left) weak HCF domain.*

PROOF. If R is a right HCF domain and if $m = [x, yz]_r$ then the modular law in the lattice $[mR, R]$ shows that (2) holds. To prove that R is a right LCM domain let $a, b \in R$ and consider $aR \cap bR$. We might as well assume $aR \cap bR \neq 0$. Then if mR is the inf of aR and bR in the lattice of principal right ideals of R it follows that $m = [a, b]_r$ and $mR = aR \cap bR$.

Now let R be an LCM domain satisfying (2). To prove the modular law in $[aR, R]$ $(a \in R^*)$ let $xR, yR, zR \supset aR$ with $zR \supset xR$. If $uR = (xR \lor yR) \cap zR$ and $vR = xR \lor (yR \cap zR)$ then we must show $uR = vR$. Now $uR \subset vR$ and hence $u = vt$ for some t. Also,

$$yR \lor uR = yR \lor vR \qquad (= yR \lor xR),$$
$$yR \cap uR = yR \cap vR \qquad (= yR \cap zR).$$

Therefore $(y, vt)_l = (y, v)_l$ and $[y, vt]_r = [y, v]_r$. By (2) this implies t is a unit and hence $uR = vR$ as desired.

Using Theorem 1 with Lemma 2 we deduce that in an LCM domain the concept of a right (weak) HCF domain is left-right symmetric. We state this result as follows.

COROLLARY. *If R is an LCM domain then R is a right (weak) HCF domain iff R is a left (weak) HCF domain.*

We recall that two elements $a, a' \in R$ are called similar, $a \sim a'$, iff $R/aR \cong R/a'R$ as R-modules. It is shown in [2] that this definition is left-right symmetric. Also, $a \sim a'$ iff there exists $b \in R$ such that $aR + bR = R$, $aR \cap bR = ba'R$ (see [2, p. 316] or [3, p. 34]). We generalize this relation and define a tr a' iff there exists $b \in R$ such that $(a, b)_l = 1$ and $[a, b]_r = ba'$. In this case $ba' = ab'$ for some b' and b tr b'.

---

[3] Note that in a commutative LCM domain (2) always holds; by factoring out (x, yz) we may assume $(x, yz) = (x, y) = 1$ in which case $[x, yz] = xyz$ and $[x, y] = xy$. Also, in a weak Bezout domain (2) holds; it is an immediate consequence of the modular law for right ideals.

Using Lemma 1 we deduce that in an LCM domain this definition is also left-right symmetric; that is, a tr a' iff there exists $b' \in R$ such that $(a', b')_r = 1$ and $[a', b']_l = ab'$. If a and a' are associates then a tr a' by taking b and b' to be units in the definition. If R is commutative then a tr a' implies a and a' are associates; this follows because in commutative rings if $(a, b) = 1$ then $[a, b] = ab$. Evidently $a \sim a'$ implies a tr a', and in a weak Bezout domain the converse holds.

If R is an LCM domain and if a tr a' then there exists $b \in R$ such that the lattice intervals $[ba'R, bR]$ and $[aR, R]$ are transposes (equivalently there exists $b' \in R$ such that $[Rab', Rb']$ and $[Ra', R]$ are transposes). If, in addition, R satisfies (2) then transposed intervals are isomorphic and therefore $[a'R, R]$ and $[aR, R]$ are isomorphic. In particular, a is prime iff a' is prime.

It can be shown (although it is not needed for our purposes) that tr is a transitive relation. If either a tr a' or a' tr a then we call a and a' *transposes*. If there is a sequence $a = a_1, a_2, \cdots, a_n = a'$ in R such that a_i and a_{i+1} are transposes for each i then a and a' are called *projective* and we write a pr a'. Projectivity is an equivalence relation in R, and is left-right symmetric if R is an LCM domain.[4] Projective elements are similar in a weak Bezout domain and are associates in a commutative ring.

If $z \in R$ then each prime factorization of z corresponds to a maximal chain in $[zR, R]$ and vice versa. It is tempting to try to prove a unique factorization theorem for right HCF domains by employing the Schreier Refinement Theorem for $[zR, R]$. While this method works well for weak Bezout domains, getting a suitable interpretation of the refinement theorem in a right HCF ring is not feasible. A direct approach for the (larger) class of right LCM domains satisfying (2) is given in the following.

THEOREM 2. *Let R be a right LCM domain satisfying* (2). *If an element has two prime factorizations, say,*

$$(3) \qquad\qquad z = p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m$$

then $n = m$ and there is a permutation σ of $\{1, 2, \cdots, n\}$ such that p_i pr $q_{\sigma(i)}$. Thus the prime factorization of an element is unique up to order of factors and projectivity.

PROOF. Let $\delta(z)$ denote the least number of prime factors of z. If $\delta(z) = 0$ there is nothing to prove and if $\delta(z) = 1$ then z is prime and the

---

[4] Strictly speaking we should speak of *right transposition* and *right projectivity* if R is not an LCM domain.

proof is trivial. Now assume that z has two prime factorizations as in (3) where $\delta(z) = n > 1$. If $p_1 R = q_1 R$ then $p_1 = q_1 u$ where u is a unit. Cancelling these factors in (3) the theorem follows by induction. If $p_1 R \neq q_1 R$ then $(p_1, q_1)_l$ exists and equals 1. Let $p_1 q_1' = q_1 p_1' = [p_1, q_1]_r$. Then p_1 pr p_1' and q_1 pr q_1' and therefore p_1' and q_1' are primes. Now $z = p_1 q_1' r$ for some r; this yields $p_2 \cdots p_n = q_1' r$ and $q_2 \cdots q_m = p_1' r$. Thus $\delta(q_1' r) < n$ and $\delta(p_1' r) < n$. By induction q_1' pr p_h and p_1' pr q_k for some h, k. Consequently p_1 pr q_k, q_1 pr p_h, and the remaining primes p_i and q_j may be paired into projective pairs through a fixed prime factorization of r.

Since projective elements are associates in commutative rings we have the following familiar result.

COROLLARY 1. *If R is a commutative LCM domain then the prime factorization of an element is unique up to order of factors and associate factors.*

Because projectivity reduces to similarity in a weak Bezout domain we have an independent proof of the following result of [2].

COROLLARY 2. *If R is a weak Bezout domain then the prime factorization of an element is unique up to order of factors and similarity.*

Weak Bezout domains can be characterized in terms of LCM domains using the following concept. If a, $b \in R$ then a and b are called *left coprime* iff $(a, b)_l = 1$. If, in addition, $1 = ar + bs$ for some r, $s \in R$ then a and b are called *left comaximal*. In the following theorem the proof, being straightforward, is omitted.

THEOREM 3. *A ring is a weak Bezout domain iff R is an LCM domain in which each left (right) coprime pair of elements having a nonzero common right (left) multiple is left (right) comaximal.*

If R is a ring in which each left coprime pair of elements having a nonzero common right multiple is left comaximal then a tr a' iff $a \sim a'$. Therefore we also have the following corollary to Theorem 2.

THEOREM 4. *Let R be a right LCM domain in which each left coprime pair of elements having a nonzero common right multiple is left comaximal. Then the prime factorization of an element is unique up to order of factors and similarity.*

Note that, in the statement of Theorem 4, condition (2) need not be stated explicitly; it may be derived from the hypotheses.

If R is an LCM domain satisfying (2) then projective elements that

have prime decompositions have the same prime factorizations in the sense of Theorem 2. This result is a corollary of the following theorem.

THEOREM 5. *Let R be an LCM domain satisfying* (2) *and let a tr a'.*
(i) *If $a = a_1 a_2$ then there exist a_1', a_2' such that $a' = a_1' a_2'$;*
(ii) *If $a' = a_1' a_2'$ then there exist a_1, a_2 such that $a = a_1 a_2$;*
in either case a_1 tr a_1' and a_2 tr a_2'.

PROOF. Let $(a, b)_l = 1$, $[a, b]_r = ab' = ba'$ and suppose $a = a_1 a_2$. Then $(a_1, b)_l = 1$, $[a_1, b]_r = a_1 b'' = ba_1'$ for some a_1', b''. Thus a_1 tr a_1'. Also $[a, b]_r = [a_1, b]_r a_2'$ for some a_2' and, so $a' = a_1' a_2'$ and $b'' a_2' = a_2 b'$. It follows by the modular law (guaranteed by (2) in Theorem 1) that $(a_2, b'')_l = 1$. Now $a_1 [a_2, b'']_r = [a, a_1 b'']_r$ which is equal to $[a, b]_r$ since $a_1 b'' = [a_1, b]_r$. Therefore $[a_2, b'']_r = a_2 b'$ and a_2 tr a_2'. The second statement of the theorem is proved in a similar way using (2') and the modular law for principal left ideals.

By induction we may extend Theorem 5 in the following way.

COROLLARY. *Let R be an LCM domain satisfying* (2). *If a pr a' and if $a = a_1 a_2 \cdots a_n$ then there exist a_1', a_2', $\cdots$, a_n' such that $a' = a_1' a_2' \cdots a_n'$ with a_i pr a_i'.*

Using the last corollary with Theorem 2 we have the following.

THEOREM 6. *Let R be an LCM domain satisfying* (2). *If z pr z' and if $z = p_1 p_2 \cdots p_n$, $z' = q_1 q_2 \cdots q_m$ where p_i and q_j are primes, then $n = m$ and there is a permutation σ of $\{1, 2, \cdots, n\}$ such that p_i pr $q_{\sigma(i)}$.*

We note that Theorem 6 and the preceding corollary have analogous statements for weak Bezout domains, where projectivity is replaced by similarity.

BIBLIOGRAPHY

1. R. A. Beauregard, *Infinite primes and unique factorization in a principal right ideal domain*, Trans. Amer. Math. Soc. 141 (1969), 245–253. MR 39 #4206.

2. P. M. Cohn, *Noncommutative unique factorization domains*, Trans. Amer. Math. Soc. 109 (1963), 313–331. MR 27 #5785.

3. N. Jacobson, *The theory of rings*, Math. Surveys, no. 2, Amer. Math. Soc., Providence, R. I., 1943. MR 5, 31.

UNIVERSITY OF RHODE ISLAND, KINGSTON, RHODE ISLAND 02881