Can. J. Math., Vol. XXIX, No. 2, 1977, pp. 307–314

AN ANALOG OF NAGATA'S THEOREM FOR MODULAR LCM DOMAINS

RAYMOND A. BEAUREGARD

1. Introduction. The theorem referred to in the title asserts that for an atomic commutative integral domain R, if S is a submonoid of R^* (the monoid of nonzero elements of R) generated by primes such that the quotient ring RS^{-1} is a *UFD* (unique factorization domain) then R is also a *UFD* [**8**]. Recently several definitions of a noncommutative *UFD* have been proposed (see the summary in [**6**]). However the analog of Nagata's theorem does not hold for all of these, the most notable illustration being that of a similarity-*UFD* which was introduced in [**5**] (but the terminology is that of [**6**]). In contrast, Nagata's theorem holds for the larger class of projectivity-*UFD* and this result is included in Section 4 below.

The notion of a projectivity-*UFD* arose from an attempt to obtain uniqueness of atomic factorizations of an element as in the commutative case, that is, for a *right LCM domain* (an integral domain in which the intersection of any two principal right ideals is again principal). Unfortunately there are right *LCM* domains in which not even the number of atomic factors in different factorizations of an element is constant (an example first noticed in [**4**] occurs below). Uniqueness (in the projectivity-*UFD* sense) has been established [**1**] for *modular* right *LCM* domains, a class which includes the commutative *LCM* domains. In addition, many results of noncommutative principal ideal domains can be carried over to modular *LCM* domains (see [**2**] and [**3**]). Our main goal here is to obtain an analog of Nagata's theorem for modular *LCM* domains thus providing the means for exhibiting additional examples to which these results apply.

2. Preliminaries. All rings considered are not necessarily commutative integral domains with unity. For a ring R, U_R denotes the group of units of R and R^* is its monoid of nonzero elements. We recall from [**1**] that if $ab' = ba'$ in R^* and if the least common right multiple $[a, b]_r$ of a and b exists then the greatest common right divisor $(a', b')_r$ of a' and b' exists and satisfies

$$(1)\qquad ab' = ba' = [a, b]_r(a', b')_r;$$

in addition, $aR \cap bR = [a, b]_rR$ and we also write $Ra' \vee Rb' = R(a', b')_r$. Thus for $x \in R^*$ in a (two sided) *LCM* domain R the interval $[xR, R] = \{aR | xR \subseteq aR \subseteq R\}$ is a lattice under inclusion. This lattice is modular if and

Received February 18, 1976.

only if R satisfies the following condition which is left-right symmetric in an LCM domain:

(M) $[a, b]_r = [a, bc]_r, (a, b)_l = (a, bc)_l \Rightarrow c \in U_R$.

In general, a ring R is said to be *(right) modular* if it satisfies (M) (whenever those quantities exist).

A 2-fir (weak Bezout domain) is an example of a modular LCM domain. In addition every commutative ring is modular. This can be shown more generally. Recall that $a \in R^*$ is *invariant* if $aR = Ra$; in this case every factor of a is a left factor, for if $a = uyv$ then $a = yvu'$ where u' is chosen so that $ua = au'$ (similarly every factor of a is a right factor). Thus if a, b, and c are invariant then there is no need for the subscripts in (M); if we assume, as we may, that $(a, b) = (a, bc) = 1$ and if we choose $b' \in R$ such that $ab' = ba$ then we have $ba = [a, b']$ by the left-right analog of (1); multiplying this equation on the left by a and then cancelling a on the right we find $ab = [a, b]$; similarly $abc = [a, bc]$, and equating these lcm's we have $ab = abc$ so that $c \in U_R$. We summarize in the following.

PROPOSITION 2.1. *The modular condition (M) holds for all invariant elements in an integral domain.*

By an m-system in R we mean a submonoid S of R^*. An element $a \in R^* \backslash U_R$ is said to be *right prime to* S if whenever $s \in S$ is a right factor of $ab (b \in R)$ then s is a right factor of b (we shall abbreviate this as $s \in S$, $s/_r ab \Rightarrow s/_r b$). The next three propositions make this concept easier in particular cases. Recall that a *right Ore system* in R is an m-system S for which $aS \cap sR \neq \emptyset$ for each $a \in R$, $s \in S$; as is well known, the right quotient ring RS^{-1} is then defined.

PROPOSITION 2.2. *Let S be a right Ore system in R with $K = RS^{-1}$. Then $a \in R^* \backslash U_R$ is right prime to S if and only if $aK \cap R = aR$.*

We omit the proof since it is straight-forward. A particular type of Ore system is an m-system which is invariant in R, i.e., every element of S is invariant in R. Of course in this case there is no need for the subscripts (indicating right division) in the definition of "right prime to S" which may be phrased "prime to S".

PROPOSITION 2.3. *Let S be an m-system which is invariant in R. Then $a \in R^* \backslash U_R$ is prime to S if and only if $aR \cap sR = asR$ for each $s \in S$.*

Proof. We always have $asR \subseteq aR \cap sR$; if a is prime to S and if $x \in aR \cap sR$ then $x = ab$ for some $b \in R$ and s/ab, hence s/b which shows $x \in asR$. The converse follows as easily.

An element $p \in R^* \backslash U_R$ is said to be a *right prime* if $p/_r ab \Rightarrow p/_r a$ or $p/_r b$. Shortly we shall be interested only in invariant primes (and the subscripts will again be omitted).

https://doi.org/10.4153/CJM-1977-034-6 Published online by Cambridge University Press

PROPOSITION 2.4.
(i) *If $a \in R$ is right prime to an m-system S then a has no right factor in $S \backslash U_R$.*
(ii) *The converse of* (i) *holds if S is generated by right primes.*

Proof. (i) If $s \in S$ and $s/_r a$ and if a is right prime to S then $s/_r 1$ so that $s \in U_R$.

(ii) Suppose $ab = rs$ where $s = p_1 \ldots p_n$ and the p_i are right primes. If a has no right factor in $S \backslash U_R$ then $p_n/_r b$, say $b = b_n p_n$; then $ab_n = rp_1 \ldots p_{n-1}$ and we continue now with p_{n-1}. We eventually wind up with $ab_1 = r$ and so $b = b_1 s$, as desired, showing a is right prime to S.

Example. Consider the skew polynomial ring

$$R = A[x, 2] = \left\{ \sum_{i=0}^{i=n} x^i a_i | a_i \in A, n \in N \right\}$$

where A is the commutative polynomial ring $A = Z_2[y]$ over the field of integers modulo 2 and where multiplication in R is defined so that $ax = xa^2$. Let $S = \{x^n | n \in N\}$ be the m-system in R generated by x. Clearly xy has no right factor in S other than 1, but xy is not right prime to S as the equation $yx = (xy)y$ shows. Note that x is a left prime but not a right prime.

PROPOSITION 2.5. *Let $a_1, a_2 \in R$ be right prime to an m-system S. Then:*
(i) *$a_1 a_2$ is right prime to S.*
(ii) *If $a_1 s_1 = a_2 s_2$ ($s_i \in S$) then $a_1 R = a_2 R$.*
(iii) *If $[a_1, a_2]_r$ exists then it has no right factor in $S \backslash U_R$.*

Proof. The proofs of (i) and (ii) are straight-forward. To prove (iii) we write $[a_1, a_2]_r = a_1 a_2' = a_2 a_1'$ and suppose $s/_r[a_1, a_2]_r$. Then $s/_r a_1'$ and $s/_r a_2'$ by definition of right prime to S; but $(a_1', a_2')_r = 1$ by (1) so that $s \in U_R$.

3. Nagata's Theorem for modular LCM domains. Hereafter S will be an invariant m-system in R and $K = RS^{-1}$ will be the corresponding quotient ring of R.

PROPOSITION 3.1. *Let $a, a_1, a_2 \in R$ be either units or prime to S such that $aK = a_1 K \cap a_2 K$, and let $s, s_1, s_2 \in S$ be such that $sR = s_1 R \cap s_2 R$. Then $asR = a_1 s_1 R \cap a_2 s_2 R$, that is, $[a_1 s_1, a_2 s_2]_r = [a_1, a_2]_r [s_1, s_2]$ in R.*

Proof. According to Proposition 2.3, $asR = aR \cap sR$ if $s \in S$ and a is prime to S; this also holds if $a \in U_R$, for $asR = aRsR = sR = aR \cap aR$. In addition, Proposition 2.2 shows that $aR = a_1 R \cap a_2 R$. Thus $asR = aR \cap sR = a_1 R \cap a_2 R \cap s_1 R \cap s_2 R = a_1 s_1 R \cap a_2 s_2 R$.

PROPOSITION 3.2. *Assume that each $x \in R^* \backslash S$ can be written $x = as$ where $s \in S$ and a is prime to S. If K is* (*right*) *modular then so is R.*

Proof. We remark that S is necessarily saturated, for if $s = ab \in S$ and if $a \notin S$ then $a = a_1 s_1$ where a_1 is prime to S; the equation $s = a_1 s_1 b$ then

https://doi.org/10.4153/CJM-1977-034-6 Published online by Cambridge University Press

implies s/s_1b so that $a_1 \in U_R$ contradicting the definition of a_1. To establish condition (M) let

(2) $[x_1, x_2]_r = [x_1, x_2x_3]_r$

and $(x_1, x_2)_l = (x_1, x_2x_3)_l$ which we may assume is unity. Let $x_i = a_is_i$ where $s_i \in S$ and $a_i \in U_R$ or is prime to S $(i = 1, 2, 3)$. We first show that $x_3 \in S$. If this is not so then $s_2a_3 = a_4s_4$ where $s_4 \in S$ and a_4 is prime to S. Then using Proposition 3.2, (2) can be written

$$[a_1, a_2]_r[s_1, s_2] = [a_1, a_2a_4]_r[s_1, s_4s_3].$$

The left factors of the last equation are prime to S in view of Proposition 2.5 (iii) and the hypothesis on R. Thus $[a_1, a_2]_r = [a_1, a_2a_4]_r$ by Proposition 2.5 (ii), and in particular, $a_1K \cap a_2K = a_1K \cap a_2a_4K$. Also, $a_1K \vee a_2K = a_1K \vee a_2a_4K = K$, for if $a_1K, a_2K \subseteq dK$ where $d \in R$ is a unit or prime to S then $a_1R, a_2R \subseteq dR$ (Proposition 2.2) which means $d \in U_R$ because $(a_1, a_2)_l = 1$ in R; similarly $a_1K \vee a_2s_4K = K$. Applying (M) which holds in K, we conclude that $a_4 \in U_K$ so that $a_4 \in S$ because S is saturated, and this contradicts the choice of a_4. We have shown $x_3 \in S$, so that with Proposition 3.2, (2) can be written

$$[a_1, a_2]_r[s_1, s_2] = [a_1, a_2]_r[s_1, s_2x_3].$$

Thus we have $[s_1, s_2] = [s_1, s_2x_3]$. Clearly $(s_1, s_2) = (s_1, s_2x_3) = 1$ because $s_i /_l x_i$. Proposition 2.1 then applies to show $x_3 \in U_R$ and the proof is concluded.

An m-system S of R is said to be *lcm-closed* if $s_1, s_2 \in S \Rightarrow sR = s_1R \cap s_2R$ for some $s \in S$. We summarize what has been established as follows (cf. [**7**, Theorem 3.1] for the commutative case).

THEOREM 3.3. *Let S be an invariant m-system which is lcm-closed in R. Assume each $x \in R^*\backslash S$ can be written $x = as$ where $s \in S$ and a is prime to S. If RS^{-1} is a modular right LCM domain then so is R.*

The next result indicates how the hypotheses of Theorem 3.3 can be satisfied in a ring R. Recall that an *atom* or *irreducible* is an element of $R^*\backslash U_R$ that has no proper factors; R is *atomic* if each member of $R^*\backslash U_R$ is a product of atoms.

PROPOSITION 3.4. *Let S be an m-system containing U_R and generated by invariant primes of R. Then*

(i) *S is lcm-closed.*

(ii) *If R has the* acc *for principal right ideals or if R is atomic then each member x of $R^*\backslash S$ can be written $x = as$ where $s \in S$ and a is prime to S.*

Proof. We remark again that S is necessarily saturated. To prove (i) let $s, t \in S$ and let $p_1, \ldots, p_k$ be their common prime factors (not necessarily distinct); thus $s = p_1 \ldots p_ks_1$ and $t = p_1 \ldots p_kt_1$ where $(s_1, t_1) = 1$. If $t \in U_R$

we are finished. Otherwise t_1 is prime to $\{s_1^n | n \in N\}$ (cf. Proposition 2.4) so that $t_1R \cap s_1R = t_1s_1R$ by Proposition 2.3; this shows $tR \cap sR = ts_1R$.

To prove (ii) let us first assume that R has the acc for principal right ideals. If some $x \in R^*\backslash S$ cannot be written in the desired form we may choose such an x with respect to which xR is maximal. Thus x cannot be prime to S so that $x = x_1s_1$ for some $s_1 \in S\backslash U_R$ (Proposition 2.4). Since $xR \subsetneq x_1R$ we may write $x_1 = as$ where $s \in S$ and a is prime to S; then $x = a(ss_1)$ contradicting the choice of x. Let us now assume that R is atomic; each atom in S is prime while each atom in $R\backslash S$ is prime to S (Proposition 2.4). Thus each $x \in R^*$ may be written $x = a_1 \ldots a_ka_{k+1} \ldots a_n$ where $a_i \in S$ for $i > k$ and $a_1 \ldots a_k$ is prime to S by Proposition 2.5.

Using Proposition 3.4 we may state Theorem 3.3 in the following form.

THEOREM 3.5. *Let S be an m-system generated by invariant primes in R. Assume that either R has the* acc *for principal right ideals or that R is atomic. If RS^{-1} is a modular right LCM domain then so is R.*

COROLLARY 3.6. *Let A be a commutative UFD. The free associative algebra $R = A[X]$ on a set X is a modular LCM domain.*

Proof. (cf. [**4**, Satz 8]) Using an argument as in the proof of Gauss' lemma it can be shown that the primes in A are primes in R. Thus $S = A^*$ is an m-system generated by central primes of R. Also, $RS^{-1} \cong A(A^*)^{-1}[X]$, the free associative algebra over a field which is known to be a 2-fir [**5**] and hence a modular *LCM* domain. Since R is atomic, Theorem 3.5 (and its left-right analog) apply to show that R is a modular *LCM* domain.

The next application deals with the ring of skew formal power series over a *PRI* (principal right ideal) domain. First we need the following result for the corresponding ring of formal Laurent series. As usual ord(f) denotes the degree of the first nonzero term of a Laurent series f.

PROPOSITION 3.7. *Let A be a PRI domain with automorphism σ and let $K = A\langle\langle x, \sigma\rangle\rangle = \{\sum_{i=n}^{\infty} a_ix^i | a_i \in A, n \in Z\}$ (where multiplication in K is defined by $xa = \sigma(a)x, x^{-1}a = \sigma^{-1}(a)x^{-1}$). Then K is a PRI domain.*

Proof. Let $0 \neq I$ be a right ideal of K and let

$$J = \{a \in A | a + h \in I, \text{ord } (h) > 0\}.$$

Clearly J is a nonzero right ideal of A and so has the form $J = aA$. Let $f = a + h \in I$ so that $fK \subseteq I$. To show the reverse inclusion let $g_1 \in I$ with first term $b_{n_1}x^{n_1}$; then $b_{n_1} \in J(g_1x^{-n_1} \in I)$ so we write $b_{n_1} = ar_1(r_1 \in A)$. If $g_2 = g_1 - fr_1x^{n_1}$, then $g_2 \in I$ and ord $(g_2) >$ ord (g_1). Proceeding by induction, suppose $g_i(i \leqq k)$ have been found in I with increasing order. If g_k has first term $b_{n_k}x^{n_k}$ then $b_{n_k} \in J$ so we write $b_{n_k} = ar_k$ and define $g_{k+1} = g_k - fr_kx^{n_k} \in I$ with ord $(g_{k+1}) >$ ord (g_k). Then $g_1 = f\sum_{k=1}^{\infty} r_kx^{n_k} \in fK$ as desired.

COROLLARY 3.8. *Let A be a PRI domain with automorphism σ. Then $R = A[[x, \sigma]] = \{\sum_{i=0}^{\infty} a_i x^i | a_i \in A\}$ (where multiplication in R is defined by $xa = \sigma(a)x$) is a modular LCM domain.*

Proof. Let S be the saturated m-system generated by the invariant prime x. Each power series in R may be written as $fx^k = x^k f'$ where $k \in N$ and f and f' have order zero and so are either units or prime to S (cf. Proposition 2.4). Also, $RS^{-1} \cong A\langle\langle x, \sigma\rangle\rangle$, the corresponding ring of formal Laurent series, which is a *PRI* domain (Proposition 3.7) hence a 2-fir, hence a modular *LCM* domain. Theorem 3.3 (and its left-right analog) apply to show that R is a modular *LCM* domain.

Remark 3.9. If σ is a monomorphism on the *PRI* domain A but not an automorphism then the power series ring of Corollary 3.8 need not be modular, although it is still a right *LCM* domain according to [**4**, Satz 9]. For example, if A is the commutative polynomial ring $Z_2[y]$ over the field of integers modulo 2 and $R = A[[x, 2]]$ where multiplication is defined by $xa = a^2x$ then the equation $xy = y^2x$ shows that R is not modular, i.e., $(x, y)_l = (x, y^2)_l = 1$ and $[x, y]_r = [x, y^2]_r = xy$ but $y \notin U_R$.

Remark 3.10. It follows that the ring of formal power series $F[[x, y]]$ in two commuting indeterminates over a skew field F is a modular *LCM* domain. However the same is not true of the polynomial ring $F[x, y]$. If $R = Q[x, y]$ where Q is the field of real quaternions then it can be shown that $(1 + ix)R \cap (1 + jy)R$ is not principal ($i^2 = j^2 = -1$); note that it contains both $(1 + ix)(1 + y^2)$ and $(1 + jy)(1 + x^2)$.

Remark 3.11. The example just given shows that unlike the commutative case, if A is an *LCM* domain then $A[x]$ need not be an *LCM* domain (even if A is a *PID*). In contrast Corollary 3.8 shows that if A is a *PRI* domain then $A[[x, \sigma]]$ is an *LCM* domain as in the commutative case. As an example in [**9**] shows, if A is an *LCM* domain then $A[[x]]$ need not be an *LCM* domain (even if A is commutative).

4. Nagata's theorem for projectivity-UFDS. We recall from [**1**] that two elements a, a' in a ring R are said to be *transposed* and we write a tr a' if $[a, b]_r = ba'$ and $(a, b)_l = 1$ for some $b \in R$. The relation tr reduces to similarity in a 2-fir and to that of being associates in a commutative ring. However, tr is not symmetric: referring to the example in Remark 3.9 we have x tr yx but yx ~~tr~~ x. We therefore define a and a' to be *projective* and we write a pr a' if there exist $a_0 = a, a_1, \ldots, a_n = a'$ where either a_{i-1} tr a_i or a_i tr a_{i-1} for each i. It was shown in [**1**] that in a modular right *LCM* domain the atomic factorization of an element is unique up to order of factors and projective factors. Following the terminology of [**6**] we say that R is a *projectivity-UFD* if R is an atomic integral domain in which atomic factorizations are unique in this sense. The corresponding analog of Nagata's theorem depends on two preliminary results.

PROPOSITION 4.1. *Let S be an m-system invariant in R and assume that each element $x \in R^*\backslash S$ can be written $x = as$ where $s \in S$ and a is prime to S. Let a be prime to S and $s \in S$.*

(i) *If $sa = a's$ then a'* tr *a.*

(ii) *If $as = sa'$ then a* tr *a',*

and in either case a' is prime to S.

Proof. If $sa = a's$ then $Ra \cap Rs = Rsa$ by the left-right analog of Proposition 2.3; thus $(s, a')_1 = 1$ (the analog of equation (1)). Also, a' is prime to S, for we may write $a' = a''s'$ where $s' \in S$ and a'' is prime to S; then $[a'', s]_r = a''s = sc$ for some $c \in R$ (Proposition 2.3). We then have $sa \in scR$, say $sa = scx$ which shows $x/_r a$ but the last equation may be written $a''s's = a''sx$ which shows $x \in S$; the conclusion is that $x \in U_R$ and so $s' \in U_R$, i.e., a' is prime to S. This also shows that $[a', s]_r = sa = a's$ so that a' tr a.

The proof of (ii) is shorter: if $s'/_r a'$ then $s'/_r s$, and so s' is a unit because $(s, a')_r = 1$ and this because $[a, s]_r = as = sa'$, by Proposition 2.3; therefore a' is prime to S and a tr a'.

The proof of (i) in Proposition 2.4 is quite short if we assume that S is generated by invariant primes in place of the "$x = as$" hypothesis. However, the present form yields the following.

COROLLARY 4.2. *Let S be an m-system invariant in R and assume that each element $x \in R^*\backslash S$ can be written $x = as$ where $s \in S$ and a is prime to S. Then the primes of S are primes of R.*

Proof. If p is a prime of S and $p/(a_1s_1)(a_2s_2)$ where $s_i \in S$ and a_i are prime to S then writing $s_1a_2 = a_2's_1$ we have a_2' and therefore a_1a_2' prime to S (Proposition 4.1 and Proposition 2.5). Therefore p/s_1s_2 and so p/s_1 or p/s_2 as desired.

PROPOSITION 4.3. *Let S be an m-system invariant in R and let $K = RS^{-1}$. Assume each element $x \in R^*\backslash S$ can be written $x = as$ where $s \in S$ and a is prime to S. If $a, a_1 \in R$ are prime to S and a* pr_K *a_1 then a* pr_R *a_1.*

Proof. We may assume that a tr_K a_1; thus $aK \cap bK = ba_1K$, $aK \vee bK = K$ for some $b \in K$. Let $b = b_1s_2s_1^{-1}$ where $s_i \in S$ and b_1 is prime to S; let $a_1s_1 = s_1a_2$, $s_2a_2 = a_3s_2$ where the a_i are prime to S and a_i pr_R a_j by Proposition 4.1. Applying Propositions 2.2 and 2.3 we have $aR \cap b_1R = aK \cap b_1K \cap R = ba_1K \cap R = b_1a_3K \cap R = b_1a_3R$, and also $aR \vee b_1R = R$ (any common left factor would be a unit in K hence in S). We conclude that a tr_R a_3 and so a pr_R a_1.

We can now give the following analog of Nagata's theorem for projectivity-*UFD*s using the proof of a general result of [**6**].

THEOREM 4.4. *Let R be an atomic integral domain and let S be an m-system generated by invariant primes of R. If $K = RS^{-1}$ is a projectivity-UFD, then so is R.*

Proof. Proposition 3.4 shows that Proposition 4.3 applies. Let $x = a_1 \ldots a_n = b_1 \ldots b_m$ be two atomic factorizations of x. If some a_i is an invariant prime then it divides and is therefore associated to some b_j; these may be brought to the right (Proposition 4.1) and cancelled and we then apply induction. Thus we may assume that no a_i or b_j is an invariant prime; then these are all prime to S and consequently atoms in K. Therefore $n = m$ and $a_i \text{ pr}_K b_{\pi(i)}$ for some permutation π of the subscripts, and so $a_i \text{ pr}_R b_{\pi(i)}$ by Proposition 4.3.

For an atomic integral domain R with unique factorization monoid S (i.e., S generated by invariant primes of S) the hypothesis that S be generated by primes of R is equivalent to the hypothesis that each element $x \in R^*\backslash S$ can be written $x = as$ for $s \in S$ and a prime to S in view of Corollary 4.2 and Proposition 3.4.

REFERENCES

1. R. A. Beauregard, *Right LCM domains*, Proc. Amer. Math. Soc. *30* (1971), 1–7.
2. ——— *Right quotient rings of a right LCM domain*, Can. J. Math. *24* (1972), 983–988.
3. ——— *Right bounded factors in an LCM domain*, Trans. Amer. Math. Soc. *200* (1974), 251–266.
4. H. H. Brungs, *Ringe mit eindeutiger Factorzerlegung*, J. Reine Angew. Math. *236* (1969), 43–66.
5. P. M. Cohn, *Noncommutative unique factorization domains*, Trans. Amer. Math. Soc. *109* (1963), 313–331.
6. ——— *Unique factorization domains*, Amer. Math. Monthly *80* (1973), 1–18.
7. R. Gilmer and T. Parker, *Divisibility properties in semigroup rings*, Michigan Math. J. *21* (1974), 65–86.
8. M. Nagata, *A remark on the unique factorization theorem*, J. Math. Soc. Japan *9* (1957), 143–145.
9. P. Samuel, *On unique factorization domains*, Ill. J. Math. *5* (1961), 1–17.

University of Rhode Island,
Kingston, Rhode Island