Canad. Math. Bull. Vol. **37** (3), 1994 pp. 289–293

FACTORIZATION IN LCM DOMAINS WITH CONJUGATION

RAYMOND A. BEAUREGARD

ABSTRACT. An atomic integral domain with conjugation has unique (in the sense of Theorem 6 below) factorization of atomic factors if it is an LCM domain. If the LCM hypothesis is dropped not even the number of atomic factors in a complete factorization of an element need be unique.

This paper is motivated, in part, by the discovery [3] that the polynomial ring $F[x,y]$ in two commuting indeterminates does not have unique factorization of atomic (that is, irreducible) factors when F is the skew field of quaternions over the field of rationals. Specifically, the number of atomic factors in a complete factorization of an element need not be constant.

All rings considered are not-necessarily commutative integral domains with unity. A ring R is said to be a *ring with conjugation* if it has an anti-automorphism $a \longrightarrow \bar{a}$ whose square is the identity map and which satisfies

$$a = \bar{a} \Rightarrow a \in \mathrm{C}(R), \tag{1}$$

where $\mathrm{C}(R)$ is the center of R. (Thus $a \longrightarrow \bar{a}$ is an involution satisfying condition (1).) For example, a quaternion algebra is a ring with (the usual) conjugation. We shall show that, unlike the example referred to above, if a ring with conjugation is an LCM domain then it does have unique factorization.

We say that $a \neq 0$ in R is *right invariant* if $Ra \subseteq aR$ and is *invariant* if $Ra = aR$; an element is (*right*) *bounded* if it is a factor of a (right) invariant element. If R is a ring with conjugation then, for each $a \in R$, $a\bar{a} \in \mathrm{C}(R)$ so that a is bounded. We also have $a\bar{a} = \bar{a}a$ [consider the equation $a(a\bar{a}) = (a\bar{a})a$]. We shall show that when a is *left-* and *right-invariant-free*, that is, has no left- or right- invariant factor other than units then $a\bar{a}$ is the two-sided bound of a (definition recalled below). Clearly a is right invariant if and only if $\bar{a}$ is left invariant. More generally we have the following.

LEMMA 1. *Let R be any ring and let $a = bc$ be an equation of nonzero elements in R. If a is left invariant and b is right invariant then c is left invariant. If a and b are invariant then c is invariant.*

PROOF. For the first statement, let $r \in R$ and choose r' such that $bcr = r'bc$ (using the left invariance of $a = bc$) and then r'' such that $r'bc = br''c$ (using the right invariance of b). On cancelling in the equation $bcr = br''c$ we obtain $cr = r''c$ showing c to be left invariant. For the second statement assume that a and b are invariant. We have just seen

Received by the editors December 16, 1992.
AMS subject classification: 16U30.

that c is left invariant. To show that c is right invariant, let $r \in R$ and choose r' such that $brc = r'bc$ and then r'' such that $r'bc = bcr''$; then $rc = cr''$ so that $Rc \subseteq cR$ as desired.

Recall that a ring R is a *right* (*left*) LCM *domain* if the intersection of any two principal right (left) ideals of R is again principal. A right and left LCM domain is referred to as an LCM domain. In case R is a ring with conjugation there is no distinction between the right and the left LCM conditions since

$$aR \cap bR = mR \quad \text{if and only if } R\bar{a} \cap R\bar{b} = R\bar{m}.$$

The set $I(R)$ of invariant elements in any LCM domain R is closed under the formation of least common multiples [1, Theorem 5.3]. Suppose that R is also *atomic* (that is, each nonzero nonunit of R is the product of atoms). Then $I(R)$ has unique factorization in the sense that any product of I-atoms (that is, nonunits in $I(R)$ with no proper invariant factors) is unique up to order of factors and associated [4, p. 156] (*cf.* also Lemma 5 below). We record this fact as follows.

PROPOSITION 2. *Let R be an atomic* LCM *domain. Then R has unique factorization of invariant elements.*

If R is a ring with the acc (ascending chain condition) for principal right ideals and the acc for principal left ideals, then it is easy to show that R is atomic. The converse is not generally true. However, if R is an LCM domain with conjugation then the converse does follow. To see this we check that

$$bR \subset aR \Rightarrow b\bar{b}R \subset a\bar{a}R.$$

The condition $bR \subset aR$ means $b = ar$ for some nonunit r in R; then $\bar{b} = \bar{r}\bar{a}$ so $b\bar{b} = ar\bar{r}\bar{a} = a\bar{a}r\bar{r}$ and $b\bar{b}R \subset a\bar{a}R$. Thus the acc for invariant principal ideals in R yields the acc for principal right ideals and (by symmetry) the acc for principal left ideals. Now if R is atomic then R has the acc for invariant principal ideals by Proposition 2 and Lemma 1.

We turn to a description of the bound of a nonzero element a in R. The set

$$I_a = \{r \in R \mid Rr \subseteq aR\}$$

is the largest two-sided ideal of R contained in aR. It is shown in [1, Theorem 2.2] that when R is an LCM domain satisfying the acc for principal right and principal left ideals, then I_a has the form $I_a = a^*R$ for some a^* in R. Moreover, a is right bounded if and only if $a^* \neq 0$, in which case a^* is the *right bound* of a. The *left bound* of a is described similarly. The left and right bounds of an element need not coincide even when one of these is central [1, Example 2.9]. If R also has a conjugation then the situation improves. For, $a\bar{a} \in a^*R$ since $a^*R = I_a$ and so $a\bar{a} = a^*t$ for some $t \in R$. Then t is left-invariant by Lemma 1. Choose $s \in R$ such that $a^* = as$. Then $a\bar{a} = a^*t = ast$ so that $\bar{a} = st$ and $a = \bar{t}\bar{s}$. Since t is left invariant, $\bar{t}$ is right invariant. If we assume that a is right-invariant-free then $\bar{t}$ and hence t are units and $a\bar{a}R = a^*R$. In a similar manner we can show that $a\bar{a}$ is the left bound of a if a is left-invariant-free. Thus a has a two-sided bound (as described in [1]) and this is given by $a\bar{a}$ in this situation. We have established the following.

THEOREM 3. *Let R be an atomic* LCM *domain with conjugation. If $a \in R$ is left- and right-invariant-free then $a\bar{a}$ is the two-sided bound of the element a.*

Theorem 3 applies to an atom a which is neither left nor right invariant showing that a has two-sided bound $a\bar{a}$. Proposition 5.1 of [1] then shows that $a\bar{a}$ is an I-atom. Thus we obtain the following.

COROLLARY 4. *Let R be an atomic* LCM *domain with conjugation. If $a \in R$ is an atom which is neither left nor right invariant then $a\bar{a}$ is an I-atom.*

This is the key step in establishing unique factorization in R. It is precisely this property that fails in the ring $F[x,y]$ when $F = Q(1,i,j,k)$ is the field of rational quaternions: if

$$f = (x^2y^2 - 1) + (x^2 - y^2)i + 2xyj,$$

then it can be shown that f is an atom [3] which is neither left nor right invariant but $f\bar{f}$ factors as

$$f\bar{f} = (x^4 + 1)(y^4 + 1), \tag{2}$$

where $\bar{f}$ is the usual conjugate of f. In an LCM domain this cannot occur. We also note that the right-hand side of equation (2) factors into the product of the four atoms $(x^2 \pm i)$, $(y^2 \pm i)$, while the left-hand side is the product of two atoms.

We shall need one additional lemma. We say that *p divides a* if $a = rps$ for some $r, s \in R$; if p is right invariant this reduces to $a \in pR$.

LEMMA 5. *Let R be an* LCM *domain. Let p be an atom in R which is either right or left invariant. Then p is a prime; that is, if p divides a product ab then p divides a or p divides b.*

PROOF. Assume that p is a right invariant atom that divides ab but does not divide a. Choose q in R such that $pR \cap aR = aqR$. Since p does not divide a we have $qR \neq R$. The right invariance of p shows ap is in pR and so in aqR. Thus $p \in qR$ and $pR = qR$ because p is an atom. Now $ab \in pR$ by hypothesis and so ab is in aqR. Thus $b \in qR = pR$ showing that p divides b. The left invariant case follows by symmetry; in this case p is always a right factor.

THEOREM 6. *Let R be an atomic* LCM *domain with conjugation. Each factorization into atomic factors is unique in the sense that if*

$$a_1a_2\cdots a_n = b_1b_2\cdots b_m \tag{3}$$

where the a_i and b_j are atoms then $n = m$ and there is a permuation σ of the subscripts such that $a_i\bar{a}_iR = b_{\sigma(i)}\bar{b}_{\sigma(i)}R$.

PROOF. Equation (3) leads to

$$a_1a_2\cdots a_n\bar{a}_n\cdots\bar{a}_2\bar{a}_1 = b_1b_2\cdots b_m\bar{b}_m\cdots\bar{b}_2\bar{b}_1, \text{ or}$$

$$a_1\bar{a}_1\cdots a_n\bar{a}_n = b_1\bar{b}_1\cdots b_m\bar{b}_m. \tag{4}$$

If some a_i is right invariant then it must divide some b_j or $\bar{b}_j$ by Lemma 5. Thus $a_iR = b_jR$ or $a_iR = \bar{b}_jR$ since b_j and $\bar{b}_j$ are atoms; in either case, a_i, $\bar{a}_i$, b_j, and $\bar{b}_j$ may be cancelled from equation (4). To illustrate, if $a_1R = \bar{b}_1R$ then $R\bar{a}_1 = Rb_1$ and, viewing things in the center C(R), we write equation (4) in the form

$$a_1a_2\bar{a}_2\cdots a_n\bar{a}_n\bar{a}_1 = \bar{b}_1b_2\bar{b}_2\cdots b_m\bar{b}_mb_1$$

which, after cancellation, eventually becomes

$$a_2\bar{a}_2\cdots a_n\bar{a}_n = b_2\bar{b}_2\cdots b_m\bar{b}_mu$$

for some unit u necessarily in C(R). Of course, this leads to $a_1\bar{a}_1R = b_1\bar{b}_1R$. If some a_i is left invariant we obtain a similar result. In this way we can assume that each a_i and b_j in equation (4) is neither left nor right invariant. Thus $a_i\bar{a}_i$ and $b_j\bar{b}_j$ are I-atoms by Corollary 4. Theorem 6 now follows from the unique factorization of invariant elements (Proposition 2).

An LCM domain R is *modular* if, for each $0 \neq a \in R$, the interval $[aR, R]$ of principal right ideals (which is a lattice under inclusion by definition) is a modular lattice. For these rings atomic factorization is unique up to order of factors and "projective" factors as described in [1, Theorem 1.3]. Now Theorem 5.2 of [1] shows that, for an atomic modular LCM domain, atoms with two-sided bounds are projective if and only if they have the same bound. Thus Theorem 6 above may be derived from [1, Theorem 1.3] in the modular case.

To illustrate rings to which Theorem 6 applies we close with three examples of atomic LCM domains with conjugation.

EXAMPLE 1. Let R be the ring of integral quaternions. Thus R consists of all quaternions of the form $\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k$ where the α_i are either all integers or all halves of odd integers. It can be shown [5, p. 356] that R is a principal right and left ideal domain. Thus R is an atomic LCM domain with the usual conjugation.

EXAMPLE 2. Let $R = S[[x,-]]$ be the ring of skew formal power series over the ring $S = Z[i]$ of Gaussian integers. Addition in R is the usual while multiplication in R follows the commutation rule $ax = x\bar{a}$ where $\bar{a}$ is the usual conjugation in S (see [4, p. 55] for a further discussion of skew power series rings). Corollary 3.8 of [2] shows that R is an LCM domain which is clearly atomic. We extend the conjugation in S to all of R by defining $\bar{f} = f_0(-x) - f_1(x)i$, where $f = f_0(x) + f_1(x)i$ and $f_0(x), f_1(x) \in Z[[x]]$. It is not difficult to show that R is a ring with conjugation. Note that the center of R is $Z[[x^2]]$ while the set of invariant elements of R consists of all elements of the form fux^n where $f \in Z[[x^2]]$, u is a unit in R, and $n \geq 0$.

EXAMPLE 3. Let $R = F[[x,y]]$ be the ring of power series in two commuting indeterminates over a quaternion field F. Then R is an LCM domain [2]. We extend the usual conjugation on F to R in the obvious way: if $f = f_0+f_1i+f_2j+f_3k$ then $\bar{f} = f_0-f_1i-f_2j-f_3k$. Thus R is an atomic LCM domain with conjugation. This example stands in contrast to the polynomial ring $F[x,y]$ described earlier, which is an atomic integral domain with conjugation but evidently not an LCM domain.

REFERENCES

1. R. A. Beauregard, *Right-bounded factors in an* LCM *domain*, Trans. Amer. Math. Soc. **200**(1974), 251–266.

2. ———, *An analog of Nagata's Theorem for modular* LCM *domains*, Canad. J. Math. **291**(1977), 307–314.

3. ———, *When is $F[x, y]$ a unique factorization domain?*, Proc. Amer. Math. Soc. **117**(1993), 67–70.

4. P. M. Cohn, *Free rings and their relations*, (2nd ed.), Academic Press, New York, London, 1985.

5. L. Redei, *Algebra*, (Vol. 1), Pergamon Press, London, 1967.

University of Rhode Island
Kingston, Rhode Island 02881
U.S.A.