UNIQUE FACTORIZATION IN THE RING $R[x]$

RAYMOND A. BEAUREGARD

Communicated by P. Schultz

Abstract

If R is a commutative unique factorization domain (UFD) then so is the ring $R[x]$. If R is not commutative then no such result is possible. An example is given of a bounded principal right and left ideal domain R, hence a similarity-UFD, for which the polynomial ring $R[x]$ in a central indeterminate x is not a UFD in any reasonable sense. On the other hand, it is shown that if R is an invariant UFD then $R[x]$ is a UFD in an appropriate sense.

1. Introduction

It is well known that for commutative rings, R is a unique factorization domain (UFD) if and only if $R[x]$ has the same property. Several noncommutative analogs of the notion of a UFD have been proposed (see the survey in [4]). However none of these notions carries over from R to the polynomial ring without further qualification of R. Counter-examples showing that certain commutative theory does not extend in the noncommutative case are often one-sided, that is, not left-right symmetric. This is illustrated with the skew polynomial ring $R[x, \sigma]$ where R is a commutative polynomial ring $\mathbb{Z}_2[y]$ over the ring of integers modulo 2, and $\sigma: R \to R$ is the monomorphism given by $\sigma(a) = a^2$ for $a \in R$; multiplication in $R[x, \sigma]$ is defined by $xa = \sigma(a)x$ (see [5, p. 51]). In this case R is a commutative principal ideal domain but the equation $xy = y^2 x$ involving the atoms (that is,

---

irreducibles) x and y shows that $R[x, \sigma]$ is not a UFD in any reasonable sense.

Our purpose in this paper is two-fold. First, we describe a symmetric example, namely that of a bounded principal right and left ideal domain R for which $R[x]$, where x is central, is not a UFD in any reasonable sense. Here R is a similarity-UFD (see [4]). Finally, we show that this situation does not arise if R is an invariant UFD.

2. Bounded and invariant elements

Recall that in an integral domain R, a nonzero element a such that $Ra \subseteq aR$ is *right invariant*. *Left invariance* is defined similarly, and a is *invariant* if $Ra = aR$. If a is right invariant and if b is a factor of a, say $a = rbt$, then $a = btr'$ where $ra = ar'$. Thus any factor of a (right) invariant element is a left factor. An element a in R is *right bounded* if it is a factor of a right invariant element. More generally, the right ideal aR is *bounded* if it contains a nonzero two-sided ideal, the largest such being its *bound*. If this largest two-sided ideal is principal as right ideal then it has the form a^*R and a^* is the *right bound* of a, unique up to right unit factor. In this case $a \in R$ has right bound a^* if and only if $0 \neq a^*R$ is the largest member in

(1) $\{dR \mid dR \subseteq aR, \text{ and } d \text{ is right invariant}\}.$

If the collection of principal right ideals is closed under intersection then a right bounded element has a right bound [1]. If $a \in R$ is both right and left bounded it is said to be *bounded*. The left bound of a is described similarly. Notwithstanding a remark to the contrary in [5, p. 313], the left and right bounds of an element a may generate ideals that are not equal even when a is bounded by a central element (cf. [1, p. 263]). However, when these ideals are equal, the right bound of a is also the left bound of a, is invariant, and is said to be the bound of a. This is the case in an atomic 2-fir [5, p. 314]. The definition of an atomic integral domain is recalled below. Recall that a *2-fir* is an integral domain in which the sum and intersection of any two principal right (or left) ideals is again principal whenever the intersection is nonzero. In fact, in this case a^* is the bound of a if and only if aR is maximal in the collection (1). For, if d_1R and d_2R are both maximal in (1) then $d_3R = d_1R + d_2R$ is in (1) and so $d_1R = d_2R = d_3R$. We summarize the required facts as follows.

PROPOSITION 1. *Let R be an atomic 2-fir and let $a \in R$. Then a is bounded if and only if it is a factor of an invariant element. If a is bounded then a^* is its bound if and only if a^*R is maximal in the collection (1), in which case $a^*R = Ra^*$ and is unique.*

For a ring R, $\mathcal{I}(R)$ denotes the set of invariant element of R, $\mathcal{C}(R)$ denotes the center of R and $\mathcal{U}(R)$ the groups of units of R. If each nonzero element of R is (right) invariant then R is said to be (right) *invariant*, and if each nonzero element of R is (right) bounded then R is (right) *bounded*. A ring is atomic if each nonzero nonunit is a product of atoms. An *atom* of R is a nonzero nonunit that has no proper factors and $\mathcal{I}$-*atom* is a nonunit of $\mathcal{I}(R)$ that has no proper factors in $\mathcal{I}(R)$. In an atomic 2-fir a bounded element is an atom if and only if its bound is an $\mathcal{I}$-atom (cf. [5, p. 314]).

3. Polynomials over the rational quaternions

Let us consider the ring $F[x]$ of polynomials in a central indeterminate x over the field F of rational quaternions. Recall that $F[x]$ is an atomic principal right and left ideal domain and hence a similarity-UFD (see [4, p. 9]). Each element in F has the form

$$a = \alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k$$

where $\alpha_i \in Q$ and F has center $\mathcal{C}(F) = Q$, the field of rationals. Thus $a \in \mathcal{C}(F)$ if and only if $a = \bar{a}$ where $\bar{a} = \alpha_0 - \alpha_1 i - \alpha_2 j - \alpha_3 k$ is the conjugate of a. For a polynomial $f = a_0 + a_1 x + \cdots + a_n x^n$ in $F[x]$ let $\bar{f} = \bar{a}_0 + \bar{a}_1 x + \cdots + \bar{a}_n x^n$. Note that the center of $F[x]$ is $Q[x]$ and that f is central if and only if $f = \bar{f}$. In particular $f\bar{f} \in Q[x]$ and so $F[x]$ is bounded. Suppose $f \in F[x]$ is invariant. For each $a \in F$ there is an $a' \in F$ such that $af = fa'$. If f is monic, this equation is possible only if $a = a'$, so f is central in this case. Factoring the lead coefficient from any polynomial we conclude that

$$\mathcal{I}(F[x]) = \mathcal{C}(F[x])\mathcal{U}(F[x]).$$

Next we describe the $\mathcal{I}$-atoms of $F[x]$.

PROPOSITION 2. *Let* $f \in F[x]$ *and assume that* f *is not invariant. Then* f *is an atom if and only if* $f\bar{f}$ *is an* $\mathcal{I}$-*atom, in which case* $f\bar{f}$ *is the bound of* f. *Furthermore, every* $\mathcal{I}$-*atom in* $F[x]$ *that is not an atom occurs in this way.*

PROOF. Let us assume without loss in generality that f is not right invariant. If f is an atom in $F[x]$ then $f\bar{f}$ is the bound of f. To see this, note that $f\bar{f}$ is invariant. With an eye on Proposition 1, let $f\bar{f} = gk$ where $g = fh$ is right invariant and $h, k \in F[x]$. Thus $\bar{f} = hk$. However $\bar{f}$ is an atom (since $f \to \bar{f}$ is an anti-automorphism of $F[x]$). Since f is not right

invariant h must be a nonunit so that k is a unit and $f\overline{f}$ is the bound of f by Proposition 1. As such $f\overline{f}$ is an $\mathcal{I}$-atom (see the final statement of Section 2). Conversely if $f\overline{f}$ is an $\mathcal{I}$-atom and if $f = gh$ where g is an atom then $f\overline{f} = g\overline{g}h\overline{h}$ so $h\overline{h}$ and therefore h must be a unit. To prove the final assertion, let $g \in F[x]$ be an $\mathcal{I}$-atom and suppose that g is not an atom. Then $g = fh$ for some atom f. Now f is not invariant; otherwise h would also be invariant (as is easily verified), hence a unit, which gives a contradiction. The first part of this proof shows that $f\overline{f}$ is the bound of f and so must divide g. Thus $f\overline{f}$ is right associated to g.

4. A counter example

Let R be the ring of integral quaternions. Thus R is the subring of F whose elements have the form

$$a = \alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k$$

where each α_i is an integer or each $2\alpha_i$ is an odd integer. It is well known [6] that R is a principal right and left ideal domain with center $\mathcal{C}(R) = \mathbb{Z}$, the ring of integers. It is shown in [6] that $a \in \mathcal{U}(R)$ if and only if $a\overline{a} = 1$, and a is an atom in R if and only if $a\overline{a}$ is a prime in $\mathbb{Z}$. It is also shown in [6, p. 353] that the set of invariant elements of R is

$$\mathcal{I}(R) = \{n(1+i)^t u \mid n \in \mathbb{Z}, \ u \in \mathcal{U}(R), \ t = 0, 1\}.$$

Thus, up to unit factors, $1 + i$ is the only atom of R which is invariant, while the $\mathcal{I}$-atoms of R are the primes in $\mathbb{Z}$. It follows that the analogue of Proposition 2 holds in R.

Since $a\overline{a} = \alpha_0^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2 \in \mathbb{Z}$, each element of R is bounded by a central element. We now show that, although R is a bounded principal right and left ideal domain and hence a similarity-UFD, $R[x]$ is not a UFD. Consider the polynomial

$$f = ax^2 + bx + c$$

where

$$a = 1 - i + k, \qquad b = 2 + 2i, \quad \text{and} \quad c = -1 + i - 2k.$$

Then

$$f\overline{f} = a\overline{a}x^4 + (a\overline{b} + b\overline{a})x^3 + (a\overline{c} + c\overline{a} + b\overline{b})x^2 + (b\overline{c} + c\overline{b})x + c\overline{c}$$

which reduces to

(2) $$f\overline{f} = 3(x^4 + 2).$$

Since $f\overline{f}$ is an atom in $Q[x]$, $f\overline{f}$ is an $\mathscr{I}$-atom in $F[x]$ where F is the field of rational quaternions. Proposition 2 then shows that f is an atom in $F[x]$. We claim that f is an atom in $R[x]$. We have just seen that f cannot be factored into degree-one factors. Thus the only possible factorization of f in $R[x]$ is $f = dg$ (or $f = gd$) for $d \in R$. But then d is a left (or right) factor of a, b, and c and so $d\overline{d}$ is a common factor of 3, 8, and 6. Thus $d\overline{d} = 1$ and d is a unit as desired.

The argument just given shows that a polynomial which is primitive in $R[x]$ and an atom in $F[x]$ is an atom in $R[x]$. Note that $x^4 + 2 = h\overline{h}$ where

$$h = a_1 x^2 + b_1 x + c_1,$$
$$a_1 = (1 - i + j + k)/2, \qquad b_1 = 1 + i, \quad \text{and} \quad c_1 = -1 + i.$$

Since $a_1 \overline{a}_1 = 1$, h is also primitive and so an atom in $R[x]$. Also, a is an atom since $a\overline{a}$ is a prime integer. Equation (2) may be written

$$(3) \qquad\qquad f\overline{f} = a\overline{a}h\overline{h}$$

where expresses a product of two atoms equal to a product of four atoms in $R[x]$. Thus, although R is a bounded similarity-UFD, $R[x]$ is not a UFD in any reasonable sense. However, see [3, Theorem 3.1]. Equation (3) also shows that Proposition 2 is not valid in $R[x]$.

5. The invariant case

In trying to prove that $R[x]$ is a UFD if R is a commutative UFD, Gauss' Lemma (in one form or other) is crucial. Equation (2) shows the failure of Gauss' Lemma in that noncommutative but symmetric setting. If we insist that R be an invariant UFD then the situation in Equation (2) cannot arise as we will show.

If R is invariant then similarity reduces to right association (which is equivalent to left association in this case). An invariant UFD is an atomic and invariant integral domain in which any factorization into atoms is unique up to order of factors and right unit factors (that is, right association). If R is such a ring then each atom a of R is clearly prime, that is, if a divides a product then it must divide at least one factor. Furthermore we claim that

$$(4) \qquad\qquad rsR = srR$$

for all r, $s \in R$. We first establish this for the case of two atoms a and b in R. By invariance we have $ab = ba'$ for some $a' \in R$. If $aR \neq a'R$ then $aR = bR$ and $bR = a'R$ by unique factorization and this is a contradiction.

Thus $a' = au$ for some unit u and $abR = baR$ as desired. By induction we obtain

$$a_1 a_2 \cdots a_n R = a_{\sigma(1)} a_{\sigma(2)} \cdots a_{\sigma(n)} R$$

for any atoms $a_i \in R$ and any permutation σ of the subscripts. Now Equation (4) follows easily. This semicommutativity of R expressed in Equation (4) allows the usual proof of Gauss' Lemma to apply and give the following result.

PROPOSITION 3 (Gauss). *Let R be an invariant UFD.*
(1) *The product of two primitive polynomials in $R[x]$ is again primitive.*
(2) *If a is prime in R then a is prime in $R[x]$.*

Now a form of Nagata's Theorem was established in [2, Theorem 4.4] for projectivity-UFDs, namely if K is a projectivity-UFD and S is an m-system (that is, a subsemigroup of $K\backslash\{0\}$) generated by (invariant) primes of K such that KS^{-1} is a projectivity-UFD then so is K. A projectivity-UFD is an atomic integral domain in which any factorization into atoms is unique up to order of factors and projective factors. The definition of projectivity (which is not needed here) is given in [2] and [4]; projectivity is a left-right symmetric equivalence relation that reduces to similarity in a 2-fir (and hence in a principal right and left ideal domain), and to right association in an invariant integral domain (see [2]).

If R is an invariant UFD and $K = R[x]$ then Proposition 3 shows that $R^* = R\backslash\{0\}$ is an m-system generated by primes of K. Also, $K(R^*)^{-1} \cong R(R^*)^{-1}[x]$ which is a similarity-UFD (and so a projectivity-UFD). Thus $R[x]$ is a projectivity-UFD in this case. We have established the following.

PROPOSITION 4. *Let R be an invariant UFD. Then the polynomial ring $R[x]$ in a central indeterminate x is a projectivity-UFD.*

Now $R[x]$ is generally not invariant; in fact it is invariant if and only if R is commutative . Thus iteration is not possible and we obtain, for example, no conclusion about the polynomial ring in two central indeterminates over a skew field. For a noncommutative illustration of Proposition 4 we may take $R = F[[y]]$, the ring of formal power series in the central indeterminate y over the field F of rational quaternions. In this case R is an invariant UFD with exactly one (up to unit factors) atom, and $R[x]$ is a projectivity-UFD.

Added in proof

We have recently come to a conclusion: $F[x, y]$ does not have unique factorization when F is the field of rational quaternions.

References

[1] R. A. Beauregard, 'Right bounded factors in an LCM domain', *Trans. Amer. Math. Soc.* **200** (1974), 251–266.
[2] R. A. Beauregard, 'An analog of Nagata's Theorem for modular LCM domains', *Canad. J. Math.* **29** (1977), 307–314.
[3] A. W. Chatters and A. A. Jordan, 'Noncommutative unique factorisation rings', *J. London Math Soc.* (2) **33** (1986), 22–32.
[4] P. M. Cohn, 'Unique factorization domains', *Amer. Math. Monthly* **80** (1973), 1–18.
[5] P. M. Cohn, *Free rings and their relations* (2nd ed.) (Academic Press, London, 1985).
[6] L Redei, *Algebra* (Vol 1) (Pergamon Press, London, 1967).

University of Rhode Island
Kingston, R.I. 02881
USA