An AP Domain That Is Not a UFD

R. C. Daileda

1 Introduction

The notions of prime and irreducible are essential to the study of factorization in commutative rings. Roughly speaking, irreducibles are used to produce factorizations of elements, while primes are used to show that factorizations are unique. More precisely, we have the following easily proved propositions.

Proposition 1. *Let R be a commutative ring with identity. If R is Noetherian then every element in R can be written as a product of irreducible elements in R.*

Proposition 2. *Let R be an integral domain. If an element of R can be written as a product of prime elements in R then this factorization is unique, up to association and the order of the factors.*

In many algebra texts, once the definitions of prime and irreducible have been made, it is usually proven shortly thereafter that primes in a domain are irreducible but that the converse to this statement, in general, is false. The real consequence of this result is that while a ring may possess factorizations into irreducibles for each of its elements, these may not be unique. Indeed, in the typical counterexamples to "irreducible implies prime" the elements always have factorizations into irreducibles (since the rings in question are Noetherian) but *do not* have factorizations into primes. This leads to the notion of a unique factorization domain (UFD), wherein one *asserts* the uniqueness of factorizations into irreducibles. A simple consequence of the definition is that every irreducible in a UFD is, indeed, prime. In fact, it is straightforward to deduce the next result from Proposition 2. Recall that an *AP domain* is a domain in which every irreducible element is prime.

Proposition 3. *Let R be an integral domain in which every element can be written as a product of irreducible elements. Then R is an AP domain if and only if R is a UFD.*

A natural question to then ask is if putting some sort of restriction on the factorizations of elements is essential to obtaining the "irreducible implies prime" statement. That is, are all AP domains also UFDs? It is the goal of this note to prove that the answer to this question is "no" by explicitly construct a non-UFD in which every irreducible element is prime.

Let F be a field and let $F[X;\mathbb{Q}_0^+]$ denote the ring of polynomials in nonnegative rational powers of X:

$$F[X;\mathbb{Q}_0^+] = \left\{ \sum_{r\in\mathbb{Q}_0^+} a_r X^r \;\middle|\; a_r \in F, \text{ almost all zero} \right\}$$

We now state our main result.

Theorem 1. *The ring $F[X;\mathbb{Q}_0^+]$ is an AP domain but is not a UFD.*

2 Proof of the Theorem

As in $F[X]$, we can define the degree of nonzero elements in $F[X;\mathbb{Q}_0^+]$. First, given

$$0 \neq f(X) = \sum_{r\in\mathbb{Q}^+\cup\{0\}} a_r X^r \in F[X;\mathbb{Q}_0^+]$$

set

$$S(f) = \{r \mid a_r \neq 0\}.$$

Then $S(f)$ is finite by and we define

$$\deg f(X) = \max_{r\in S(f)}\{r\}.$$

It is easy to see that the degree has the familiar property $\deg f(X)g(X) = \deg f(X) + \deg g(X)$ for nonzero $f(X), g(X) \in F[X;\mathbb{Q}_0^+]$. Using the degree it is trivial to verify that $F[X;\mathbb{Q}_0^+]^\times = F$.

Given $r \in \mathbb{Q}^+$ define $\phi_r : F[X;\mathbb{Q}_0^+] \to F[X;\mathbb{Q}_0^+]$ by $\phi_r(f(X)) = f(X^r)$. It is easy to see that this is a homomorphism. In fact, we can say a good deal more.

Lemma 1. *For $r \in \mathbb{Q}^+$, ϕ_r is an automorphism of $F[X;\mathbb{Q}_0^+]$ satisfying $\deg \phi_r(f(X)) = r \deg f(X)$.*

Proof. For any $r \in \mathbb{Q}^+$, ϕ_r is an automorphism since $1/r \in Q^+$ and $\phi_{1/r}$ provides the inverse homomorphism. As for the degree statement, it is clearly true if $f(X)$ is a (nonzero) constant. So let $f(X) \in F[X;\mathbb{Q}_0^+]$ have positive degree. Then

$$\phi_r(f(X)) = \phi_r\left(\sum_{s\in S(f)} a_s X^s\right) = \sum_{s\in S(f)} a_s X^{rs}$$

which proves the result in this case. □

Since $F[X]$ can be viewed (in the obvious way) as a subring of $F[X;\mathbb{Q}_0^+]$ and these two rings have the same units, we immediately obtain the next result.

Lemma 2. *Let $f(X) \in F[X]$. If $f(X)$ is irreducible in $F[X;\mathbb{Q}_0^+]$ then $f(X)$ is irreducible in $F[X]$.*

Proof. A nontrivial factorization in $F[X]$ is a nontrivial factorization in $F[X;\mathbb{Q}_0^+]$. □

We are now in a position to prove the second part of the theorem.

Lemma 3. *Let $f(X) \in F[X;\mathbb{Q}_0^+]$ have positive degree. If $f(X)$ is irreducible it is prime.*

Proof. Suppose that $f(X)$ divides $a(X)b(X) \in F[X;\mathbb{Q}_0^+]$. Then there is a $g(X) \in F[X;\mathbb{Q}_0^+]$ so that $f(X)g(X) = a(X)b(X)$. Choose $n \in \mathbb{Z}^+$ so that $nr \in \mathbb{Z}$ for all $r \in S(f) \cup S(g) \cup S(a) \cup S(b)$. Then $\phi_n(f(X)), \phi_n(g(X)), \phi_n(a(X)), \phi_n(b(X)) \in F[X]$ and

$$\phi_n(f(X))\phi_n(g(X)) = \phi_n(f(X)g(X)) = \phi_n(a(X)b(X)) = \phi_n(a(X))\phi_n(b(X)).$$

The fact that $f(X)$ is irreducible in $F[X;\mathbb{Q}_0^+]$ and ϕ_n is an automorphism implies that $\phi_n(f(X))$ is irreducible in $F[X;\mathbb{Q}_0^+]$ as well. The preceding lemma then implies that $\phi_n(f(X))$

is irreducible in $F[X]$ as well. Since we are only dealing with polynomials at this point, and $F[X]$ is a UFD, we conclude (without loss of generality) that $\phi_n(a(X)) = c(X)\phi_n(f(X))$ for some $c(X) \in F[X]$. Applying $\phi_{1/n}$ we conclude that

$$a(X) = \phi_{1/n}(c(X))f(X).$$

That is, $f(X)$ divides $a(X)$ in $F[X;\mathbb{Q}_0^+]$ and hence $f(X)$ is prime. □

We now turn to proving the first part of the theorem. We will focus on elements of the form aX^r for $a \in F^\times$ and $r \in \mathbb{Q}^+$. Because the degree of such an element is positive, these are not units. Moreover we have the next fact.

Lemma 4. *Let $a \in F^\times$, $r \in \mathbb{Q}^+$. The only divisors of aX^r in $F[X;\mathbb{Q}_0^+]$ are those of the form bX^s where $b \in F^\times$ and $s \in \mathbb{Q}^+ \cup \{0\}$ with $s \leq r$.*

Proof. Let $f(X) \in F[X;\mathbb{Q}_0^+]$ be a divisor of aX^r. Then we can find $g(X) \in F[X;\mathbb{Q}_0^+]$ so that $aX^r = f(X)g(X)$. As above, there is a positive integer n so that $\phi_n(aX^r), \phi_n(f(X))$ and $\phi_n(g(X))$ are all elements of $F[X]$. Moreover, the fact that ϕ_n is a homomorphism implies

$$aX^{rn} = \phi_n(aX^r) = \phi_n(f(X))\phi_n(g(X)).$$

Since we are working in $F[X]$ at this point, and X is irreducible there, we must have $\phi_n(f(X)) = bX^t$ for some $b \in F^\times$ and nonnegative integer $t \leq rn$. But then

$$f(X) = \phi_{1/n}(bX^t) = bX^{t/n}$$

and $t/n \leq r$, so that $f(X)$ has the required form. This finishes the proof. □

The next lemma concludes the proof of the theorem.

Lemma 5. *The ring $F[X;\mathbb{Q}_0^+]$ is not a UFD. In particular, the element $X \in F[X;\mathbb{Q}_0^+]$ cannot be written as a product of irreducible elements in $F[X;\mathbb{Q}_0^+]$.*

Proof. We have just seen that the only divisors of X are of the form aX^r where $a \in F^\times$ and $0 \leq r \leq 1$ is a rational number. But no such element is irreducible in $F[X;\mathbb{Q}_0^+]$. For if $r = 0$ then aX^r is a unit, while if $r > 0$ then $aX^r = (aX^{r/2})X^{r/2}$ and neither of the factors on the right is a unit. Hence X cannot be written as a product of irreducibles. □