ON UNIQUE FACTORIZATION DOMAINS

JIM COYKENDALL AND WILLIAM W. SMITH

Abstract. In this paper we attempt to generalize the notion of “unique factorization domain” in the spirit of “half-factorial domain”. It is shown that this new generalization of UFD implies the now well known notion of half-factorial domain. As a consequence, we discover that the one of the standard axioms for unique factorization domains is slightly redundant.

1. Introduction and Motivation

The notion of unique factorization is one that is central in the study of commutative algebra. A unique factorization domain (UFD) is an integral domain, \( R \), where every nonzero nonunit can be factored uniquely. More formally we record the following standard definition.

**Definition 1.1.** We say that an integral domain, \( R \), is a UFD if every nonzero nonunit in \( R \) can be factored into irreducible elements, and if we have

\[
\alpha_1 \alpha_2 \cdots \alpha_n = \beta_1 \beta_2 \cdots \beta_m
\]

with each \( \alpha_i, \beta_j \) irreducible in \( R \) then

a) \( n = m \) and

b) there is a \( \sigma \in S_n \) such that \( \alpha_i = u_i \beta_{\sigma(i)} \) for all \( 1 \leq i \leq n \) where each \( u_i \) is a unit of \( R \).

We remark here that a domain with the property that every nonzero nonunit of \( R \) can be factored into irreducibles (or atoms) is said to be atomic. So a UFD is an atomic domain that satisfies conditions a) and b) above. We will use this terminology hereafter.

In 1960 the notion of the half-factorial property first appeared in a paper of Carlitz [3]. The terminology “half-factorial domain” first appeared when the results from [3] were generalized by Zaks [9]. Since that time many factorization properties have been investigated by a number of authors (see [1, 2], among others). The half-factorial property has gotten a bit of attention as well (for example see [4, 6, 7, 8]).

Historically, half-factorial domains have “half the axioms” of UFDs (namely axiom a) from above). In a question of the second author, it was asked if there are nontrivial examples of “other half” factorial domains (that is, domains that have the “other half” of the axioms UFDs: namely b) above). To be more precise (and with apologies to the reader) we make the following definition.

**Definition 1.2.** We say that the atomic integral domain, \( R \), is an OHFD if given

\[
\alpha_1 \alpha_2 \cdots \alpha_n = \beta_1 \beta_2 \cdots \beta_m
\]
with each $\alpha_i, \beta_j$ irreducible in $R$ then there is a $\sigma \in S_n$ such that $\alpha_i = u_i \beta_{\sigma(i)}$ for all $1 \leq i \leq n$ where each $u_i$ is a unit of $R$.

Intuitively speaking, an OHFD is an atomic domain where a given element may have many factorizations of different lengths, but for any positive integer $n$, the element has at most one factorization of length $n$. Since its inception, the concept of half-factorial has borne much fruit. This lends much promise to the concept of OHFD introduced above. We will show, however, that this definition is only a temporary one. It is shown in the next section that any OHFD is an HFD. Since the two properties in tandem obvious imply UFD, it will follow that any OHFD is a UFD. We find it interesting that, as a consequence, the standard definition of UFD can be weakened considerably by essentially eliminating condition a).

2. Properties of an OHFD

We note at the outset of this section that although the title is “properties of an OHFD,” the results that we present carry through in the context of monoids until Theorem 2.10. Indeed, the results numbered 2.1 through 2.9 only depend on the (multiplicative) monoid structure of our OHFD and hence could be considered results for an “OHFM.” In Theorem 2.10 and its corollaries, the additive structure of the OHFD comes into play (and so are results that apply strictly in the context of domains). In Example 2.13 we underscore the importance of the additive structure by presenting an example of a OHFM which does not have the HFM property.

To get to the heart of the factorization properties of an OHFD, we need to introduce the notion of “nondegenerate factorization”. The motivation of this approach is simply the observation that any two factorizations of nonequal lengths

$$\pi_1 \pi_2 \cdots \pi_n = \xi_1 \xi_2 \cdots \xi_m$$

gives rise to the nonequal length factorizations

$$\pi_1 \pi_2 \cdots \pi_n \alpha_1 \alpha_2 \cdots \alpha_t = \xi_1 \xi_2 \cdots \xi_m \alpha_1 \alpha_2 \cdots \alpha_t.$$

To streamline our study we make the following definition.

**Definition 2.1.** We say that the irreducible factorization

$$\pi_1 \pi_2 \cdots \pi_n = \xi_1 \xi_2 \cdots \xi_m$$

is nondegenerate if the irreducibles $\pi_i$ and $\xi_j$ are pairwise non-associate.

It is easy to see that any (nonunique) irreducible factorization can be reduced to a nondegenerate factorization by canceling the associate pairs.

**Definition 2.2.** Let $R$ be an atomic domain and $\pi_1 \in R$ an irreducible element. We say that $\pi_1$ is “long” (resp. “short”) if there is an nondegenerate irreducible factorization

$$\pi_1 \pi_2 \cdots \pi_n = \xi_1 \xi_2 \cdots \xi_m$$

with $n > m$ (resp. $n < m$).
Although it is clear that prime elements are neither long nor short, it is not clear that assigning this label to a nonprime irreducible is well-defined. We will show that for an OHFD this assignment makes sense.

**Proposition 2.3.** Suppose that \( R \) is an OHFD and let 
\[
\pi_1 \pi_2 \cdots \pi_k = \xi_1 \xi_2 \cdots \xi_m
\]
and 
\[
\alpha_1 \alpha_2 \cdots \alpha_r = \beta_1 \beta_2 \cdots \beta_n
\]
be two nondegenerate irreducible factorizations with \( k > m \) and \( n > r \). Then each \( \pi_i \) is associate to some \( \beta_j \) and conversely (this holds as well as the \( \alpha_i \)’s and \( \xi_j \)’s).

**Proof.** Let \( a := n - r \) and \( b := k - m \). Note that in the factorizations 
\[
\pi_1^a \pi_2^a \cdots \pi_k^a \alpha_1^b \alpha_2^b \cdots \alpha_r^b = \xi_1^a \xi_2^a \cdots \xi_m^a \beta_1^b \beta_2^b \cdots \beta_n^b
\]
the lengths are the same (since \( ak + br = am + bn \)). Since \( R \) is an OHFD, each \( \pi_i \) must appear on the right side of the equality. Hence each \( \pi_i \) is an associate of some \( \beta_j \) (since all \( \pi_i \)’s and \( \xi_j \)’s are nonassociate). By symmetry, it is also the case that each \( \beta_j \) is an associate of some \( \pi_i \). The same argument shows that the \( \alpha_i \)’s and \( \xi_j \)’s are associate. \( \square \)

**Proposition 2.4.** Let \( R \) be an OHFD that is not an HFD and \( \pi \in R \) a nonprime irreducible. Then \( \pi \) cannot be both long and short.

**Proof.** Using the notation from above, assume that \( \pi_1 \) is both long and short. Replace \( \alpha_1 \) by \( \pi_1 \) in the hypothesis of the above result. Hence we obtain that \( \pi_1 \) is an associate to some \( \xi_i \) (and clearly \( \pi_1 \) is self-associate). This contradicts the nondegeneracy of the first factorization. \( \square \)

**Corollary 2.5.** There are only finitely many long (resp. short) irreducibles. What is more, given any pair of factorizations 
\[
\pi_1 \pi_2 \cdots \pi_k = \xi_1 \xi_2 \cdots \xi_m
\]
with \( k > m \) and an arbitrary long (resp. short) irreducible \( \beta \) (resp. \( \alpha \)), \( \beta \) is an associate of some \( \pi_i \) (resp. \( \alpha \) is an associate of some \( \xi_j \)).

**Proof.** Again using the notation of the above we let \( \{ \pi_1, \pi_2, \ldots, \pi_k \} \) be the (long) irreducibles involved in the factorization 
\[
\pi_1 \pi_2 \cdots \pi_k = \xi_1 \xi_2 \cdots \xi_m
\]
with \( k > m \).

Now suppose that \( \beta \) is an arbitrary long irreducible. By definition, \( \beta \) is involved in some nondegenerate different length factorization (with \( \beta \) on the “long” side). By the above, \( \beta \) is an associate of some \( \pi_i \). The proof for short irreducibles is identical. \( \square \)

We now observe that any irreducible in \( R \) that is neither long nor short is necessarily prime.

**Lemma 2.6.** If \( x \in R \) be an irreducible element that is neither long nor short, then \( x \) is prime.
Proof. Assume that \( x | ab \) with \( a, b \in R \). So there is a \( c \in R \) such that

\[ cx = ab. \]

We produce irreducible factorizations \( c = c_1 c_2 \cdots c_r \), \( b = b_1 b_2 \cdots b_s \), and \( a = a_1 a_2 \cdots a_t \) and write

\[ c_1 c_2 \cdots c_r x = a_1 a_2 \cdots a_t b_1 b_2 \cdots b_s. \]

Since \( x \) is neither long nor short there are two cases to consider. In the first case, the factorizations above are of equal length (in which case they are unique) and \( x \) is an associate of some \( b_i \) or \( a_j \). In the second case the factorizations are not of equal length. In this case, since \( x \) is not associated to any long or short irreducible, the factorization must be degenerate. Hence (again) \( x \) is associated to some \( b_i \) or \( a_j \). In either case, we get that \( x | a \) or \( x | b \).

Now that we have some preliminary results in hand, we will adopt a more convenient notation. We have not demanded so far that \( \pi_i \) is non-associate to \( \pi_j \) if \( i \neq j \) (and indeed there is no reason to expect this to be true). We will now list our “canonical bad length factorization” in a form more convenient for future computational purposes:

\[ \pi_1^{a_1} \pi_2^{a_2} \cdots \pi_k^{a_k} = \xi_1^{b_1} \xi_2^{b_2} \cdots \xi_m^{b_m}, \]

with \( \sum_{i=1}^{k} a_i > \sum_{i=1}^{m} b_i \), and all irreducibles pairwise non-associate.

In the next result, we show that there is essentially one “master factorization” which itself produces all the nondegenerate factorizations of different length.

**Definition 2.7.** Let \( \{ \pi_1, \pi_2, \cdots, \pi_k \} \) and \( \{ \xi_1, \xi_2, \cdots, \xi_m \} \) respectively denote the sets of long and short irreducibles in \( R \). Among all factorizations

\[ \pi_1^{a_1} \pi_2^{a_2} \cdots \pi_k^{a_k} = \xi_1^{b_1} \xi_2^{b_2} \cdots \xi_m^{b_m}, \]

we select one with \( a_1 \) minimal and call this factorization the master factorization (MF).

**Remark 2.8.** Note that Corollary 2.5 shows that each \( a_i, b_j > 0 \).

**Proposition 2.9.** Let

\[ \pi_1^{a_1} \pi_2^{a_2} \cdots \pi_k^{a_k} = \xi_1^{b_1} \xi_2^{b_2} \cdots \xi_m^{b_m} \]

be the MF. Then any nondegenerate factorization is a power of this MF. That is, any two nondegenerate factorizations of different lengths are of the form (up to associates)

\[ \pi_1^{a_1 t} \pi_2^{a_2 t} \cdots \pi_k^{a_k t} = \xi_1^{b_1 t} \xi_2^{b_2 t} \cdots \xi_m^{b_m t}. \]

for some \( t \geq 1 \).

**Proof.** We know by Corollary 2.5 that any two nondegenerate factorizations of different lengths must be of the form

\[ \pi_1^{c_1} \pi_2^{c_2} \cdots \pi_k^{c_k} = \xi_1^{d_1} \xi_2^{d_2} \cdots \xi_m^{d_m} \]

with each \( c_i, d_j > 0 \).
We also have that \( A := \sum_{i=1}^{k} a_i > B := \sum_{i=1}^{m} b_i \) and \( C := \sum_{i=1}^{k} c_i > D := \sum_{i=1}^{m} d_i \). We apply the same technique as earlier by setting \( s := C - D \) and \( r := A - B \). We now look at the factorization

\[
p_1^{a_1s}p_2^{a_2s} \cdots p_k^{a_ks}r_1^{d_1r}r_2^{d_2r} \cdots r_m^{d_mr} = p_1^{c_1r}p_2^{c_2r} \cdots p_k^{c_kr}r_1^{b_1s}r_2^{b_2s} \cdots r_m^{b_ms}
\]

which is of equal length as \( sA + rD = AC - AD + AD - BD = AC - BC + BC - BD = rC + sB \). Hence the factorization is unique and we have that \( sa_i = rc_i \) for all \( 1 \leq i \leq k \) and \( sb_i = rd_i \) for all \( 1 \leq i \leq m \). In particular, \( \frac{s}{r}a_1 = c_1 \) and by the minimality of \( a_1 \), we have that \( \frac{s}{r} \geq 1 \). From this it follows that \( a_i \leq c_i \) for all \( 1 \leq i \leq k \) and \( b_i \leq d_i \) for all \( 1 \leq i \leq m \).

We next claim that for all \( 1 \leq i \leq k \), \( a_i \) divides \( c_i \) and for all \( 1 \leq j \leq m \), \( b_j \) divides \( d_j \) (and what is more the quotients \( \frac{s}{r}a_i \) and \( \frac{d}{b}c_i \) are all the same). We simultaneously apply the Euclidean algorithm to all of the exponents above and obtain the systems of equations

\[
c_i = q_ia_i + r_i \quad \text{and} \quad d_i = Q_ib_i + R_i
\]

where each remainder \( r_i, R_i \) satisfies \( 0 \leq r_i < a_i \) and \( 0 \leq R_i < b_i \).

We again consider the factorization

\[
p_1^{c_1s}p_2^{c_2s} \cdots p_k^{c ks} = s_1^{d_1} \cdots s_m^{d_m}.
\]

Since each \( a_i \leq c_i \) and \( b_i \leq d_i \), we can divide the left side of the above equation by \( p_1^{a_1s}p_2^{a_2s} \cdots p_k^{a ks} \) and in tandem divide the right side by \( s_1^{a_1} \cdots s_m^{a_m} \). After applying this simple algorithm a number of times, there is a first occurrence where at least one of the exponents of either \( \pi_i \) (for some \( i \)) or \( \xi_j \) (for some \( j \)) is equal to some \( r_i \) or \( R_j \). This gives the factorization

\[
p_1^{v_1s}p_2^{v_2s} \cdots p_k^{v ks} = s_1^{w_1} \cdots s_m^{w_m}
\]

where one of the \( v_i \)'s is \( r_i \) or one of the \( w_i \)'s is \( R_i \). If, at each step this \( v_i \) and \( w_i \) is 0, then we are done. If not, recall that we have shown that if the factorization above is not of equal length, every \( v_i \) is of the form \( \frac{s}{r}a_i \), and that every \( w_i \) of the form \( \frac{s}{r}b_i \) (with \( s \) and \( r \) chosen as above, \( \frac{s}{r} \geq 1 \)), we obtain that

\[
v_i \geq a_i > r_i \quad \text{and} \quad w_i \geq b_i > R_i
\]

which is a contradiction. So at some point in the algorithm, we must have achieved equal length (and hence unique) factorization. But this is clearly a contradiction since the irreducibles \( \pi_i \) are pairwise non-associate with the irreducibles \( \xi_j \). Hence we must have \( v_i = 0 \) and \( w_i = 0 \) (for all \( i \)) at the same step of the algorithm. This means that \( q_i = q_j = Q_i = Q_j \) for all \( i, j \) and \( r_i = 0 \) for all \( i, j \). This concludes the proof.

\[\square\]

We now introduce the main theorem. At this juncture, our results depart from dependence only upon the multiplicative structure of our OHFD.

**Theorem 2.10.** If \( R \) is an OHFD then \( R \) is an HFD.

**Proof.** Assume that \( R \) is an OHFD that is not an HFD. In keeping with the notation above we will let our MF be...
\[ \pi_1^{a_1} \pi_2^{a_2} \cdots \pi_k^{a_k} = \xi_1^{b_1} \xi_2^{b_2} \cdots \xi_m^{b_m}. \]

with \( \sum_{i=1}^{k} a_i > \sum_{i=1}^{m} b_i \).

There are a number of cases to consider.

**Case 1:** \( k \geq 2 \) and \( m \geq 2 \).

In this case we consider the factorization

\[ (\pi_1^{a_1} - \xi_1^{b_1})(\pi_1^{a_1} \pi_2^{a_2} \cdots \pi_k^{a_k} - \xi_2^{b_2} \xi_3^{b_3} \cdots \xi_m^{b_m}). \]

It is easy to see that \( \pi_1 \) divides the product displayed above. We also observe that \( \pi_1 \) divides neither \( \xi_1 \) nor \( \xi_2 \xi_3 \cdots \xi_m \). Indeed, if \( \pi_1 \) divides \( \xi_2^{b_2} \xi_3^{b_3} \cdots \xi_m^{b_m} \), then we have that there is a \( c \in R \) such that

\[ c \pi_1 = \xi_2^{b_2} \xi_3^{b_3} \cdots \xi_m^{b_m} \]

and since \( \pi_1 \) is not associated with any of the \( \xi_i \)'s, then this must be (after factoring \( c \)) a factorization of unequal lengths. Since the factorization is nondegenerate with respect to \( \pi_1 \) the left hand side must be the “long” side. But now, Proposition 2.9 demands that \( \xi_1 \) must divide the right hand side. So we now have that there is a \( d \in R \) such that

\[ d \xi_1 = \xi_2^{b_2} \xi_3^{b_3} \cdots \xi_m^{b_m} \]

but since \( \xi_1 \) cannot be long and short, this means that the factorization above is unique or the factorization is degenerate. In either case, \( \xi_1 \) is associated with \( \xi_i \) for some \( i > 1 \) which is a contradiction. The proof that \( \pi_1 \) does not divide \( \xi_1 \) is similar.

With this in hand we obtain that

\[ (\pi_1^{a_1} - \xi_1^{b_1})(\pi_1^{a_1} \pi_2^{a_2} \cdots \pi_k^{a_k} - \xi_2^{b_2} \xi_3^{b_3} \cdots \xi_m^{b_m}) = k \pi_1. \]

Factoring \( (\pi_1^{a_1} - \xi_1^{b_1}) \) = \( \alpha_1 \alpha_2 \cdots \alpha_s \) and \( (\pi_1^{a_1} \pi_2^{a_2} \cdots \pi_k^{a_k} - \xi_2^{b_2} \xi_3^{b_3} \cdots \xi_m^{b_m}) = \beta_1 \beta_2 \cdots \beta_t \), we obtain

\[ \alpha_1 \alpha_2 \cdots \alpha_s \beta_1 \beta_2 \cdots \beta_t = k \pi_1 \]

with \( \alpha_i \) and \( \beta_j \) irreducible. The previous argument shows that \( \pi_1 \) is not associated to any of the \( \alpha_i \)'s or \( \beta_j \)'s. So these must be factorizations of different lengths, and since \( \pi_1 \) is not associated to any irreducible on the left hand side, this means that the right hand side must be the “long” side.

We now apply Proposition 2.9 to obtain that \( \xi_1 \) must be associated with one of the irreducibles on the left side. In particular, this means that \( \xi_1 \) must divide either \( (\pi_1^{a_1} - \xi_1^{b_1}) \) or \( (\pi_1^{a_1} \pi_2^{a_2} \cdots \pi_k^{a_k} - \xi_2^{b_2} \xi_3^{b_3} \cdots \xi_m^{b_m}) \). Of course this means that \( \xi_1 \) must divide either \( \pi_1^{a_1} \) or \( \xi_2^{b_2} \xi_3^{b_3} \cdots \xi_m^{b_m} \). But if \( \xi_1 \) divides \( \pi_1^{a_1} \) then \( \pi_1^{a_1} = c \xi_1 \) and these factorizations are of different length (after factoring \( c \)). Similar to the arguments before, we have a contradiction since \( \pi_1 \) is not associated to \( \pi_1 \) if \( i \neq 1 \). Also if \( \xi_1 \) divides \( \xi_2^{b_2} \xi_3^{b_3} \cdots \xi_m^{b_m} \) then \( \xi_1 = \xi_2^{b_2} \xi_3^{b_3} \cdots \xi_m^{b_m} \) and since \( \xi_1 \) is short, it must be associated to some \( \xi_j \) for \( i > 1 \) which is a contradiction. So we cannot possess a MF of this form.

**Case 2:** \( k \geq 2 \) and \( m = 1 \) or \( k = 1 \) and \( m \geq 2 \).
These cases are symmetric and we will only show the case $k \geq 2$ and $m = 1$. In this case it is clear that $b_1 \geq 2$. First consider the MF

$$\pi_1^{a_1} \pi_2^{a_2} \cdots \pi_k^{a_k} = \xi_1^{b_1}.$$  

And now consider the factorization

$$(\pi_1^{a_1} - \xi_1)(\pi_1^{a_1} \pi_2^{a_2} \cdots \pi_k^{a_k} - \xi_1^{b_1 - 1}).$$

As before, $\pi_1$ divides this product, but neither of the two elements in the product. If we (irreducibly) factor $(\pi_1^{a_1} - \xi_1) = \alpha_1 \alpha_2 \cdots \alpha_s$ and $(\pi_1^{a_1} \pi_2^{a_2} \cdots \pi_k^{a_k} - \xi_1^{b_1 - 1}) = \beta_1 \beta_2 \cdots \beta_t$ then we have

$$\alpha_1 \alpha_2 \cdots \alpha_s \beta_1 \beta_2 \cdots \beta_t = k \pi_1.$$  

Since $\pi_1$ does not divide any of the irreducibles on the left side, the above must be factorizations of different lengths. Proposition 2.9 again shows that the right side of the equation is the long side and that $\xi_1$ must be associated to some (in fact all) nondegenerate irreducibles on the left. In particular, it must be the case that at least $b_1$ of the left irreducibles are associated to $\xi_1$ (as the master factorization has $b_1$ factors of $\xi_1$). Note that since $\xi_1$ does not divide $(\pi_1^{a_1} - \xi_1)$ it cannot be associated to any $\alpha_i$. Hence (at least) $b_1$ of the $\beta_i$’s must be associated to $\xi_1$. This implies that $\xi_1^{b_1}$ divides $(\pi_1^{a_1} \pi_2^{a_2} \cdots \pi_k^{a_k} - \xi_1^{b_1 - 1})$. Since $\xi_1^{b_1}$ divides $\pi_1^{a_1} \pi_2^{a_2} \cdots \pi_k^{a_k}$, it must divide $\xi_1^{b_1 - 1}$ which is a contradiction.

**Case 3:** $k = m = 1$.

In this final case, our MF is of the form

$$\pi^a = \xi^b$$

with $a > b \geq 2$. In this case we note that any $R$–linear combination of $\pi$ and $\xi$ is a nonunit (indeed, note that if $M$ is a maximal ideal of $R$ such that $\pi \in M$ then certainly $\xi \in M$).

We consider

$$(\pi - \xi)(\pi^{a - 1} - \xi^{b - 1}).$$

As before, $\pi$ divides this product and we get

$$(\pi - \xi)(\pi^{a - 1} - \xi^{b - 1}) = k \pi,$$

and as before we factor $(\pi - \xi) = \alpha_1 \alpha_2 \cdots \alpha_s$ and $(\pi^{a - 1} - \xi^{b - 1}) = \beta_1 \beta_2 \cdots \beta_t$ to obtain

$$\alpha_1 \alpha_2 \cdots \alpha_s \beta_1 \beta_2 \cdots \beta_t = k \pi.$$  

Note that, similarly to the previous cases, $\pi$ cannot divide any of the irreducibles on the left (as, again, this forces $\pi$ to be a divisor of either $(\pi - \xi)$ or $(\pi^{a - 1} - \xi^{b - 1})$ and the techniques of earlier cases show that this cannot happen). Hence these (after factoring $k$) are two factorizations of different lengths. Proposition 2.9 show that each $\alpha_i$ and $\beta_j$ is divisible by $\xi$ hence $\xi$ divides $\pi - \xi$.

Hence $\xi$ divides $\pi$ and this is a contradiction.

This exhausts the cases for the form of a MF, and hence there is no OHFD that is not an HFD. \qed
Here is a rather striking corollary.

**Corollary 2.11.** An integral domain is an OHFD if and only if it is a UFD.

*Proof.* \((\Leftarrow)\) is obvious. On the other hand, if \(R\) is an OHFD then \(R\) is an HFD and clearly these two properties in tandem imply UFD. \(\square\)

One interesting consequence of this is that it suffices to declare that an atomic integral domain is a UFD if any two equal length factorizations are the same (up to units and reordering). So in a certain sense, the condition \(a)\) from the definition of UFD in the introduction is not needed.

Another useful result is that we can now retire the definition of OHFD (since the concept is equivalent to UFD). Before we dispose of it, however, we list an immediate corollary that is of some theoretical and aesthetic interest.

**Corollary 2.12.** Any atomic domain that is not an UFD has two different factorizations of the same length.

*Proof.* If not then \(R\) is an OHFD and hence a UFD. \(\square\)

As a final note, it should be pointed out that although we have retired this “OHFD” notion for integral domains, this notion of “OHFM” for monoids can exist apart from the notion of “UFM” (see [5] for a far more complete discussion factorization in the setting of monoids). It is of interest to once again point out that our results (until Theorem 2.10) can be couched in terms of monoid factorizations.

We conclude with an example highlighting contrast. This example, in conjunction with the proof of the main theorem, plainly illustrates some of the hazards that can appear in making the transition between the setting of monoids to the setting of integral domains.

**Example 2.13.** Consider the natural numbers \(\mathbb{N}\) and consider the additive submonoid of \(\mathbb{N}\) generated by \(\{n, m\}\) where \(2 \leq n < m\) and \(\gcd(n, m) = 1\). To make comparisons with the earlier part of this paper easier, we now consider the multiplicative monoid generated by \(a = e^n\) and \(b = e^m\).

In the monoid \(M = \langle a, b \rangle\), the only two irreducibles are the elements \(a\) and \(b\) and hence the only nondegenerate factorizations are of the form

\[a^x = b^y.\]

In fact, \(a\) is “long” and \(b\) is “short” since \(a^m = b^n\) and \(n \leq m\), and this particular factorization \((a^m = b^n)\) is easily seem to be the MF for this monoid and is also certainly an example of factorizations of the same element possessing different lengths.

To see that \(M\) is an OHFM we suppose that we have the factorization

\[a^{k_1}b^{k_2} = a^{s_1}b^{s_2}\]

with \(k_1 + k_2 = s_1 + s_2\).

This gives that \(k_1n + k_2m = s_1n + s_2m\), which in turn yields

\[(k_1 - s_1)n = (s_2 - k_2)m.\]

Since \(n\) and \(m\) are relatively prime, we have that there is an \(x \in \mathbb{Z}\) such that

\[nx = s_2 - k_2\]
and

\[ mx = k_1 - s_1. \]

From this we obtain

\[(m - n)x = (k_1 + k_2) - (s_1 + s_2) = 0 \]

since the factorizations are of the same length. Hence \( x = 0 \) (since \( m \neq n \)) and so \( s_1 = k_1 \) and \( s_2 = k_2 \). This gives the uniqueness of the factorization.

References