U-FACTORIZATIONS IN COMMUTATIVE RINGS WITH ZERO DIVISORS

Nicholas Roersma

Wabash College
Crawfordsville, IN 47933-0352 U.S.A.

ABSTRACT.For a commutative ring R with identity, we define an alternate method of factorization, called a U-factorization. We determine all possible rearrangements of a U-factorization and extend several finite factorization characterizations to U-factorizations.

1. Introduction

Some mathematicians have successfully classified a portion of the feasible swaps for finite U-factorizations (for example, see [3]). The first portion of the paper extends these results and classifies all possible swaps. In [1] and [3], properties of rings and domains are extended into U-factorization properties of rings, namely bounded factorizations rings and finite factorization rings. In contrast, in this paper the implications of properties of a particular ring (being a principal ideal ring, présimplifiable ring, or a direct product of rings) with respect to U-factorizations are explored.

Let R be a commutative ring with unity throughout the paper. Since principal ideals will be considered often throughout this paper, recall that the *principal ideal* generated by $a \in R$ is $(a) = \{ar \mid r \in R\}$. The set of units of R will be denoted as $U(R)$. If $a \in R$ is a nonunit, then by a *factorization of* a we mean $a = a_1 a_2 \cdots a_s$ where each $a_i \notin U(R)$.

Definition 1.1. *Two elements $a, b \in R$ are said to be* ***associates*** *if $a \mid b$ and $b \mid a$; thus $(a) = (b)$ which will be denoted by $a \sim b$.*

Definition 1.2. *A nonunit $a \in R$ is* ***irreducible*** *(or an* ***atom****) if whenever $a = bc$ implies $a \sim b$ or $a \sim c$.*

This is a less restrictive definition of an irreducible element than most may be accustomed to. Elements of a ring being associates will be the only relation between two elements explored in this paper. Stronger conditions of strongly associate and very strongly associate can be found in [2].

Factorizations are well behaved for the most part, but consider $3 \in \mathbb{Z}_6$. In $\mathbb{Z}_6$, 3 is irreducible and trivially $3 = 3$ is a valid factorization. However, $3 = 3 \cdot 3 = 3^2$

1991 *Mathematics Subject Classification.* 13A99.

which is another valid factorization; thus 3 is idempotent, an element $x \in R$ such that $x^2 = x$. Since 3 is idempotent, $3 = 3^n$ for any $n \in \mathbb{N}$. Yet the ring itself is finite, but the factorization of an element can be arbitrarily long. U-factorizations help alleviate this problem.

Definition 1.3. *For a nonunit $r \in R$, if $r = a_1 a_2 \cdots a_n b_1 b_2 \cdots b_m$ where $a_i, b_j \in R$ that are nonunits, then $r = a_1 a_2 \cdots a_n \lceil b_1 b_2 \cdots b_m \rceil$ is a **U-factorization** if:*

(1) *$a_i(b_1 b_2 \cdots b_m) = (b_1 b_2 \cdots b_m)$ for $1 \leq i \leq n$, and*
(2) *$b_j(b_1 b_2 \cdots \hat{b}_j \cdots b_m) \neq (b_1 b_2 \cdots \hat{b}_j \cdots b_m)$ for $1 \leq i \leq m$ (where $\hat{b}_j$ denotes the removal of the element).*

We will call the a_i's inessential divisors of this U-factorization of r, and b_j's essential divisors of this U-factorization of r.

Now in $\mathbb{Z}_6$, $3 = 3^n \lceil 3 \rceil$ for any $n \in \mathbb{N}$ since $((3 \cdot 3)) = (3)$. The length of the U-factorization is measured by counting the number of essential divisors. This example yields a U-factorization of length one. Clearly, this U-factorization is better behaved with one essential divisor than the regular factorization that is arbitrarily long (though there remains an arbitrary number of inessential divisors).

The idea of a U-factorization seems a little odd at first; however, the factorization gives more information than a normal factorization. As defined, the essential divisors of the factorization give us the most interesting information, creating an element whose generated ideal is equal to that of the ideal generated by the factorized element. The inessential divisors simply take us from the ideal to the specific element. The relation between a normal factorization and a U-factorization is well behaved. The following lemma and proof can be found in [1].

Lemma 1.4. *Any factorization of $r \in R$ can be rearrranged to form a U-factorization of r.*

Lemma 1.4 leads to the easy creation of U-factorizations.

Example 1.5. In $\mathbb{Z}$, $12 = 2 \cdot 6 = 3 \cdot 4$. Since $(12) \neq (2), (3), (4)$, or (6), $12 = \lceil 2 \cdot 6 \rceil = \lceil 3 \cdot 4 \rceil$. Notice that there are no inessentials in these U-factorizations. Even though $(12) = (-12)$, we have that $12 = -1\lceil -12 \rceil$ is not a valid U-factorization because all the elements of the U-factorization must be non-units and $-1 \in U(\mathbb{Z})$. Corollary 3.6 will show all U-factorizations in $\mathbb{Z}$ have no inessential divisors.

2. Finite U-factorization Properties

Given a U-factorization, is it possible to swap essential divisors for inessential divisors? In Example 1.5, this is not possible since we have no inessential divisors. That no rearrangements are possible given a U-factorization without inessential divisors follows simply from the definition of a U-factorization.

Lemma 2.1. *If $r = \lceil b_1 b_2 \cdots b_m \rceil$ is a U-factorization, then no other U-factorization is possible via rearrangement of this U-factorization.*

Proof. By definition of a U-factorization: $b_i(b_1 b_2 \cdots \hat{b}_i \cdots b_m) \neq (b_1 b_2 \cdots \hat{b}_i \cdots b_m)$ for $1 \leq i \leq m$.WLOG consider $b_1 b_2 (b_3 b_4 \cdots b_m)$. Here
$(b_3 b_4 \cdots b_m) \supseteq (b_2 b_3 b_4 \cdots b_m) \supsetneq (b_1 b_2 b_3 b_4 \cdots b_m)$ and
$(b_3 b_4 \cdots b_m) \supseteq (b_1 b_3 b_4 \cdots b_m) \supsetneq (b_1 b_2 b_3 b_4 \cdots b_m)$. Together these give

$r \neq b_1b_2\lceil b_3b_4\cdots b_m\rceil$. Similar arguments can be made for any number of attempted removed essential divisors. ☐

Now consider the example given in the introduction: $3 = 3\lceil 3\rceil$ in $\mathbb{Z}_6$. Note that we can swap the essential divisor for the inessential divisor, although the swap is trivial. The question remains: When can we possibly rearrange a given U-factorization, and if a rearrangement of a U-factorization is possible what are the implications?

Lemma 2.1 is the first step in showing that U-factorizations and groupings of inessentials or essentials behave as one would expect. Similar containment arguments used in the proof of Lemma 2.1 are used to prove the following lemma found in [1].

Lemma 2.2. *The following statements are true for a commutative ring R:*

(1) $r = a_1a_2\cdots a_n\lceil b_1b_2\cdots b_m\rceil$ *is a U-factorization if and only if* $r = (a_1a_2)a_3\cdots a_n\lceil b_1b_2\cdots b_m\rceil$ *is a U-factorization, i.e., we can treat all inesseantials as one inessential.*

(2) *If* $r = a\lceil b_1b_2\cdots b_m\rceil$ *is a U-factorization, then* $r = a\lceil (b_1b_2)b_3\cdots b_m\rceil$ *is a U-factorization.*

(3) *If* $r = a\lceil (b_1b_2)b_3\cdots b_m\rceil$ *is a U-factorization, then, either* $r = a\lceil b_1b_2\cdots b_m\rceil$, $r = ab_1\lceil b_2b_3\cdots b_m\rceil$, *or* $r = ab_2\lceil b_1b_3\cdots b_m\rceil$ *is a U-factorization.*

Example 2.3. In $\mathbb{Z}_{30}$, $10 = 2\lceil 4\cdot 5\rceil = 2\lceil (2\cdot 2)\cdot 5\rceil$, but $10 \neq 2\lceil 2\cdot 2\cdot 5\rceil$ because $2(2\cdot 5) = (20) = (10) = (2\cdot 5)$ so it violates the definition of a U-factorization; however, $10 = 2\cdot 2\lceil 2\cdot 5\rceil = 4\lceil 2\cdot 5\rceil$ as parts (1) and (3) of Lemma 2.2 guarantee.

These may appear to be the only interesting, though trivial, rearrangements possible for U-factorizations. However, the next example illustrates that it is possible for essential and inessential divisors to be swapped, and Lemma 2.5 will give a necessary and sufficient condition for a simple swap.

Example 2.4. In $\mathbb{Z}_{12}$, $3 = 3\cdot 9$. Here $(3) = (9)$. Therefore, $3 = 3\lceil 9\rceil = 9\lceil 3\rceil$. Moreover, $9 = 3\lceil 3\rceil$. Though again trivial, we can swap the inessential for the essential divisors.

Lemma 2.5. *Let* $0 \neq r = a\lceil b\rceil$ *in* R*. Then* $r = b\lceil a\rceil$ *if and only if there exists an idempotent* $e \in R$ *such that* (a), (b), (r), *and* (e) *are all equal.*

Proof. ($\Longrightarrow$) Assume $r = a\lceil b\rceil = b\lceil a\rceil$. By definition of a U-factorization, $(r) = (a) = (b)$, and $r = ab$. Now $(r) = (ab) = (a)(b) = (a)(a)$ (since $(a) = (b)$) $= (a)^2$. From this, there exist $s, t \in R$ such that $as, at \in (a)$ and $as\cdot at = a$. Consider $sat = s(as\cdot at)t = (sat)^2$. Thus sat is idempotent in R. Now $a\cdot sat = a$ gives $a \in (sat)$ and $a\cdot st = sat$ gives $sat \in (a)$: Therefore, $(r) = (a) = (sat)$, and since r is a nonzero nonunit, sat is a nontrivial idempotent.

($\Longleftarrow$) Let $r = a\lceil b\rceil$ and $(a) = (b) = (r) = (e)$ where e is some idempotent. Clearly, $b(a) = (ba) = (b)(a) = (e)(e) = (e)^2 = (e) = (a)$. Therefore, $r = b\lceil a\rceil$ is a U-factorization of r. ☐

Lemma 2.5 yields an extremely well behaved relationship, namely, the ring must have a nontrivial idempotent element in order to even consider swapping all essential divisors for all inessential divisors. Reviewing Example 2.4, we see that $(3) = (9)$ and $9 = 9^2 \bmod(12)$. Now we consider U-factorizations of a nonunit $r \in R$ where $r = abc$.

Corollary 2.6. *Let $r \in R$ be a nonzero nonunit and $r = abc$:*

1. *If $r = \lceil abc \rceil$, then no rearrangements of the U-factorization are possible.*
2. *Given $r = a\lceil bc \rceil$, then $r = bc\lceil a \rceil$ if and only if there exists an idempotent $e \in R$ such that (a), (b), (r), and (e) are all equal.*

Proof. (1) See Lemma 2.1 .

(2) See Lemma 2.2 parts (1) and (2) and Lemma 2.5. □

Corollary 2.6 part (2) also covers the case when $r = bc\lceil a \rceil = a\lceil bc \rceil$. Nonetheless, Corollary 2.6 obviously does not cover all feasible rearrangements of three elements because $r = a\lceil bc \rceil = b\lceil ac \rceil$ could possibly occur. The following examples illustrate when this arrangement is and is not possible.

Example 2.7. In $\mathbb{Z}_{24}$, only two elements can be written with the above rearrangement. The first is $16 = 2\lceil 2 \cdot 4 \rceil$ with a trivial rearrangement of switching 2 for 2. And, $8 = 4\lceil 2 \cdot 4 \rceil = 2\lceil 4 \cdot 4 \rceil$. Notice that $(16) = (8)$ and that 16 is an idempotent in $\mathbb{Z}_{24}$. The other idempotent of the ring is 9 which cannot be written with this rearrangment. Although $(9) = (3) = (15) = (21)$, simple algebra shows that none of these numbers may yield a U-factorization of 9. Particularly $9 \neq \lceil ab \rceil$ because either $(9) = (a) = (b)$, which implies $9 = a\lceil b \rceil = b\lceil a \rceil$ from Lemma 2.5, or $b \in U(R)$.

Example 2.8. There are many examples of this rearrangment in $\mathbb{Z}_6 \times \mathbb{Z}_8$. One is $(4, 2) = (2, 1)\lceil (2, 1)(1, 2) \rceil$ having a trivial rearrangement, but note that $(4, 2)^2 = (4, 4) \neq (4, 2)$ and, even stronger, $(4, 2)^2 = (4, 4) \nsim (4, 2)$. The same is true for $(2, 2)$, $(2, 6)$, and $(4, 6)$, the associates of $(4, 2)$. Hence, this rearrangment of the form $r = a\lceil bc \rceil = b\lceil ac \rceil$ need not have the strict property of Lemma 2.5. For another nontrivial rearrangement, again with a nonidempotent ideal, we find that $(3, 4) = (3, 1)\lceil (3, 3)(1, 4) \rceil = (3, 3)\lceil (3, 1)(1, 4) \rceil$.

Notice that in each example, we have $r = a\lceil bc \rceil = b\lceil ac \rceil$ where either $(a) = (b)$ or $a \in (b)$. Is this condition necessary and sufficient? No, it is not because Example 2.7 gave $8 = 2\lceil 4 \cdot 4 \rceil$ in $\mathbb{Z}_{24}$ where $(2) \neq (4)$ and $2 \notin 4$ even though the rearrangement $8 = 4\lceil 2 \cdot 4 \rceil$ is possible. However, the condition is sufficient.

Lemma 2.9. *If $r = a\lceil bc \rceil$ and $a \in (b)$, then $r = b\lceil ac \rceil$ or $r = bc\lceil a \rceil$.*

Proof. Let $r = a\lceil bc \rceil$ and $a \in (b)$. Then there exists some $d \in R$ such that $a = bd$. So, $(ac) = (bdc)$, a subset of (bc). If $(ac) = (bc)$, then we are done. So assume $(ac) \subsetneq (bc)$. Here, by definition of U-factorization, $(r) = (bc) \supsetneq (ac) \supseteq b(ac) = (abc) = (r)$. This yields $(r) \supsetneq (r)$, an obvious contradiction. Hence, $(ac) = (bc) = (r)$. From assumption $r = abc$ and $(r) \neq (c)$. If $(r) \neq (a)$, then we have $r = b\lceil ac \rceil$. If $(r) = (a)$, then we have $r = bc\lceil a \rceil$. □

Lemma 2.9 gives a simple rule for creating the desired rearrangements. The opposite condition, $r = a\lceil bc \rceil$ and $b \in (a)$ does not necessarily imply $r = b\lceil ac \rceil$ as shown in the next example.

Example 2.10. In $\mathbb{Z}_{36}$, consider $18 = 3\lceil 9 \cdot 2 \rceil$. Here $9 \in (3)$ and $9\lceil 3 \cdot 2 \rceil = 9\lceil 6 \rceil$ is not a U-factorization of 18. This is because $(18) = \{0, 18\}$ so $6 \notin (18)$ implying $(6) \neq (18)$.

Lemma 2.9 gives us a condition when $r = a\lceil bc\rceil$ yields $b\lceil ac\rceil$. Nonetheless, we still are without a necessary condition given the rearrangement. Lemma 2.11 provides such a necessary condition.

Lemma 2.11. *If $r = a\lceil bc\rceil = b\lceil ac\rceil$, then there exists a proper nontrivial ideal I such that $a, b \in I$.*

Proof. Let $r = a\lceil bc\rceil = b\lceil ac\rceil$. Consider the subset $(a, b) = \{ax + by \mid x, y \in R\}$. First, show (a,b) an ideal. For any $x, y, s, t \in R$, $(ax + by) - (as + bt) = ax - as + by - bt = a(x - s) + b(y - t) = am + bn \in I$ for some $m, n \in R$. For any $x, y, r \in R$, $r(ax + by) = rax + rby = a(rx) + b(ry) = ac + bd \in I$ for some $c, d \in R$. Therefore, I is an ideal by the two step test.

Assume $(a, b) = R$. Then there exists $s, t \in R$ such that $as + bt = 1$. Multiply through by c yields $c(as + bt) = c1$ implying $acs + bct = c$. From assumption and the definition of a U-factorization, we have that $(r) = (bc) = (ac)$ so there exist $m, n \in R$ such that $rm = ac$ and $rn = bc$. Now $c = (ac)s + (bc)t = (rm)s + (rn)t = r(ms + nt)$. Thus, $r \mid c$. From assumption we have $c \mid r$, and together, $r \sim c$ or $(r) = (c)$. This contradicts that $r = a\lceil bc\rceil$ is a U-factorization. Therefore, $(a, b) \subsetneq R$. Now let $(a, b) = I \subsetneq R$. □

Lemma 2.12. *Let R be a principal ideal ring (PIR). If $r = a\lceil bc\rceil = b\lceil ac\rceil$, then a, b share a common irreducible divisor.*

Proof. From Lemma 2.11 we know that $(a, b) = I$, a nontrivial, proper ideal. Since R is a PIR, every ideal is of the form (x) where $x \in R$ implies there exists a $d \in R$ such that $I = (a, b) = (d)$. In [4], Gallian shows that in a PIR, any strictly increasing chain of ideals $I_1 \subset I_2 \subset I_3 \subset \dots$ must be finite in length– i.e., every ideal is contained in some maximal ideal. So let $(d) \subset M \neq R$, where M is a maximal ideal. Since R is a PIR, $M = (m)$ for some $m \in R$. Moreover, from [4], M is maximal gives m is irreducible. Now we have that $a, b \in (m)$ implies that there exist $x, y \in R$ such that $mx = a$ and $my = b$. This implies $m|a$ and $m|b$. Therefore, a and b share an irreducible divisor m. □

The corollary is very convenient because some of our easiest examples of rings are PIRs. In fact, all the previous examples in this paper have been PIRs. However, if Lemma 2.11 were stronger, it would allow us to know exactly when and what rearrangements of a given finite U-factorization are possible. This is because Lemma 2.11 is a crucial portion in the following lemmas that lead to the classification of all finite U-factorizations. We will begin this classification process by showing conditions for all possible rearrangements of U-factorizations containing three elements. Then we will do the same for U-factorizations containing four elements. Finally we'll extend this result to all finite U-factorizations.

Lemma 2.13. *Let $r = ab\lceil c\rceil$. Then $r = ac\lceil b\rceil$ if and only if there exists an idempotent $e \in R$ such that (b), (c), (r), and (e) are all equal.*

Proof. The proof is similar to that of Lemma 4. □

Theorem 2.14. *Let $r, a, b, c \in R$ and $r = abc$. Then, WLOG, the possible U-factorizations and rearrangements are listed below:*

(1) *If $r = \lceil abc\rceil$, then no rearrangements are possible.*

(2) *If* $r = a\lceil bc\rceil$, *then, either* $r = bc\lceil a\rceil$ *if and only if there exists an idempotent* $e \in R$ *such that* (bc), (a), (r), *and* (e)*are all equal,* $r = b\lceil ac\rceil$ *and there exists a proper nontrivial ideal* I *such that* $a, b \in I \subsetneq R$, *or no rearrangements are possible.*

(3) *If* $r = ab\lceil c\rceil$, *then, either* $r = ac\lceil b\rceil$ *if and only if there exists an idempotent* $e \in R$ *such that* (c), (b), (r), *and* (e) *are all equal,* $r = c\lceil ab\rceil$ *if and only if there exists an idempotent* $e \in R$ *such that* (c), (ab), (r), *and* (e) *are all equal, or no rearrangements are possible.*

This classifies all the possible rearrangements of U-factorizations with three elements. It very easily extends to the classification of all possible rearrangements of U-factorizations with four elements.

Lemma 2.15. *Let* $r, a, b, c, d \in R$ *and* $r = abcd$. *Then, WLOG, the possible U-factorizations and rearrangements are listed below:*

(1) *If* $r = a\lceil bcd\rceil$, *then, either* $r = bcd\lceil a\rceil$ *if and only if there exists an idempotent* $e \in R$ *such that* (a), (bcd), (r), *and* (e) *are all equal,* $r = b\lceil acd\rceil$ *there exists a proper nontrivial ideal* I *such that* $a, b \in I$, $r = bc\lceil ad\rceil$ *there exists a proper nontrivial ideal* I *such that* $a, bc \in I$, *or no rearrangements are possible.*

(2) *If* $r = ab\lceil cd\rceil$, *then, either* $r = cd\lceil ab\rceil$ *if and only if there exists an idempotent* $e \in R$ *such that* (cd), (ab), (r), *and* (e) *are all equal,* $r = c\lceil abd\rceil$ *there exists a proper nontrivial ideal* I *such that* $ab, c \in I$, *or* $r = ac\lceil bd\rceil$ *there exists a proper nontrivial ideal* I *such that* $b, c \in I$, *or or no rearrangements are possible.*

Proof. The proof of (1) follows from Lemma 2.5 and Lemma 2.11, and the proof of (2) is clear. □

Now we've shown conditions for any possible swap of U-factorizations with four or fewer elements. This can easily be extended to any number of finite elements, for in any swap we have four types of elements: inessentials to remain inessentials, inessentials to be swapped for essentials, essentials to be swapped for inessentials, and essentials to remain essentials. The proofs of each feasible swap would simply combine all the element in one group (say inessentials to remain inessentials) and create one element through their product as Lemma 2.2 allows. We can now think of this as a swap of four elements, not of n elements. Therefore, all the possible rearrangements are summarized in Lemma 2.1, Lemma 2.5, and Lemma 2.11.

As previously mentioned, if there exists a stronger implication (possibly necessary and sufficient) for the case of $r = a\lceil bc\rceil = b\lceil ac\rceil$ in Lemma 2.11, we strengthen the implication for all finite swaps. Stronger implications do occur when the ring has some stronger properties, as when a ring is a PIR in Lemma 2.12.

3. Direct Products and U-factorizations

Earlier, it was mentioned that all the examples in this paper are PIRs. Most of the examples are even more well behaved than arbitrary PIR rings. Indeed they are présimplifiable rings or a direct product of a finite number of présimplifiable rings.

Definition 3.1. *A ring R is said to be* ***présimplifiable*** *if for any $x \in R$, $x = xy$ implies either $x = 0$ or $y \in U(R)$.*

Lemma 3.2. *Any integral domain D is présimplifiable.*

Proof. Left to the reader. □

The idea behind présimplifiable rings is to create a ring that is nearly an integral domain, saving as many domain properties as possible while still allowing zero-divisors. Many of the results for domains transfer easily to présimplifiable rings, and by Lemma 3.2, all results for présimplifiable rings are true for domains. In [3], Axtell shows that domains cannot have inessential divisors. This will be shown to be true for présimplifiable rings.

Lemma 3.3. *A ring R is présimplifiable if and only if for every nonzero $a, b \in R$, $(a) = (b)$ and $a = bc$ implies $c \in U(R)$.*

Proof. ($\Longrightarrow$) In a présimplifiable ring R, let $(a) = (b)$. Then there exists $d \in R$ such that $ad = b$. Now $a = bc = (ad)c = a(dc)$ gives $dc \in U(R)$ since R is présimplifiable. Therefore, $d, c \in U(R)$.

($\Longleftarrow$) Let $0 \neq a, b \in R$ a ring where $(a) = (b)$ and $a = bc$ implies $c \in U(R)$. Simply let $b = a$ and it follows that R is présimplifiable. □

Theorem 3.4. *In R, every U-factorization of a nonzero nonunit element has no inessential divisors if and only if R is a présimplifiable ring.*

Proof. ($\Longleftarrow$) Let R be a présimplifiable ring and $0 \neq r \in R$ a nonunit. By parts (1) and (2) of Lemma 2.2, we only need consider $r = a\lceil b\rceil$ with $a, b \in R$. So, if $r = a\lceil b\rceil$ with $a, b \in R$, then $(r) = (b)$ implies that for any $c \in R$, if $r = bc$, then $c \in U(R)$ by Lemma 3.3. Therefore $a \in U(R)$. However, this a contradiction, since $r = a\lceil b\rceil$ implies $a \notin U(R)$ by definition of a U-factorization. Therefore, in a présimplifiable rings there exists no inessential divisors in the U-factorizations.

($\Longrightarrow$) Let every U-factorization in R of a nonzero nonunit have no inessential divisors. Consider nonunit nonzero $r \in R$ such that $r = ra$. Clearly $(r) = (r)$. If $a \notin U(R)$, then $r = a\lceil r\rceil$. This U-factorization of r has an inessential divisor which contradicts our assumption. Thus, $r = a\lceil r\rceil$ is not a valid U-factorization implying $a \in U(R)$. Hence, for every nonzero nonunit $r \in R$, $r = ra$ implies that $a \in U(R)$. Thus, R is a présimplifiable ring. □

Lemma 3.2 easily yields examples of these properties, $\mathbb{Z}$. In fact, Lemma 3.2 was used to create Example 1.5. However, the following finite product property for présimplifiable rings is more useful.

Theorem 3.5. *Let $R = \prod_{i=1}^{n} R_i$ where R_i is présimplifiable for $1 \leq i \leq n$. Then a nonzero nonunit $r = (r_1, r_2, \ldots, r_n)$ has no inessential divisors if and only if $r_i \neq 0$ for $1 \leq i \leq n$.*

Proof. ($\Longleftarrow$) Consider a nonzero nonunit $r = (r_1, r_2, \ldots, r_n) \in R$ and $r_i \neq 0$ for $1 \leq i \leq n$. If $r = a\lceil b\rceil$ with $a, b \in R$ where $a = (a_1, a_2, \ldots, a_n)$ and $b = (b_1, b_2, \ldots, b_n)$, then $(r_i) = (b_i)$ for $1 \leq i \leq n$.

If r_i is a nonunit, then $r_i = a_i b_i$ and $(r_i) = (b_i)$. From Theorem 3.4, $a_i \in U(R_i)$. Therefore, for a nonzero nonunit r_i, it follows that $a_i \in U(R_i)$. If r_i is a unit, then $r_i = a_i b_i$. Since $r_i \in U(R_i)$, it follows that $a_i, b_i \in U(R_i)$.

Therefore, $r_i \in U(R_i)$ implies $a_i \in U(R_i)$. Therefore, all a_i are units (since $r_i \neq 0$ for $1 \leq i \leq n$) yielding that $a \in U(R)$. Thus, $r \neq a\lceil b \rceil$ since it is not a valid U-factorization because a is a unit. So, a U-factorization of r has no inessential divisors.

($\Longrightarrow$) Consider a nonunit $r = (r_1, r_2, \ldots, r_n) \in R$, such that $r_i = 0$ for some $1 \leq i \leq n$. WLOG let $r_1 = 0$ and let 1_i be the unity of R_i. Then $r = (0, r_2, r_3, \ldots, r_n) = (0, 1_2, 1_3, \ldots, 1_n)\lceil (0, r_2, r_3, \ldots, r_n) \rceil$ and clearly $(0, 1_2, 1_3, \ldots, 1_n) \notin U(R)$. □

Now we may construct the conditions that form the basis for all the examples in this paper.

Corollary 3.6. *Any U-factorization of a nonzero nonunit $r \in \mathbb{Z}$ or $\mathbb{Z}_{p^n}$, where p is a prime and n a natural number, has no inessential divisors.*

Proof. $\mathbb{Z}$ is an integral domain so it is présimplifiable by Lemma 3.2. Consider $\mathbb{Z}_{p^n}$ where p is a prime and n a natural number and let x be a nonzero nonunit of $\mathbb{Z}_{p^n}$. By definition of a nonunit of $\mathbb{Z}_{p^n}$, $p \mid x$, so $x = p^m k$, for some $m, k \in \mathbb{N}$ and $p \nmid k$, $m < n$. If $x = xy$, $y \in \mathbb{Z}_{p^n}$, then $x(y-1) = 0 \bmod (p^n)$ or $x(y-1) = p^n l$, $l \in \mathbb{N}$. Rearrangement yields $(p^m k)(y-1) = p^n l$ implying $k(y-1) = p^{n-m} l$. Finally, $p \mid k(y-1)$. From Euclid's lemma $p \mid k$ or $p \mid (y-1)$. Since $p \nmid k$, $p \mid (y-1)$ which implies that $p \nmid y$. Since $p \nmid y$, $y \in U(\mathbb{Z}_{p^n})$. Therefore, for a nonunit x, $x = xy$ implies $x = 0$ or y a unit and so $\mathbb{Z}_{p^n}$ is présimplifiable by definition. It now follows from Theorem 3.4 that any U-factorization of $\mathbb{Z}_{p^n}$ has no inessential divisors. □

Corollary 3.7. *Let R_i be either $\mathbb{Z}$ or $\mathbb{Z}_{p_i^{n_i}}$ where p_i is a prime and n_i a natural number. Then any U-factorization of a nonzero nonunit $r = (r_1, r_2, \ldots, r_m) \in \prod_{i=1}^{m} R_i$ has no inessential divisors if and only if $r_i \neq 0$ for $1 \leq i \leq m$.*

These corollaries can both be proven without ever referencing Theorem 3.4 or Theorem 3.5. Without referencing the theorems, the proofs rely solely on introductory level number theory.

The importance of Corollary 3.7 is that any $\mathbb{Z}_m$, where $m \in \mathbb{N}$, can be decomposed into a direct product of rings of the form $\mathbb{Z}_{p_i^{n_i}}$. In particular, when $m = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$ where the p_i's are distinct primes, then $\mathbb{Z}_m = \mathbb{Z}_{p_1^{n_1}} \times \mathbb{Z}_{p_2^{n_2}} \times \cdots \times \mathbb{Z}_{p_k^{n_k}}$. A proof of this decomposition of $\mathbb{Z}_m$ can be found in [4, Lemma 11.1].

References

[1] Ahmet G. Agargun, D.D. Anderson and Silvia Valdes Leon, Factorizations in Commutative Rings with Zero Divisors III, *Factorization in Integral Domains, Lecture Notes in Pure Appl. Math.*, vol. 189, Marcel Dekker, New York, 1997.

[2] D.D. Anderson and Silvia Valdes Leon, Factorizations in Commutative Rings with Zero Divisors, *Rocky Mountain J. Math.* 26 (1996), 439–480.

[3] M.C. Axtell, U-factorizations in Commutative Rings with Zero Divisors, *Communications in Algebra*, to appear.

[4] J.A. Gallian, *Contemporary Abstract Algebra, ed. 4*, Houghton Mifflin Company, New York, 1998.