involve
a journal of mathematics

Nonunique factorization over quotients of PIDs

Nicholas R. Baeth, Brandon J. Burns,
Joshua M. Covey and James R. Mixco

msp

2018 vol. 11, no. 4

INVOLVE 11:4 (2018)
dx.doi.org/10.2140/involve.2018.11.701

Nonunique factorization over quotients of PIDs

Nicholas R. Baeth, Brandon J. Burns,
Joshua M. Covey and James R. Mixco

(Communicated by Vadim Ponomarenko)

We study factorizations of elements in quotients of commutative principal ideal domains that are endowed with an alternative multiplication. This study generalizes the study of factorizations both in quotients of PIDs and in rings of single-valued matrices. We are able to completely describe the sets of factorization lengths of elements in these rings, as well as compute other finer arithmetical invariants. In addition, we provide the first example of a finite bifurcus ring.

1. Introduction

Of course every commutative principal ideal domain (PID) is a unique factorization domain and every nonzero nonunit factors uniquely as a product of irreducible (prime) elements. It is not surprising that this property of unique factorization passes, in some sense, to any quotient ring of a PID. However, if D is a PID and n is the product of two or more primes in D, then $D/(n)$ contains nonzero zerodivisors that make factorization more interesting. For example, in $\mathbb{Z}/(900)$, $\overline{30}$ factors only as $\overline{30}=\overline{2}\cdot\overline{3}\cdot\overline{5}$, while $\overline{100}$ factors as $\overline{2}^2\cdot\overline{5}^2\cdot\overline{46}^a\cdot\overline{55}^b$ for any $a, b\in\mathbb{N}_0$. In fact, if D is a PID and n is the product of at least two primes of D, there are elements in $D/(n)$ that have unique factorization and others that have infinitely many factorizations — and of arbitrarily long lengths. A complete characterization of how elements factor over quotients of PIDs is given in [Baeth et al. 2017] and is summarized here in Proposition 3.1. The goal of this note is to study factorizations in quotients of PIDs endowed with an alternative multiplicative structure. The purpose is threefold: First, by introducing a more general multiplication in a principal ideal ring, we generalize both the results of [Baeth et al. 2017] (factorization in quotients of PIDs) and of [Baeth et al. 2011; Jacobson 1965] (factorization in rings of single-valued matrices). Secondly, we give examples of finite bifurcus rings, thus giving an affirmative answer to Open Problem 2.1.3 of [Adams et al. 2009]. Finally, we provide an even larger class of examples of commutative rings R such that every element of R is

MSC2010: 13A05, 13F15.
Keywords: factorizations, zerodivisors, bifurcus.

a zerodivisor and such that the set of factorization lengths of each element is a discrete interval, with many of these intervals being infinite.

We begin by defining, for any commutative ring R, an alternate multiplicative structure. Let R be a commutative ring and fix an element $k \in R$. We now define multiplication in $S_k(R)$ which, as an additive abelian group, is equal to R. For each pair of elements $r, s \in R$, we define the product of the corresponding elements $[r], [s] \in S_k(R)$ to be $[r][s] = [krs]$. The notation is convenient when distinguishing multiplication in R and in $S_k(R)$ and is motivated by the following (though less general) formulation of $S_k(R)$. With k a positive integer, we denote by $[r]$ the $k \times k$ single-valued matrix whose k^2 entries all equal r. With $S_k(R)$ the set of all such matrices over R and viewing R as a $\mathbb{Z}$-algebra so that

$$k \cdot r = \underbrace{r + \cdots + r}_{k} = kr,$$

we see that if $[r], [s] \in S_k(R)$, then $[r][s] = [krs]$ as in the original definition. With $R = \mathbb{Z}$, the ring of integers, and $k = 2$, this structure was introduced in [Jacobson 1965] to give examples of nonunique factorization of integers. This study was generalized in [Baeth et al. 2011] to $k \geq 2$ where more precise information about factorizations was gathered. Over the past several decades, factorization theory, and in particular the study of lengths of factorizations of elements in rings and semigroups, has become a major area of algebraic and combinatorial research. See, for example, the recent expository article [Geroldinger 2016] or the comprehensive text [Geroldinger and Halter-Koch 2006]. We will illustrate, using the structure of $S_k(R)$ where R is either a PID or the quotient of a PID, the existence of rings for which the factorization length set of every element is a discrete interval.

If R is a commutative ring, $R^\times$ denotes the set of *units* — elements with multiplicative inverses. Of course if R does not have a multiplicative identity, then $R^\times = \varnothing$. We say that an element $[r] \in S_k(R)$ is *irreducible* if it is impossible to write $[r] = [x][y]$ for any $[x], [y] \in S_k(R)$. In the cases of interest (see Setup 3.2) $S_k(R)$ has no units and this definition coincides with the usual definition of irreducibility in integral domains and cancellative semigroups and to the definition of *very strong irreducibles* as in [Ağargün et al. 2001; Anderson and Valdes-Leon 1996; 1997] in rings with zerodivisors. In this note we will first determine the set of irreducible elements of $S_k(R)$. Then, for each nonirreducible element $[r] \in S_k(R)$, we will compute its *length set*

$$\mathsf{L}([r]) = \{t : [r] = [x_1] \cdots [x_t] \text{ with each } [x_i] \text{ irreducible}\}.$$

This invariant is well-studied in the realm of cancellative commutative semigroups, see [Geroldinger and Halter-Koch 2006; Geroldinger 2016], and was computed for $S_k(\mathbb{Z})$ in [Baeth et al. 2011]. When R is either a principal ideal domain or a quotient of a principal ideal domain, we will show that $\mathsf{L}([r])$ is always either a singleton set or an interval of integers. When $a, b \in \mathbb{Z}$ with $a < b$, we denote by $[a, b]$ the discrete interval $\{a, a+1, \dots, b\}$. Similarly, $[a, \infty) = \{a, a+1, \dots\}$. Throughout, if D is PID, then for elements $x, y \in D$, we denote by $(x, y) = \{rx + sy : r, s \in R\}$ the ideal generated by x and y. A greatest common divisor d of x and y is an element r such that $(x, y) = (r)$. Note that with $D^\times$ denoting the set of units of D, $(x, y) = (r) = (s)$ if and only if $s = ru$ for some $u \in D^\times$.

In the remainder of this section, before turning our attention to proper quotients of PIDs, we generalize the results of [Baeth et al. 2011]. In Section 2 we give some preliminary results about the structure of $S_k(R)$ where R is the quotient of a PID. Our main results are contained in Section 3, where we describe factorizations of elements in $S_k(R)$ where R is a quotient of a PID.

The following lemma and theorem describe factorization in $S_k(D)$ where D is a PID. It should not be surprising that the results obtained here are essentially the same as those obtained in [Baeth et al. 2011], where $R = \mathbb{Z}$ (and k is a positive integer). In fact, the proofs of these results are only slightly modified from those in that paper and thus we do not include them here.

Lemma 1.1. *Let D be a PID, let $k \in D \setminus (D^\times \cup \{0\})$, and let $[a] \in S_k(D)$. Then $[a]$ is irreducible in $S_k(D)$ if and only if $k \nmid a$.*

For $a, b \in D$, we define $\nu_b(a)$ to be the largest integer m such that a is divisible by b^m. Then we have the following classification of length sets in $S_k(D)$ when D is a PID.

Theorem 1.2. *Let D be a PID, let $k \in D \setminus (D^\times \cup \{0\})$, and let $[a] \in S_k(D)$.*

(1) *If k is prime, then $|\mathsf{L}([a])| = 1$.*

(2) *If $k = p^m$ for some prime p, then*

$$\mathsf{L}([a]) = \left[\left\lceil \frac{\nu_p(a) + m}{2m - 1} \right\rceil, \nu_m(a) + 1 \right].$$

(3) *If k is not the power of a prime, then $\mathsf{L}([a]) = [2, \nu_m(a) + 1]$.*

We note that if k is prime, then $S_k(D)$ is *half-factorial*; that is, the length set of any factorization is a singleton set. When k is not prime, each element has either a singleton length set or its length set is a discrete interval. When k is not the power of a prime, $S_k(D)$ is *bifurcus*; that is, every nonirreducible element can be represented as the product of two irreducible elements.

2. The structure of $S_k(D/(n))$

Throughout the next two sections, $R = D/(n)$, where D is a commutative principal ideal domain and n is a nonzero nonunit nonprime of D. For convenience we use the notation $\bar{x}$ to denote the coset $x+(n)$ in $D/(n)$. Before investigating factorization in $S_k(R)$ in Section 3, we give some preliminary results and make a few basic observations about $S_k(R)$. We begin by showing that $S_k(R)$ has no multiplicative identity except for in the trivial case, where $S_k(R) \cong R$.

Proposition 2.1. *Let $R = D/(n)$, where D is a PID and $n \in D \setminus (D^\times \cup \{0\})$. The following statements are equivalent*:

(1) 1 *is a greatest common divisor of k and n.*

(2) $S_k(R)$ *has a multiplicative identity.*

(3) $S_k(R) \cong R$.

Proof. If 1 is a greatest common divisor of k and n, there exist $x, y \in D$ with $kx + ny = 1$. Then, in R, $\bar{k}\bar{x} = \bar{1}$. For any $[\bar{a}] \in S_k(R)$, $[\bar{a}][\bar{x}] = [\overline{axk}] = [\bar{a}]$ and $[\bar{x}]$ is the multiplicative identity of $S_k(R)$. Conversely, suppose $S_k(n)$ has a multiplicative identity $[\bar{u}]$. Then $[\bar{1}][\bar{u}] = [\bar{1}]$ and so $\bar{u}\bar{k} = \bar{1}$ in $D/(n)$. But then $ku + nv = 1$ for some $v \in D$, and so 1 is a greatest common divisor of k and n. Therefore (1) and (2) are equivalent. The fact that (3) implies (2) is trivial since $R = D/(n)$ has a multiplicative identity. We now show that (1) implies (3). Since 1 is a greatest common divisor of k and n, we have $\overline{k^{-1}}\bar{k} = \bar{1}$ for some $k^{-1} \in D$. It is then trivial to check that the map $\varphi : D/(n) \to S_k(R)$ defined by $\varphi(\bar{a}) = [\overline{k^{-1}a}]$ is a ring isomorphism. □

Before investigating the multiplicative structure of $S_k(R)$, we note that k need only be considered modulo n. If $k \equiv k' \mod n$ with $k, k' \in D$, then $\bar{k} = \overline{k'}$ in R and the following result is immediate.

Proposition 2.2. *Let $k \equiv k' \mod n$.*

(1) *If $k' = 0$, then all nonzero elements of $S_k(R)$ are irreducible.*

(2) *If $k' \neq 0$, then $S_k(R) \cong S_{k'}(R)$.*

Suppose that $S_k(R) \ncong R$. Clearly $[\bar{0}]$ is a zerodivisor of $S_k(R)$. If $d \neq 1$ is a greatest common divisor of k and n, then $k = dy$ and $n = dz$ for some $y, z \in D$. Consider $[\overline{az}] \in S_k(R)$ with $a \in D$. Then

$$[\overline{az}][\bar{x}] = [\overline{kazx}] = [\overline{(dy)azx}] = [\overline{(dz)ayx}] = [\overline{(n)ayx}] = [\overline{(0)ayx}] = [\bar{0}]$$

for every $[\bar{x}] \in S_k(R)$. Thus we have the following result.

Proposition 2.3. *Let D be a PID and let $R = D/(n)$ for some nonzero nonunit n of D. If 1 is not a greatest common divisor of k and n, then all elements of $S_k(R)$ are zerodivisors.*

Note that what the argument preceding Proposition 2.3 really shows is that for each $a \in D$, with $z = n/d$ for some greatest common divisor d of k and n, the element $[\overline{az}] \in S_k(R)$ annihilates all elements of $S_k(R)$. Moreover, if $d \neq 1$ is a greatest common divisor of k and n, then $[\overline{az}] \neq [\bar{0}]$ for some $a \in D$. That is, an element of the form $[\overline{az}]$ is a sort of *psuedozero* as it annihilates all other elements of $S_k(R)$. This element $z \in D$ has an additional interesting property in terms of factorizations. Suppose $\bar{x} = \overline{az+c}$ and $\bar{y} = \overline{bz+c}$ for some $a, b, c \in D$. Then for all $[\bar{w}] \in S_k(R)$, we have $[\bar{x}][\bar{w}] = [\bar{c}][\bar{w}] = [\bar{y}][\bar{w}]$.

3. Length sets in $S_k(R)$

The goal of this section is to compute the length set $\mathsf{L}([\bar{x}])$ for each $[\bar{x}] \in S_k(D/(n))$. We will obtain results similar to those in Theorem 1.2 but find that for some $[\bar{x}]$, $\mathsf{L}([\bar{x}])$ is unbounded, much as is the case for some elements in $D/(n)$. We begin by recalling the following proposition, [Baeth et al. 2017, Theorem 3.4], that describes factorization in $D/(n)$ with the usual multiplication.

Proposition 3.1. *Let n be a nonzero nonprime element of a PID D and let $\bar{x} \in D/(n)$ with $\gcd(x, n) = d$. If $p \mid (n/d)$ for every prime divisor p of n, then $\bar{x}$ factors uniquely in $D/(n)$ and $\mathsf{L}_{D/(n)}(\bar{x}) = \{t\} = \mathsf{L}_D(d)$. Otherwise, $\bar{x}$ has infinitely many distinct factorizations in $D/(n)$ and $\mathsf{L}_{D/(n)}(\bar{x}) = [t, \infty)$, where $\mathsf{L}_D(d) = \{t\}$.*

Since factorization in $D/(n)$ is already understood, we focus on the case when $S_k(R) \ncong R$. Based on Propositions 2.1 and 2.2 we set some blanket hypotheses for the remainder of this manuscript.

Setup 3.2. Let D be a PID, let n be a nonzero nonunit of D and let $R = D/(n)$. Also let $k \in D$ be a nonzero nonunit in D with $n \nmid k$ and $(n, k) = (d) \neq D$.

First we classify the *irreducible elements* — elements that cannot be represented as a product of two nonzero elements of $S_k(R)$.

Proposition 3.3. *Let the notation be as in Setup 3.2. Then $[\bar{a}] \in S_k(R)$ is irreducible if and only if $d \nmid a$ in D.*

Proof. Suppose that $d \mid a$. Then $a \in (d) = (k, n)$ in D and so $a = kx + ny$ for some $x, y \in D$. But then $[\bar{a}] = [\overline{kx+ny}] = [\overline{kx}] = [\bar{1}][\bar{x}]$ is not irreducible in $S_k(R)$. Conversely, suppose that $[\bar{a}]$ is not irreducible in $S_k(R)$. Then $[\bar{a}] = [\bar{x}][\bar{y}] = [\overline{kxy}]$ for some $x, y \in D$. Then $\bar{a} = \overline{kxy}$ in $D/(n)$ and so $a = kxy + nz$ for some $z \in D$. Then, since $d \mid k$ and $d \mid n$, we know $d \mid a$. □

Now that we have classified the irreducible elements of $S_k(R)$, we work to compute the length sets of nonzero elements in $S_k(R)$. Throughout we will need the following definition. For $a \in D$, define $\nu_{(n,k)}(a)$, if it exists, to be the smallest positive integer m such that $\gcd(k^m, n) \nmid a$. This gives an analog to the valuation $\nu_b(a)$ which was used in the description of lower bounds of length sets in Theorem 1.2.

Remark 3.4. Note that if $R = D/(n)$ is the quotient of a PID D and $n = p_1^{t_1} \cdots p_s^{t_s}$ with $p_1, \ldots, p_s$ distinct primes in D and $t_1, \ldots, t_s$ positive integers, then the decomposition of R by the Chinese remainder theorem immediately gives a decomposition on $S_k(R)$ as $S_k(R) \cong S_k(D/(p_1^{t_1})) \times \cdots \times S_k(D/(p_s^{t_s}))$. One could then study factorization in $S_k(R)$ by piecing together information about factorization in each $S_k(D/(p_i^{t_i}))$. Though this simplifies some calculations, it obfuscates exactly how elements factor in $S_k(R)$. However, this decomposition does clarify the definition of $\nu_{(n,k)}(a)$ since

$$\nu_{(p^t,k)}(a) = \min_{m \geq 1}\{m : \min\{m\nu_p(k), t\} > \nu_p(a)\} = \left\lfloor \frac{\nu_p(a)}{\nu_p(k)} + 1 \right\rfloor$$

if p is a prime in D and k is a positive integer.

In the next proposition we investigate upper bounds on $\mathsf{L}([\bar{a}])$.

Proposition 3.5. *Let the notation be as in Setup 3.2. Let* $[\bar{a}] \in S_k(n)$:

(1) *If* $\nu_{(n,k)}(a)$ *exists*, *then* $\max \mathsf{L}([\bar{a}]) \leq \nu_{(n,k)}(a)$.

(2) *If* $\nu_{(n,k)}(a)$ *does not exist*, *then* $\mathsf{L}([\bar{a}])$ *is unbounded.*

Proof. Let $[\bar{a}] \in S_k(n)$ and assume that $\nu_{(n,k)}(a)$ exists. Suppose that $[\bar{a}] = \prod_{j=1}^{l}[\bar{b}_j]$, where each $[\bar{b}_j]$ is irreducible. Then $a \equiv k^{l-1}b_1 \cdots b_l \mod n$ and so $\gcd(k^{l-1}, n) \mid a$. Thus $l - 1 < \nu_{(n,k)}(a)$ and so $l \leq \nu_{(n,k)}(a)$. Now assume that $\nu_{(n,k)}(a)$ does not exist. That is, $\gcd(k^m, n) \mid a$ for all $m \geq 1$. For $m \geq 1$, set d_m to be a greatest common divisor of k^m and n. Then $d_m = k^m x + ny$ for some $x, y \in D$. Since $d_m \mid a$, we know $a = d_m b = k^m xb + nyb$ for some $b \in D$. Then $[\bar{a}] = [\bar{1}]^m[\overline{xb}]$. Since $[\bar{1}]$ is irreducible and since $[\overline{xb}]$ is either irreducible or can be factored as the product of irreducibles, $[\bar{a}]$ has a factorization of length at least $m+1$. Since m was arbitrarily chosen, $\mathsf{L}([\bar{a}])$ is unbounded. □

We now show that if $\nu_{(n,k)}(a)$ exists, then $[\bar{a}]$ has a factorization of length $\nu_{(n,k)}(a)$. First we observe the following fact, which is immediate using the ideal inclusion $(a, b)(a^{m-1}, b) \subseteq (a^m, b)$.

Lemma 3.6. *Let D be a PID and let $a, b \in D$. If m is a positive integer*, *then* $\gcd(a^m, b) \mid \gcd(a, b)\gcd(a^{m-1}, b)$.

Proposition 3.7. *Let the notation be as in Setup 3.2. Let* $[\bar{a}] \in S_k(R)$ *and assume that* $\nu_{(n,k)}(a)$ *exists. Then* $\nu_{(n,k)}(a) \in \mathsf{L}([\bar{a}])$.

Proof. Clearly $[\bar{1}]$ is irreducible. We will show that there is $[\bar{b}] \in S_k(n)$ such that $[\bar{a}] = [\bar{b}][\bar{1}]^{\nu_{(n,k)}(a)-1}$ with $[\bar{b}]$ irreducible. Let $d' = \gcd(k^{\nu_{(n,k)}(a)-1}, n)$, $k' = k^{\nu_{(n,k)}(a)-1}/d'$, $a' = a/d'$, and $n' = n/d'$. Then $\gcd(k', n') = 1$ and so there exist $x, y \in D$ such that $n'x + k'y = 1$. Let $b = a'y$. Then

$$k^{\nu_{(n,k)}(a)-1}b = d'k'a'y = ak'y = a - xan' = a - a'xn,$$

whence $k^{\nu_{(n,k)}(a)-1}b \equiv a \mod n$. We now show that $[\bar{b}]$ is irreducible. If $d \mid b$, then since $d' \mid k^{\nu_{(n,k)}(a)-1}$, we have $dd' = \gcd(k,n)\gcd(k^{\nu_{(n,k)}(a)-1}, n) \mid bk^{\nu_{(n,k)}(a)-1}$. Then, by Lemma 3.6, $\gcd(k^{\nu_{(n,k)}(a)}, n) \mid \gcd(k,n)\gcd(k^{\nu_{(n,k)}(a)-1}, n)$. This would imply $\gcd(k^{\nu_{(n,k)}(a)}, n) \mid bk^{\nu_{(n,k)}(a)-1}$ and $\gcd(k^{\nu_{(n,k)}(a)}, n) \mid n$. But $\gcd(k^{\nu_{(n,k)}(a)}, n) \nmid a$, contradicting $a \equiv k^{\nu_{(n,k)}(a)-1}b \mod n$. Thus $[\bar{b}]$ is irreducible and $\nu_{(n,k)}(a) \in \mathsf{L}([\bar{a}])$. □

Now (1) of Proposition 3.5 becomes: if $\nu_{(n,k)}(a)$ exists, then $\max \mathsf{L}([\bar{a}]) = \nu_{(n,k)}(a)$.

For the remainder of this section we consider two cases. Let d be a greatest common divisor of k and n. First we suppose that d is not the power of a prime. In this case we show that $S_k(R)$ is bifurcus and hence $\mathsf{L}([\bar{a}]) = [2, \sup \mathsf{L}([\bar{a}])]$ for all nonirreducibles $[\bar{a}] \in S_k(R)$. We then consider when d is the power of some prime in D. In this case we compute the minimum value in $\mathsf{L}([\bar{a}])$ and again show that $\mathsf{L}([\bar{a}]) \subseteq [\min \mathsf{L}([\bar{a}]), \sup \mathsf{L}([\bar{a}])]$ with equality if k is also a prime power. In each case we explicitly give factorizations of $[\bar{a}]$ of each possible length. We begin with the simpler case when d is not a prime power.

Proposition 3.8. *Let the notation be as in Setup 3.2. Suppose that $d = st$ for some relatively prime $s, t \in D$. Then $2 \in \mathsf{L}([\bar{a}])$ for all nonzero nonirreducible $[\bar{a}] \in S_k(R)$.*

Proof. If $[\bar{a}]$ is not irreducible, then $d \mid a$. Then $a \in (d) = (n,k)$ and so $a = kx + ny$ for some $x, y \in D$. Write $x = d^r z$ with $r \geq 0$ and $d \nmid z$. Then, without loss of generality, $s \nmid z$. Now

$$[\bar{a}] = [\overline{kx}] = [\overline{kd^r z}] = [\overline{ks^r t^r z}] = [\overline{s^r}][\overline{t^r z}].$$

Since $d \nmid s^r$ and $d \nmid t^r z$, we have $[\overline{s^r}]$ and $[\overline{t^r z}]$ are irreducible. □

Since $2 \in \mathsf{L}([\bar{a}])$ for all nonzero nonirreducible $[\bar{a}] \in S_k(R)$, we know $S_k(R)$ is a finite bifurcus ring. This provides an affirmative answer to Open Problem 2.1.3 of [Adams et al. 2009].

Note that if $l \in \mathsf{L}([\bar{a}])$ with $l > 2$, then $[\bar{a}] = [\bar{b}_1] \cdots [\bar{b}_l]$ with each $[\bar{b}_i]$ irreducible. Since $S_k(R)$ is bifurcus, $[\bar{b}_1][\bar{b}_2][\bar{b}_3] = [\bar{c}_1][\bar{c}_2]$ for some $[\bar{c}_1]$, $[\bar{c}_2]$ irreducible. Then $[\bar{a}] = [\bar{c}_1][\bar{c}_2][\bar{b}_4] \cdots [\bar{b}_l]$ is a factorization of $[\bar{a}]$ of length $l-1$. Therefore we have the following corollary.

Corollary 3.9. *Let the notation be as in Setup 3.2. Let $[\bar{a}] \in S_k(n)$. Let d be a greatest common divisor of k and n and suppose that d is not a prime power in D:*

(1) *If $\nu_{(n,k)}(a)$ exists, then $\mathsf{L}([\bar{a}]) = [2, \nu_{(n,k)}(a)]$.*

(2) *If $\nu_{(n,k)}(a)$ does not exist, then $\mathsf{L}([\bar{a}]) = [2, \infty)$.*

In addition to a complete description of the length sets of elements in $S_k(D/(n))$, if $\gcd(k,n)$ is not a prime power, then the ring is bifurcus and [Adams et al. 2009, Theorem 1.1] tells us also the *catenary degree* is $\mathsf{c}(S_k(D/(n))) = 3$ and the *tame* *degree* is $\mathsf{t}(S_k(D/(n))) = \infty$; see [Geroldinger and Halter-Koch 2006, Chapter 1.6] for definitions.

We now consider when a greatest common divisor of k and n is a prime power and set some notation for the remainder of this section. Let $n = xp^r$, $k = yp^s$, and $d = p^t$, where p is a prime in D, $p \nmid x, y$, and $r, s \geq 1$. Then $t = \min\{r, s\} \geq 1$. Moreover, since $\bar{y} \in D/(n)^\times$, there is $w \in D$ with $yw \equiv 1 \bmod n$. We will consider factorizations of $[\bar{a}] \in S_k(n)$ where $a = zp^u$ with $p \nmid z$. Note that in this setting, similar to Remark 3.4,

$$\nu_{(n,k)}(a) = \min_{m \geq 1}\big\{m : \min\{ms, r\} > u\big\}.$$

Therefore $\nu_{(n,k)}(a)$ exists if and only if $r > u$. When it does exist, $\nu_{(n,k)}(a) = \lfloor u/s + 1 \rfloor$. Thus we consider two cases: $r > u$ and $r \leq u$. In each case we suppose that $l \in \mathsf{L}([\bar{a}])$; i.e., $[\bar{a}] = [\bar{a}_1] \cdots [\bar{a}_l]$ with each $[\bar{a}_i]$ irreducible so that $a \equiv k^{l-1} a_1 \cdots a_l \bmod n$ and hence $p^{s(l-1)} \mid a$.

First, suppose that $u < r$. We then consider two subcases determined by the relation of $(l-1)s$ to u and r. If $u < (l-1)s$, then $p^{s(l-1)} \nmid a$ and so $[\bar{a}]$ has no factorization of length l. Alternatively, $(l-1)s \leq u < r$. Since $p^{s(l-1)} \mid a$ and $a = zp^u$, we know $p^{u-(l-1)s} \mid a_1 \cdots a_l$. As each $[\bar{a}_i]$ is irreducible, $p^t \nmid a_i$ for each i. By the pigeonhole principle, $\lceil (u-(l-1)s)/(t-1) \rceil \leq l$. Conversely, suppose $j = \lceil (u-(l-1)s)/(t-1) \rceil \leq l$. Then

$$[\bar{a}] = [\overline{p^{u-(l-1)s-(t-1)(j-1)} w^{l-1} z}][\overline{p^{t-1}}]^{j-1}[\bar{1}]^{l-j}$$

is a factorization of $[\bar{a}]$ of length l. Thus, when $u < r$, we know $[\bar{a}]$ has a factorization of length l if and only if $\lceil (u-(l-1)s)/(t-1) \rceil \leq l$, equivalently $\lceil (u+s)/(t+s-1) \rceil \leq l \leq \lfloor u/s + 1 \rfloor$.

Now suppose that $r \leq u$ and consider three subcases. First, suppose that $(l-1)s \leq r \leq u$. Then $p^{r-(l-1)s} \mid a_1 \cdots a_l$ and as in the case above, $\lceil (r-(l-1)s)/(t-1) \rceil \leq l$. Conversely, if $j = \lceil (r-(l-1)s)/(t-1) \rceil \leq l$, then

$$[\bar{a}][\overline{p^{r-(l-1)s-(t-1)(j-1)w^{l-1}} z(p^{u-r}+x)}][\overline{p^{t-1}}]^{j-1}[\bar{1}]^{l-j}$$

is a factorization of $[\bar{a}]$ of length l. Now suppose that $r \leq (l-1)s < u$. Note that if $p \mid (p^{u-(l-1)s} + x + mxp^r)$ for some m, then $p \mid x$. Thus $p \nmid (p^{u-(l-1)s} + x + mxp^r)$ for all $m \in D$ and so $[\overline{p^{u-(l-1)s} + x}]$ is irreducible and

$$[\bar{a}] = [\overline{p^{u-(l-1)s} + x}][\overline{w^{l-1}}][\bar{1}]^{l-2}$$

is a factorization of $[\bar{a}]$ of length l. Finally, suppose that $r \leq u \leq (l-1)s$. Since $(p, x) = 1$, there is $v \in D$ with $vp \equiv 1 \bmod x$. That is, $vp = 1 + xb$ for some $b \in D$ and so $vp \cdot p^r = (1+xb)p^r = p^r + nb \equiv p^r \bmod n$. In fact, $v^j p^{j+r} \equiv p^r \bmod n$

for all $j \geq 0$. Now, choosing $j > (l-1)s + r - u$,

$$[\overline{v^j p^{r+j+(u-r)-(l-1)s} + x}][\overline{w^{l-1}z}][\bar{1}]^{l-2}$$

is a factorization of $[\bar{a}]$ of length l. Thus, when $r \leq u$, we know $[\bar{a}]$ has a factorization of length l if and only if $l \geq \lceil (r+s)/(t+s-1) \rceil$. In summary, we have the following proposition.

Proposition 3.10. *Let the notation be as in Setup 3.2. Let $[\bar{a}] \in S_k(n)$. Let $n = xp^r$, $k = yp^s$, $d = p^t$, and $a = zp^u$, where p is a prime in D, $p \nmid x, y, z$, and $r, s \geq 1$:*

(1) *If $\nu_{(n,k)}(a)$ exists, then $\mathsf{L}([\bar{a}]) = [\lceil (u+s)/(t+s-1) \rceil, \nu_{(n,k)}(a)]$.*

(2) *If $\nu_{(n,k)}(a)$ does not exist, then $\mathsf{L}([\bar{a}]) = [\lceil (r+s)/(t+s-1) \rceil, \infty)$.*

Even though $S_k(D/(n))$ is not bifurcus if $\gcd(k, n)$ is a prime power, we can still bound the catenary degree and compute the tame degree. Since for any $[\bar{a}] \in S_k(D/(n))$, we have $\min \mathsf{L}([\bar{a}]) \leq \lceil (r+s)/(t+s-1) \rceil$, an argument analogous to that of [Adams et al. 2009, Theorem 1.1] gives that $\mathsf{c}(S_k(D/(n))) \leq \lceil (r+s)/(t+s-1) \rceil$. Since there exist elements with arbitrarily long factorization lengths, [Geroldinger and Halter-Koch 2006, Theorem 1.6.6] gives that $\mathsf{t}(S_k(D/(n))) \geq \rho(S_k(D/(n)) = \infty$.

In conclusion, whenever $[\bar{a}] \in S_k(R)$ with $(k, n) \neq D$, we have $\mathsf{L}([\bar{a}]) = [\min \mathsf{L}([\bar{a}]), \sup \mathsf{L}([\bar{a}])]$, with $\sup \mathsf{L}([\bar{a}]) = \infty$, if and only if $\nu_{(n,k)}(a)$ does not exist. Together, Corollary 3.9 and Proposition 3.10 completely describe the length sets of elements in the ring $S_k(R)$ subject to the conditions laid out in Setup 3.2. The remaining cases are either trivial or are dealt with in Theorems 1.2 and 3.1. Moreover, the catenary degree is always bounded and the tame degree is always infinite.

References

[Adams et al. 2009] D. Adams, R. Ardila, D. Hannasch, A. Kosh, H. McCarthy, V. Ponomarenko, and R. Rosenbaum, "Bifurcus semigroups and rings", *Involve* **2**:3 (2009), 351–356. MR Zbl

[Ağargün et al. 2001] A. G. Ağargün, D. D. Anderson, and S. Valdes-Leon, "Factorization in commutative rings with zero divisors, III", *Rocky Mountain J. Math.* **31**:1 (2001), 1–21. MR Zbl

[Anderson and Valdes-Leon 1996] D. D. Anderson and S. Valdes-Leon, "Factorization in commutative rings with zero divisors", *Rocky Mountain J. Math.* **26**:2 (1996), 439–480. MR Zbl

[Anderson and Valdes-Leon 1997] D. D. Anderson and S. Valdes-Leon, "Factorization in commutative rings with zero divisors, II", pp. 197–219 in *Factorization in integral domains* (Iowa City, 1996), edited by D. D. Anderson, Lecture Notes in Pure and Appl. Math. **189**, Dekker, New York, 1997. MR Zbl

[Baeth et al. 2011] N. Baeth, V. Ponomarenko, D. Adams, R. Ardila, D. Hannasch, A. Kosh, H. McCarthy, and R. Rosenbaum, "Number theory of matrix semigroups", *Linear Algebra Appl.* **434**:3 (2011), 694–711. MR Zbl

[Baeth et al. 2017] N. Baeth, B. Burns, and J. Mixco, "A fundamental theorem of modular arithmetic", *Period. Math. Hungar.* **75** (2017), 356–367.

[Geroldinger 2016] A. Geroldinger, "Sets of lengths", *Amer. Math. Monthly* **123**:10 (2016), 960–988. MR Zbl

[Geroldinger and Halter-Koch 2006] A. Geroldinger and F. Halter-Koch, *Non-unique factorizations: algebraic, combinatorial and analytic theory*, Pure and Applied Mathematics **278**, Chapman & Hall, Boca Raton, FL, 2006. MR Zbl

[Jacobson 1965] B. Jacobson, "Matrix number theory: an example of nonunique factorization", *Amer. Math. Monthly* **72**:4 (1965), 399–402. MR Zbl

Received: 2017-05-31 Accepted: 2017-08-14

baeth@ucmo.edu *School of Computer Science and Mathematics, University of Central Missouri, Warrensburg, MO, United States*

branjburns@gmail.com *Americo Financial Life and Annuities, Kansas City, MO, United States*

jcovey94@gmail.com *Department of Mathematics, Washington University in Saint Louis, Saint Louis, MO, United States*

james.mixco@slu.edu *Department of Mathematics and Computer Science, Saint Louis University, Saint Louis, MO, United States*

involve

msp.org/involve

INVOLVE YOUR STUDENTS IN RESEARCH

Involve showcases and encourages high-quality mathematical research involving students from all academic levels. The editorial board consists of mathematical scientists committed to nurturing student participation in research. Bridging the gap between the extremes of purely undergraduate research journals and mainstream research journals, *Involve* provides a venue to mathematicians wishing to encourage the creative involvement of students.

See inside back cover or msp.org/involve for submission instructions. The subscription price for 2018 is US $190/year for the electronic version, and $250/year (+$35, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscriber address should be sent to MSP.

Involve (ISSN 1944-4184 electronic, 1944-4176 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840, is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

Involve peer review and production are managed by EditFLOW® from Mathematical Sciences Publishers.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

involve

2018 vol. 11 no. 4