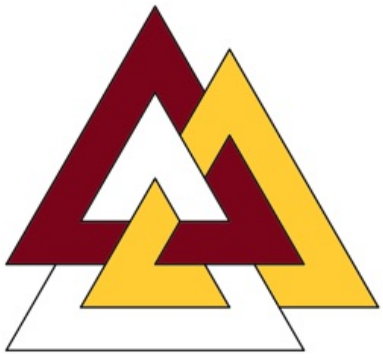
The Minnesota Journal of Undergraduate Mathematics

A note on the covering number of some finite rings

Houssein El Turkey and Cassandra Pray

University of New Haven



The Minnesota Journal of Undergraduate Mathematics

Volume 2 (2016-2017 Academic Year)

Sponsored by
School of Mathematics
University of Minnesota
Minneapolis, MN 55455

The Minnesota Journal of Undergraduate Mathematics

Volume 2 (2016-2017 Academic Year)

A note on the covering number of some finite rings

Houssein El Turkey and Cassandra Pray*

University of New Haven

Abstract. The minimum number of proper subrings needed to cover a ring R is called the *covering number* of R. In this paper, we compute the covering number of certain finite rings. When the ring is not coverable, we provide an element that generates the whole ring.

1. Introduction

It is well known in group theory that no group is the union of two of its proper subgroups. However, it is possible to write certain groups as a union of three or more of their proper subgroups. Given a group G, a *cover* of G is defined to be a set of proper subgroups whose union is all of G. If such a cover exists, then the minimum number of proper subgroups needed to cover G is called the *covering number* of G. The covering number of certain families of finite groups can be found in the literature. For example, the covering number of some symmetric and alternating groups was calculated in [2] and [5].

The same notion of covers and covering numbers can be extended to rings. Since groups cannot be covered by two proper subgroups, then a ring cannot be covered by two proper subrings. Hence the next covering number to consider is three. Lucchini and A. Maròti [3] described all possible ways to write a ring as the union of three of its proper subrings. In [6], the author described the necessary conditions for a finite semisimple ring to be coverable and gave formulas for the covering numbers in certain cases.

Determining that a ring is coverable and determining its covering number are distinct problems. For example, the matrix rings $M_2(\mathbb{Z}_p)$ are noncommutative and thus coverable (See Theorem 4.1) but finding their covering numbers is more challenging. The unpublished work of Lucchini and Maròti [4] provides a formula for $\sigma(M_n(q))$ over a field with q elements, but their published version [3] did not include that result. It is not clear whether their formula works in all cases. However, if we restrict n to 2 and q to a prime p, their formula gives $\sigma(M_2(\mathbb{Z}_p)) = \frac{p^2-p}{2} + p + 1$. In a correspondence with Werner [7], he confirmed this formula and communicated a proof of this result ([7]). The authors of [4] and [7] give a procedure for finding the covers which we utilize in our computations to verify this formula. The key idea evolves around finding the subrings that stabilize the linear subspaces of the two-dimensional vector space $\mathbb{F}_p^2$. To complete the cover, the

* *Corresponding author*

other subrings have generating elements (see Definition 2.2) with irreducible minimal polynomial. Note that for $p = 2, 3$, this formula gives $4, 7$ respectively which we verify through finding the needed subrings. For $p = 3$, Python code was used to generate these subrings. We provide our work for $p = 2, 3$:

Example 1.1. We prove that $\sigma(M_2(\mathbb{Z}_2)) = 4$. The subrings needed to cover $M_2(\mathbb{Z}_2)$ are

$$S_1 = \left\{ \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} : a, b, d \in \mathbb{Z}_2 \right\}, \quad S_2 = \left\{ \begin{bmatrix} a & b \\ c & 0 \end{bmatrix} : a, b, c \in \mathbb{Z}_2 \right\},$$

$$S_3 = \left\{ \begin{bmatrix} a & b \\ c & a+b-c \end{bmatrix} : a, b, c \in \mathbb{Z}_2 \right\}, \text{ and}$$

$$S_4 = \left\langle \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \right\rangle = \left\{ \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \right\}.$$

Example 1.2. We prove that $\sigma(M_2(\mathbb{Z}_3)) = 7$. The subrings needed to cover $M_2(\mathbb{Z}_3)$ are:

$$T_1 = \left\{ \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} : a, b, d \in \mathbb{Z}_3 \right\}, \quad T_2 = \left\{ \begin{bmatrix} a & 0 \\ c & d \end{bmatrix} : a, c, d \in \mathbb{Z}_3 \right\},$$

$$T_3 = \left\{ \begin{bmatrix} a & b \\ c & a+b-c \end{bmatrix} : a, b, c \in \mathbb{Z}_3 \right\}$$

$$T_4 = \left\{ \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 2 & 2 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 0 & 2 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 2 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 2 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 2 \\ 1 & 2 \end{bmatrix}, \begin{bmatrix} 0 & 2 \\ 2 & 0 \end{bmatrix},$$

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 2 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 2 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 2 \\ 0 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 2 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 2 \\ 2 & 1 \end{bmatrix},$$

$$\begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}, \begin{bmatrix} 2 & 0 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 2 & 0 \\ 2 & 1 \end{bmatrix}, \begin{bmatrix} 2 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}, \begin{bmatrix} 2 & 1 \\ 2 & 0 \end{bmatrix}, \begin{bmatrix} 2 & 2 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 2 & 2 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 2 & 2 \\ 2 & 2 \end{bmatrix} \right\}$$

$$T_5 = \left\langle \begin{bmatrix} 0 & 2 \\ 1 & 0 \end{bmatrix} \right\rangle = \left\{ \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 2 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 2 & 1 \end{bmatrix}, \begin{bmatrix} 2 & 1 \\ 2 & 2 \end{bmatrix}, \begin{bmatrix} 0 & 2 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 2 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 2 & 2 \\ 1 & 2 \end{bmatrix} \right\}$$

$$T_6 = \left\langle \begin{bmatrix} 0 & 1 \\ 1 & 2 \end{bmatrix} \right\rangle = \left\{ \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 2 \end{bmatrix}, \begin{bmatrix} 0 & 2 \\ 2 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 2 \\ 2 & 2 \end{bmatrix}, \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 2 & 2 \\ 2 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \right\}$$

$$T_7 = \left\langle \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \right\rangle = \left\{ \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}, \begin{bmatrix} 2 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 2 \\ 2 & 0 \end{bmatrix}, \begin{bmatrix} 2 & 2 \\ 2 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 2 \\ 2 & 2 \end{bmatrix} \right\}$$

In contrast, showing that a ring is not coverable is an easier problem. It was stated in [6, Lemma 1.4] that a ring is coverable if and only if $R \neq \langle a \rangle$ for all $a \in R$. For example, the ring $\mathbb{Z}_n$, $n \in \mathbb{N}$, is generated by the identity element which means that $\mathbb{Z}_n = \langle 1 \rangle$ is not coverable. Thus, to show a ring R is not coverable, we only need to find an element $a \in R$ such that $R = \langle a \rangle$. In this paper we compute the covering number of a variety of coverable rings. We also give examples of rings that are not coverable. In these cases, we find an element that generates (see Definition 2.2) the whole ring. Given prime numbers p and q, we consider the following rings: commutative rings of order pq, noncommutative rings of order p^2, and the quotient ring $\mathbb{Z}_p[x]/(f)$ when f is a polynomial of degree 2.

2. Preliminaries

A ring is a set R with two binary operations, addition $(+)$ and multiplication $(\cdot)$. These two operations are associative, addition is abelian, it has an inverse operation, and is distributive over multiplication. A ring is commutative if $ab = ba$ for all $a,\ b \in R$. A ring with unity is a ring which has a multiplicative identity element. A field is a commutative ring with unity in which every nonzero element has a multiplicative inverse. A subring of R is a subset of R that is a ring itself under these operations. A subset I of a ring R is called an ideal if it is an abelian group under addition and for any $i \in I$ and $r \in R$, $ri \in I$ and $ir \in I$. The quotient ring R/I is the set of equivalence classes (cosets) $a+I$, $a \in R$, such that $a+I = b+I$ if and only if $a-b \in I$. Multiplication and addition of cosets is defined by multiplying and adding the representatives of these cosets. These operations are known to be well-defined. If R is a commutative ring and $a \in R$, the set Ra is an ideal called the ideal generated by a and it is denoted by $(a) = Ra$.

Definition 2.1. A ring R is *coverable* if it is equal to the union of proper subrings. The *covering number* of a ring R, denoted by $\sigma(R)$, is the minimum number of subrings needed to cover R. If R is not coverable, we say $\sigma(R) = \infty$.

The following definition will be needed throughout this paper:

Definition 2.2. For $a \in R$, the *subring generated by* a is the set of elements of the form

$$c_n a^n + c_{n-1} a^{n-1} + \cdots + c_1 a,$$

where $n \geq 1$ and each $c_i \in \mathbb{Z}$. This subring will be denoted by $\langle a \rangle$. Note that this is not the cyclic subgroup of $R^\times$ when a is a unit. We say R is *generated by* a if $R = \langle a \rangle$.

3. Commutative rings of order pq

In this section, we discuss the covering of some commutative rings of order pq where p and q are primes. The main result is:

Theorem 3.1. *For primes p and q, we have*

$$\sigma(\mathbb{Z}_p \times \mathbb{Z}_q) = \begin{cases} 3 & p = q = 2 \\ \infty & \text{otherwise.} \end{cases}$$

Furthermore, $\sigma(\mathbb{Z}_{pq}) = \infty$, and $\sigma(R) = \infty$ if $R \neq \mathbb{Z}_2 \times \mathbb{Z}_2$ is a commutative ring with unity of order p^2.

We first motivate this theorem through the following examples:

Example 3.2. The ring $\mathbb{Z}_2 \times \mathbb{Z}_2$ is the union of its subrings $\langle(1,0)\rangle = \{(1,0),(0,0)\}$, $\langle(1,1)\rangle = \{(1,1),(0,0)\}$, and $\langle(0,1)\rangle = \{(0,1),(0,0)\}$, and therefore the covering number $\sigma(\mathbb{Z}_2 \times \mathbb{Z}_2) = 3$ by [6, Example 1.5].

Example 3.3. Let $p = 3$. By [6, Theorem 3.5], $\mathbb{Z}_3 \times \mathbb{Z}_3$ is not coverable. We show that $\mathbb{Z}_3 \times \mathbb{Z}_3 = \langle(1,2)\rangle$. Let $y = (1,2)$, then $y^2 = (1,1)$. To generate the elements of the subring $\langle(1,2)\rangle$, we use the linear combinations $a(1,2) + b(1,1) \in \mathbb{Z}_3 \times \mathbb{Z}_3$ with $a, b \in \mathbb{Z}$. By reducing the coefficients modulo 3, the linear combinations give all the elements of $\mathbb{Z}_3 \times \mathbb{Z}_3$. Similarly, we can check $\mathbb{Z}_5 \times \mathbb{Z}_5 = \langle(1,4)\rangle$.

We generalize this example for any $p \geq 3$:

Lemma 3.4. *If $p \geq 3$, $\mathbb{Z}_p \times \mathbb{Z}_p = \langle(1,p-1)\rangle$ and $\sigma(\mathbb{Z}_p \times \mathbb{Z}_p) = \infty$.*

Proof. By [6, Theorem 3.5], the ring $\mathbb{Z}_p \times \mathbb{Z}_p$ is not coverable thus $\sigma(\mathbb{Z}_p \times \mathbb{Z}_p) = \infty$. We also find a generating element. Let $y = (1,p-1)$, then $y^2 = (1,1) \pmod{p}$ which is the identity element of $\mathbb{Z}_p \times \mathbb{Z}_p$. Then any element of $\langle y\rangle$ will simplify to a linear combination $a(1,p-1) + b(1,1) = (a+b, a(p-1)+b)$ where $0 \leq a, b \leq p-1$. These linear combinations will give all elements of $\mathbb{Z}_p \times \mathbb{Z}_p$, therefore $\mathbb{Z}_p \times \mathbb{Z}_p = \langle(1,p-1)\rangle$ and $\sigma(\mathbb{Z}_p \times \mathbb{Z}_p) = \infty$ for $p \geq 3$. □

The next required step in proving Theorem 3.1 is considering the case $p \neq q$:

Lemma 3.5. *For distinct primes p and q, $\mathbb{Z}_p \times \mathbb{Z}_q = \langle(1,1)\rangle$ and $\sigma(\mathbb{Z}_p \times \mathbb{Z}_q) = \infty$.*

Proof. By [6, Corollary 2.2], if $\{R_i : 1 \leq i \leq t\}$ is a collection of finite rings with $|R_i| = p_i^{n_i}$, where p_i are pairwise distinct, then $\prod_{i=1}^{t} R_i$ is coverable if and only if at least one R_i is coverable. Thus for distinct primes p and q, the ring $\mathbb{Z}_p \times \mathbb{Z}_q$ is not coverable since both $\mathbb{Z}_p$ and $\mathbb{Z}_q$ are not coverable, and hence $\sigma(\mathbb{Z}_p \times \mathbb{Z}_q) = \infty$. We also show that $(1,1)$ will generate this ring. Let $(x,y) \in \mathbb{Z}_p \times \mathbb{Z}_q$. We want to find an integer n such that

$$(x,y) = n(1,1) = (n \pmod{p}, n \pmod{q})$$

Therefore, we want to solve the system

$$n \equiv x \pmod{p}$$
$$n \equiv y \pmod{q}$$

Since p and q are relatively prime, the Chinese Remainder Theorem guarantees an integer solution for n. Therefore, $\mathbb{Z}_p \times \mathbb{Z}_q = \langle(1,1)\rangle$. □

For the second part of Theorem 3.1, we discuss the commutative ring $\mathbb{Z}_{pq}$ of order pq:

Lemma 3.6. *For primes p and q, $\sigma(\mathbb{Z}_{pq}) = \infty$.*

Proof. Since $\mathbb{Z}_n = \langle 1\rangle$ for any $n \in \mathbb{N}$, then $\mathbb{Z}_{pq} = \langle 1\rangle$ which proves $\sigma(\mathbb{Z}_{pq}) = \infty$. □

For the last part of Theorem 3.1, we need the following:

Lemma 3.7. *If $R \neq \mathbb{Z}_2 \times \mathbb{Z}_2$ is a commutative ring with unity of order p^2, then $\sigma(R) = \infty$.*

Proof. It is well known that there are four finite commutative rings with unity of order p^2. They are: the finite field $\mathbb{F}_{p^2}$, $\mathbb{Z}_{p^2}$, $\mathbb{Z}_p \times \mathbb{Z}_p$, and $\mathbb{Z}_p[x]/(x^2)$.

The rings $\mathbb{Z}_p \times \mathbb{Z}_p$ ($p \geq 3$) and $\mathbb{Z}_{p^2}$ were handled in Lemmas 3.4 and 3.6. The ring $\mathbb{F}_{p^2}$ is not coverable because $\mathbb{F}_{p^2} = \langle a \rangle$ where a is a generator of the cyclic group of units of $\mathbb{F}_{p^2}$. The quotient ring $\mathbb{Z}_p[x]/(x^2)$ is not coverable because it is equal to the subring $\langle x + 1 + (x^2) \rangle$. In such quotient ring, we will write a coset $f(x) + I$ as $f(x)$. Let y be the coset $y = x + 1$, then using $x^2 = 0$, we can inductively show that $y^k = kx + 1 \pmod{p}$, $k \in \mathbb{N}$. It follows that $y^p = 1$. Thus, $\sum_{k=1}^{p} a_k y^k$ will generate all elements of $\mathbb{Z}_p[x]/(x^2)$. □

We conclude this section by proving Theorem 3.1.

Proof. Suppose $p = q = 2$. Then Example 3.2 shows $\mathbb{Z}_2 \times \mathbb{Z}_2$ is coverable and $\sigma(\mathbb{Z}_2 \times \mathbb{Z}_2) = 3$. The case $p = q \geq 3$ and $p \neq q$ are handled respectively by Lemmas 3.4 and 3.5. The second part of Theorem 3.1 is proved in Lemmas 3.6 and 3.7. □

4. Noncommutative rings of order p^2

In this section, we discuss noncommutative rings of order p^2. We have:

Theorem 4.1. *Every noncommutative ring of order p^2 is coverable.*

Proof. Every noncommutative ring is coverable since any subring $\langle a \rangle$, $a \in R$, is commutative and hence will not be equal to R (See [6, Lemma 1.4]). □

It would be interesting to find the subrings that would cover these rings. According to [1],

Proposition 4.2. *There are two noncommutative rings (without a unity) of order p^2:*

$$E = \langle a, b; pa = pb = 0, a^2 = a, b^2 = b, ab = a, ba = b \rangle$$

$$F = \langle a, b; pa = pb = 0, a^2 = a, b^2 = b, ab = b, ba = a \rangle$$

We consider the case $p = 2$. The ring E is covered by the subrings $\langle a \rangle$, $\langle b \rangle$, and $\langle a + b \rangle$. Thus, $\sigma(E) = 3$. Similarly, $\sigma(F) = 3$. In fact, these two rings have matrix realizations as follows. Consider the subrings of the matrix ring $M_2(\mathbb{Z}_2)$ of 2×2 matrices over $\mathbb{Z}_2$:

$$R = \left\{ \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} \right\},$$

$$R' = \left\{ \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix} \right\}.$$

Both rings $R \cong F$ and $R' \cong E$ are non-commutative of order 4. Each nonzero element in R or R' generates a subring of order 2. Thus both R and R' have covers by three subrings (See [3, Examples 2.3, 2.4]). Therefore, $\sigma(R) = \sigma(R') = 3$. We have not looked at the cases when $p \geq 3$.

5. Quotients of polynomial rings

In Lemma 3.7, we proved that $\mathbb{Z}_p[x]/(x^2)$ is not coverable. This motivated us to look at other quotient rings of the polynomial ring $\mathbb{Z}_p[x]$. Let f be a polynomial of degree 2 in $\mathbb{Z}_p[x]$. Without any loss of generality, we can assume f to be monic. If f is irreducible, then the quotient ring $\mathbb{Z}_p[x]/(f)$ is a finite field which is not coverable since it can be generated by any generator of the cyclic group of units. If f is a monic reducible polynomial of degree 2, then assume $f = (x+a)(x+b)$ where $a, b \in \mathbb{Z}_p$. Our main result in this section is:

Theorem 5.1. *Let $a, b \in \mathbb{Z}_p$, then*

$$\sigma\left(\mathbb{Z}_p[x]/(f)\right) = \begin{cases} 3 & p = 2,\ f = x(x+1) \\ \infty & \textit{otherwise.} \end{cases}$$

We handle these cases in a series of lemmas. We previously handled the case $(a, b) = (0, 0)$ in Lemma 3.7. We also handle the case $p = 2$ separately:

Lemma 5.2. $\sigma\left(\mathbb{Z}_2[x]/(f)\right) = \begin{cases} 3 & f = x(x+1) \\ \infty & f = x^2 \textit{ or } f = (x+1)^2. \end{cases}$

Proof. Note that $\mathbb{Z}_2[x]/(x(x+1)) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ where the isomorphism takes 0 to $(0,0)$, 1 to $(1,1)$, x to $(1,0)$, and $x+1$ to $(0,1)$. Since $\mathbb{Z}_2 \times \mathbb{Z}_2$ is coverable, then $\mathbb{Z}_2[x]/(x(x+1))$ is coverable. In particular, since $\mathbb{Z}_2 \times \mathbb{Z}_2$ is the union of its subrings $\langle(1,0)\rangle, \langle(0,1)\rangle$, and $\langle(1,1)\rangle$, then $\mathbb{Z}_2[x]/(x(x+1))$ is equal to the union of its subrings $\langle x\rangle, \langle x+1\rangle$, and $\langle 1\rangle$. Therefore $\sigma\left(\mathbb{Z}_2[x]/(x(x+1))\right) = 3$. We note that this ring is isomorphic to the ring in [3, Example 2.1].

From the proof of Lemma 3.7, we have $\mathbb{Z}_2[x]/(x^2) = \langle x+1\rangle$ and $\sigma\left(\mathbb{Z}_2[x]/(x^2)\right) = \infty$. For the last case, take $y = x$ then $y^2 = x^2 = -2x - 1 = -1$. Thus the linear combinations $a_1 y + a_2 y^2$ will generate all elements of $\mathbb{Z}_2[x]/((x+1)^2)$. Therefore, $\mathbb{Z}_2[x]/((x+1)^2) = \langle x\rangle$ and $\sigma\left(\mathbb{Z}_2[x]/((x+1)^2)\right) = \infty$. □

From now on, we can assume $p \geq 3$. We start by a motivating example:

Example 5.3. The ring $\mathbb{Z}_3[x]/(x(x+1))$ is not coverable because it is equal to the subring $\langle x+2\rangle$. Similarly, $\mathbb{Z}_5[x]/(x(x+1))$ is equal to the subring $\langle x+4\rangle$. Consider the ring $\mathbb{Z}_3[x]/(x(x+2))$. In this ring, we have $x^2 = x$ (as cosets). Let $y = x+1$, then $y^2 = x^2+2x+1 = 1$. The linear combination $Ay + B$, $A, B \in \mathbb{Z}_3$, will generate all elements of the quotient ring. Therefore, $\mathbb{Z}_3[x]/(x(x+2)) = \langle x+1\rangle$ and thus it is not coverable.

More generally,

Lemma 5.4. *If $p \geq 3$ is prime and $b \in \mathbb{Z}_p \setminus \{0\}$, then $\mathbb{Z}_p[x]/(x(x+b)) = \langle x+p-b\rangle$ and $\sigma(\mathbb{Z}_p[x]/(x(x+b))) = \infty$.*

Proof. Let $y = x+p-b \equiv x-b \pmod p$. Then we can inductively show that for $k \geq 1$,

$$y^k = (-1)^{k-1}(2^k - 1)b^{k-1}x + (-b)^k.$$

By Fermat's Little Theorem, $2^{p-1} \equiv 1 \pmod{p}$ and $b^{p-1} \equiv 1 \pmod{p}$. Since $p-1$ is even, we have $y^{p-1} \equiv 1 \pmod{p}$.

Any element in $\mathbb{Z}_p[x]/(x(x+b))$ is of the form $Ax+B+I$ where $I=(x(x+b))$ and $A,B \in \mathbb{Z}_p$ under the condition $x^2=-bx$. The linear combinations, with $c_k \in \mathbb{Z}_p$,

$$\sum_{k=1}^{p-1} c_k y^k = \sum_{k=1}^{p-1} c_k((-1)^{k-1}(2^k-1)b^{k-1}x+(-b)^k) = \sum_{k=1}^{p-1} c_k(-1)^{k-1}(2^k-1)b^{k-1}x + c_k(-b)^k$$

will generate all the elements of $\mathbb{Z}_p[x]/(x(x+1))$ since b is invertible modulo p. The first term in the sum will give the terms of degree 1 in the cosets while the second term will give the constant term in the cosets. □

The only case left is when $f=(x+a)(x+b)$ where both a and b are nonzero. We verify the theorem using the following example:

Example 5.5. Consider the ring $\mathbb{Z}_3[x]/((x+1)(x+2))$ where we have $x^2=1$. Let $y=x$, then $y=x^2=1$ which implies that $\mathbb{Z}_3[x]/((x+1)(x+2))=\langle x\rangle$ and thus it is not coverable.

Similarly, consider the ring $\mathbb{Z}_5[x]/((x+2)(x+3))$ where we have $x^2=4$. let $y=x$, then $y=x^2=4$ which implies that $\mathbb{Z}_5[x]/((x+2)(x+3))=\langle x\rangle$ and thus it is not coverable.

More generally,

Lemma 5.6. *Let $p \geq 3$ be a prime and $a,b \in \mathbb{Z}_p$ with both $a,b \neq 0$. Then $\mathbb{Z}_p[x]/((x+a)(x+b)) = \langle x\rangle$ and $\sigma\left(\mathbb{Z}_p[x]/((x+a)(x+b))\right)=\infty$.*

Proof. Let $y=x$. Then $y^2=x^2=-(a+b)x-ab$ since $x^2+(a+b)x+ab=0$. By taking any linear combination $Ay+By^2$, $A,B \in \mathbb{Z}_p$, we have

$$Ay+By^2 = Ax+B(-a-b)x+B(-ab) = x(A-aB-bB)-abB.$$

To generate any element $xs+t \in \mathbb{Z}_p[x]/((x+a)(x+b)$, for some $s,t \in \mathbb{Z}_p$, we need to solve $-abB=t$ and $A-aB-bB=s$. Since a^{-1} and b^{-1} exist in $\mathbb{Z}_p$, the first equation gives $B=-a^{-1}b^{-1}t$ and the second equation gives $A=s-b^{-1}t-a^{-1}t$. Thus any element of $\mathbb{Z}_p[x]/((x+a)(x+b))$ can be written as $Ax+Bx^2$ which implies $\mathbb{Z}_p[x]/((x+a)(x+b))=\langle x\rangle$ and $\sigma\left(\mathbb{Z}_p[x]/((x+a)(x+b))\right)=\infty$. □

We conclude by noting that Lemmas 5.2, 5.4, and 5.6 prove Theorem 5.1. These computations leave, however, some unanswered questions: what happens if we increase the degree of f or what happens if we replace p by a prime power p^n? For example, it was shown in [6] that if f is monic and irreducibe, then the local ring $\mathbb{Z}_{p^n}[x]/(f)$ is not coverable. Another direction could be studying the covering number of some noncommutative rings (see Section 4) or some infinite rings.

6. Acknowledgments

The authors would like to acknowledge the author of [6], N. Werner, for his valuable input. We thank him for introducing to us some of the questions in this paper. We also thank the referee(s) for their helpful comments.

References

[1] B. Fine, Classification of finite rings of order p^2, *Mathematics Magazine*. **66**(4) (1993) pp. 248–252.
[2] L. C. Kappe and J. Redden, On the covering number of small alternating groups, *Computational Group Theory and the Theory of Groups II*, Contemporary Mathematics **511** (2010), Amer. Math. Soc. Providence, RI, pp. 109–125.
[3] A. Lucchini and A. Maròti, Rings as the union of proper subrings, *Algebr. Represent. Theor.* **15** (2012) pp. 1035–1047.
[4] A. Lucchini and A. Maròti, Rings as the union of proper subrings (draft, 2010), available at: `http://arxiv.org/abs/1001.3984v1`.
[5] A. Maròti, Covering the symmetric groups with proper subgroups, *J. Comb. Theory, Ser. A* **110** (2005) pp. 97–111.
[6] N. J. Werner, Covering numbers of finite rings, *Amer. Math. Monthly*, **122**(6) (2015) pp. 552–566.
[7] N. J. Werner, The covering number of $M_2(\mathbb{F}_p)$, *work in progress*.

Student biographies

Cassandra Pray: (*Corresponding author:* cpray1@unh.newhaven.edu) Cassandra was an undergraduate junior/senior studying applied mathematics at the University of New Haven when this work was done. She graduated in May 2017 and she will be pursuing a master's degree in applied mathematics at the Indiana University of Pennsylvania in Fall 2017.