Spring 2016

A Cycle Generating Function On Finite Local Rings

Tristen Kirk Wentling

A CYCLE GENERATING FUNCTION ON FINITE LOCAL RINGS

A Masters Thesis

Presented to

The Graduate College of

Missouri State University

In Partial Fulfillment

Of the Requirements for the Degree

Master of Science, Mathematics

By

Tristen K. Wentling

May 2016

A CYCLE GENERATING FUNCTION ON FINITE LOCAL RINGS

Department of Mathematics

Missouri State University, May 2016

Master of Science

Tristen K. Wentling

ABSTRACT

We say a function $f(x)$ generates a cycle if its output returns the initial value for some number of successive applications of $f(x)$. In this thesis, we develop a class of polynomial functions $f_\alpha(x)$ for finite local rings and associated functions $\varphi_\alpha(x) = f(x) + x$. We show that the zeros of $f_\alpha(x)$ are precisely the fixed points of $\varphi_\alpha(x)$ and that every ring element is either one of these fixed points or is in a cycle of fixed length equal to the order of 2 in the associated group of units. Particular emphasis is given to rings of integers modulo the square of a prime. The construction of these polynomial functions arose from exploring constructions of polynomials in a similar manner to that embodied in the recent work of Dr. Cameron Wickham and Dr. Mark Rogers and the development of π-polynomials in "Polynomials Inducing the Zero Function on Local Rings"[5].

KEYWORDS: local rings, polynomials, graph theory, primes, abstract algebra

This abstract is approved as to form and content

_____

Mark Rogers, PhD
Chairperson, Advisory Committee
Missouri State University

A CYCLE GENERATING FUNCTION ON FINITE LOCAL RINGS

By

Tristen K. Wentling

A Masters Thesis
Submitted to the Graduate College
Of Missouri State University
In Partial Fulfillment of the Requirements
For the Degree of Master of Science, Mathematics

May 2016

Approved:

_____
Mark Rogers, PhD

_____
Cameron Wickham, PhD

_____
Richard Belshoff, PhD

_____
Julie Masterson, PhD: Dean, Graduate College

ACKNOWLEDGEMENTS

I would like to thank Dr. Rogers in particular for all the time he's spent working with me throughout the course of developing and writing this thesis and for being there whenever I needed help, guidance, and direction. I would like to thank Dr. Wickham for his suggestions and support in the development of my thesis. More generally I would like to thank all the faculty and staff of the Mathematics department at Missouri State University, many of whom have contributed to who I am as an aspiring mathematician today.

I dedicate this thesis to my ever patient wife Jessyca Wentling and our three children: Jakeb, Zekariah, and Ada.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

INTRODUCTION

Our purpose herein is to establish the existence and properties of a class of functions that generate cycles in certain kinds of local rings. The driving motivation in the development of this type of function arose from the research of Dr. Mark Rogers and Dr. Cameron Wickham who together introduce the concept of π-polynomials which involve ideals of zero function maps on finite local rings in conjunction with maps that send other ring elements to the maximal ideal. There is a direct analogy in the method of construction of the foundation of the functions explored here, which we call α-polynomials. Given their developmental importance, it is beneficial in the course of development of α-polynomials to understand the construction and some of the properties which belong to π-polynomials and thus an early section is dedicated to this purpose. Prior to their treatment we include some background material on local rings and define α-polynomial functions, which appear as $f_\alpha(x)$ and the associated function $\varphi_\alpha(x) = f_\alpha(x) + x$. We give special consideration to the ring $\mathbb{Z}/p^2\mathbb{Z}$ and its relation to graph theory. We assume some familiarity with graph theory but also note that the relevant definitions and concepts can be found in Appendix (A). We then turn to the more general setting of local rings having the condition $\mathfrak{m}^2 = 0$ where $\mathfrak{m}$ is the maximal ideal of the ring. Here we omit the connection to graph theory but show the similar behavior of $f_\alpha(x)$ and $\varphi_\alpha(x)$. We then briefly observe α-polynomials in finite fields and give examples of their misbehavior in rings having even cardinality. The development of α-polynomials came about through computational exploration using Sage [7]. Sage is an open-source mathematics software system which incorporates and draws upon several computer algebra systems such as GAP, Singular, and Macaulay 2. The concept used entailed devising constructions similar to the π-polynomials developed by Rogers and Wickham. Sage simplified many of our computations and enabled rapid development of the related graphs in rings of the form $\mathbb{Z}/p^2\mathbb{Z}$. The source code for the main examples is in Appendix B.

ALGEBRAIC DEFINITIONS AND CONCEPTS

Throughout we will make use of the following definitions and terminology based on Dummit and Foote's *Abstract Algebra* [2]. A *maximal ideal* is an ideal $\mathfrak{m}$ of a ring R such that the only ideals containing it are $\mathfrak{m}$ and R. A commutative ring R with identity 1_R is called *local* if it has a unique maximal ideal.

One often useful property in local rings is the characterization of the unit elements of such rings.

THEOREM 2.1. *If R is a local ring with maximal ideal $\mathfrak{m}$ then every element of $R \setminus \mathfrak{m}$ is a unit.*

Proof. Let R be a local ring with maximal ideal $\mathfrak{m}$ and let $a \in R \setminus \mathfrak{m}$. Assume (a), the ideal generated by a, is a proper ideal; then (a) must be contained in some maximal ideal. Since R is a local ring with unique maximal ideal $\mathfrak{m}$, we have $(a) \subseteq \mathfrak{m}$, but then $a \in \mathfrak{m}$, which is contradiction. Hence (a) is not proper, i.e., $(a) = R$. Thus $1_R = a \cdot b$ for some $b \in R$ and hence a is a unit in R. □

This characterization, all unit elements being exactly those elements not in the maximal ideal, will be useful in particular in the proofs of Lemma 5.1 and Theorems 2.9, 4.5, 4.6, and 5.7.

DEFINITION 2.2 (fixed point). *Given a function $\varphi : R \to R$ defined on a ring R, we call an element $r \in R$ a fixed point of $\varphi(x)$ if and only if $\varphi(r) = r$.*

The idea of the following theorem will be the characterization of exactly which ring elements are zeros of one function and their correspondence with the fixed points of another.

THEOREM 2.3. *Let $f : R \to R$ be a function defined on the ring R and define $\varphi(x) = f(x) + x$. For all $r \in R$, r is a fixed point of $\varphi(x)$ if and only if $f(r) = 0$.*

Proof. First, assume $r \in R$ is a fixed point of $\varphi(x)$. Then $f(r) + r = r$. Hence, after subtracting r from both sides of the equation, $f(r) = 0$. Now, assume $f(r) = 0$ for some $r \in R$. By adding r to both sides we see that $f(r) + r = r$ and thus r is a fixed point of $f(x) + x = \varphi(x)$. Therefore we have that for all $r \in R$, r is a fixed point of $\varphi(x)$ if and only if $f(r) = 0$. □

This relationship between two functions, $f(x)$ and $\varphi(x) = f(x) + x$ is crucial to the development of our results. This also explains our choice of notation as we will see that when we take $f_\alpha(x)$ to be an α-polynomial function there is immediately a corresponding function $\varphi_\alpha(x) = f_\alpha(x) + x$.

Before we formally define α-polynomials, one more detail is required. Recall that LaGrange's Theorem says that if H is a subgroup of a finite group G, then $|H|$ divides $|G|$ [2]. Then we can obtain some specific properties of the group.

LEMMA 2.4. *Let R be a finite local ring with maximal ideal $\mathfrak{m}$ such that $|\mathfrak{m}| = t$. Then $|R| = q \cdot t$ where $q = |R/\mathfrak{m}|$.*

Proof. Since a ring is an abelian group under addition by definition, and $\mathfrak{m}$ is an ideal of R, $\mathfrak{m}$ is a normal subgroup of R under addition. So by LaGrange's Theorem, $|\mathfrak{m}|$ divides $|R|$. Since $\mathfrak{m}$ is normal in R, the quotient group $R/\mathfrak{m}$ is well defined. Hence $|R| = |R/\mathfrak{m}| \cdot |\mathfrak{m}| = q \cdot t$ where $q = |R/\mathfrak{m}|$. □

Lemma 2.4 will be beneficial to defining α-polynomials because the value t for a local ring R will be a part of that definition by way of the maximal ideal, which we highlight in the following remark and subsequent definition of α-polynomials.

REMARK 2.5. *Suppose R is a finite local ring with maximal ideal $\mathfrak{m} = \{m_1, m_2, \ldots, m_t\}$. If $\alpha \in R/\mathfrak{m}$, then $\alpha = \overline{a} = \{a + m_1, a + m_2, \ldots, a + m_t\}$ for some a in R. In particular, each element of $R/\mathfrak{m}$ is a subset of R with cardinality t. We will also often take $m_1 = 0$.*

DEFINITION 2.6 (α-polynomial). *Let R be a finite local ring with maximal ideal $\mathfrak{m}$. For any $\alpha \in R/\mathfrak{m}$ we define $f_\alpha(x) = \prod_{i=1}^{t}(x - \alpha_i)$, where $\alpha = \{\alpha_1, \alpha_2, \ldots, \alpha_t\} \subseteq R$, to be an α-polynomial.*

Now that we have defined exactly what an α-polynomial is, we can explore some more general properties of both $f_\alpha(x)$ and $\varphi_\alpha(x)$ in local rings. Specific properties when restrained to certain types of local rings, and especially their behavior in them, will be explored in more detail for particular types of rings.

We begin with a characterization of the roots of $f_\alpha(x)$ and their correspondence with the fixed points of $\varphi_\alpha(x)$.

THEOREM 2.7. *Let R be a finite local ring and let $\alpha \in R/\mathfrak{m}$. If $f_\alpha(x) = \prod_{i=1}^{t}(x - \alpha_i)$ and $\varphi_\alpha(x) = f_\alpha(x) + x$, then the only zeros of f_α are $\alpha_i \in \alpha$ and thus the only fixed points of $\varphi_\alpha(x)$ are the elements of α.*

Proof. For all $\alpha_i \in \alpha$, $f_\alpha(\alpha_i) = 0$ since each α_i is explicitly a root of $f_\alpha(x)$ by construction, hence α_i is a fixed point of $\varphi_\alpha(x)$ by Theorem 2.3.

Let $r \in R$ such that $r \neq \alpha_i$ for any i, i.e., $r \notin \alpha$. let $a \in R$ such that $\alpha_i = a + m_i$. If $r - \alpha_i \in \mathfrak{m}$ then $r - a \in \mathfrak{m}$ since $m_i \in \mathfrak{m}$ and $\mathfrak{m}$ is closed under addition. This is a contradiction, however, since $r - a = r - (a + m_i)$. Thus $r - \alpha_i \notin \mathfrak{m}$ for any i and, more specifically, $r - \alpha_i$ is a unit by Theorem 2.1. Then $f_\alpha(r) = \prod_{i=1}^{t}(r - \alpha_i)$ is a product of units and hence non-zero. Hence, since $f_\alpha(r)$ is non-zero, by Theorem 2.3, r is not a fixed point of $\varphi_\alpha(x)$. Therefore we have that the elements of α are the only fixed points of $\varphi_\alpha(x)$. □

The upcoming theorems, namely Theorems 2.8 and 2.9, establish some properties of $f_\alpha(x)$, which in particular aid in proving the properties of $\varphi_\alpha(x)$ found in Theorem 2.10.

THEOREM 2.8. *Let R be a finite local ring with maximal ideal $\mathfrak{m}$ such that $2 \nmid |R|$ and $|R| = |R/\mathfrak{m}| \cdot t$. Then for an α-polynomial $f_0(x)$ in $R[x]$, $f_0(-x) = -f_0(x)$.*

Proof. First, observe that if $2 \nmid |R|$, then $2 \nmid t$ either. Further, note that $\mathfrak{m} = -\mathfrak{m}$ since -1 is a unit. Hence:

$$\begin{aligned} f_0(-x) &= \prod_{i=1}^{t}(-x - m_i) \\ &= (-1)^t \prod_{i=1}^{t}(x - (-m_i)) \\ &= (-1)^t \prod_{i=1}^{t}(x - m_i) = -f_0(x) \end{aligned}$$

. □

THEOREM 2.9. *Let R be a finite local ring with identity such that $2 \nmid |R|$ with maximal ideal $\mathfrak{m}$. Then for $\alpha \in R/\mathfrak{m}$ an α-polynomial over R has the following properties:*

a. $f_\alpha(x) = f_0(x - a)$

b. $f_\alpha(-x) = -f_{-\alpha}(x)$

Proof. For part a., observe that:

$$\begin{aligned} f_\alpha(x) &= \prod_{i=1}^{t}(x - \alpha_i) \\ &= \prod_{i=1}^{t}(x - (a + m_i)) \\ &= \prod_{i=1}^{t}((x - a) - m_i) \\ &= f_0(x - a) \end{aligned}$$

i.e., $f_\alpha(x) = f_0(x - a)$ as desired. Now for part b., since $2 \nmid |R|$, $2 \nmid t = |\mathfrak{m}|$, so using

part a. and the fact that $\mathfrak{m} = -\mathfrak{m}$ (relabeling $\mathfrak{m}$ as necessary below):

$$\begin{aligned} f_\alpha(-x) &= \prod_{i=1}^{t}(-x - \alpha_i) \\ &= \prod_{i=1}^{t}(-x - (a + m_i)) \end{aligned}$$

$$\begin{aligned} &= \prod_{i=1}^{t}(-1)((x + a) + m_i) \\ &= (-1)^t \prod_{i=1}^{t}((x - (-a)) - m_i) \\ &= -f_0(x - (-a)) = -f_{-\alpha}(x) \end{aligned}$$

□

We will now consider the function $\varphi_\alpha(x) = f_\alpha(x) + x$ in greater detail. Using the above theorem we can obtain some similar but non-identical properties for $\varphi_\alpha(x)$.

THEOREM 2.10. *Let R be a finite local ring with identity such that $2 \nmid |R|$. Then if $f_\alpha(x)$ is an α-polynomial over R and $\varphi_\alpha(x) = f_\alpha(x) + x$, then $\varphi_\alpha(x)$ has the following properties:*

a. $\varphi_0(-x) = -\varphi_0(x)$.

b. $\varphi_\alpha(x) = \varphi_0(x - a) + a$

c. $\varphi_\alpha(-x) = -\varphi_{-\alpha}(x)$

Proof. For each part we show that the difference is zero for each pair of expressions above. For part a., we take the difference and apply the definition of $\varphi_\alpha(x)$ above and

apply part b. of 2.9, hence:

$$\begin{aligned}
&\varphi_0(-x) + \varphi_0(x) \\
&= f_0(-x) - x + f_0(x) + x \\
&= f_0(x) - f_0(x) + x - x = 0
\end{aligned}$$

Similarly, for part b., we again use the definition but apply part a. of 2.9, thus:

$$\begin{aligned}
&\varphi_\alpha(x) - \varphi_0(x - a) - a \\
&= f_\alpha(x) + x - (f_0(x - a) + (x - a)) - a \\
&= f_\alpha(x) - f_\alpha(x) + x - x + a - a = 0
\end{aligned}$$

Lastly, for part c., we follow the method of part b. and thus:

$$\begin{aligned}
&\varphi_\alpha(-x) + \varphi_{-\alpha}(x) \\
&= f_\alpha(-x) - x + f_{-\alpha}(x) + x \\
&= -f_{-\alpha}(x) + f_{-\alpha}(x) - x + x = 0
\end{aligned}$$

□

While the properties above don't make many demands for the local ring R, as we will see in later sections that we can extend our study by restricting certain properties of the ring. First, however, we will make use of one more general definition that will give us a more distinct statement of later results.

If R is a local ring with maximal ideal $\mathfrak{m}$, then $\overline{R} = R/\mathfrak{m}$ is a field with cardinality $q = p^n$. In other words, $\overline{R} \cong \mathbb{F}_q$. We also know $\mathbb{F}_q \cong \mathbb{F}_p^n$ [2]. Then since $\mathbb{F}_p$ is the prime subfield of $\mathbb{F}_q$, there is a natural correspondence between $\overline{R}^\times$ and $(\mathbb{Z}/p\mathbb{Z})^\times$.

Definition 2.11 ($\tau(p)$). *Let p be a prime integer. Then we let $\tau(p)$ be the order of* 2

in $(\mathbb{Z}/p\mathbb{Z})^{\times}$. *That is,* $\tau(p)$ *is the smallest* n *such that* $2^n = 1$ *in* $(\mathbb{Z}/p\mathbb{Z})^{\times}$ [4].

As mentioned previously, π-polynomials were a strong factor in developing α-polynomials. As we have seen, α-polynomials are formed by taking a product of linear polynomials formed from a specific set of elements, namely those belonging to the same congruence class modulo the maximal ideal. Next we will discuss the construction and some properties of π-polynomials and observe how they also can be constructed by taking a product of certain elements of a local ring.

PI-POLYNOMIALS

One approach to studying polynomials over different types of rings is the exploration of zeros, or roots, of these polynomials. In some cases, as in algebraic geometry, we are often concerned further with entire sets of values which evaluate to zero, in other words, varieties. How about functions, however, which induce the zero function on some given ring? In "Polynomials Inducing the Zero Function on Finite Local Rings," Rogers and Wickham explore the *zero function ideal* $\mathcal{Z}(R)$ of a finite local ring R [5]. Specifically, they are concerned with how composing maps that send elements from a local ring to its maximal ideal with maps sending elements of the maximal ideal to zero serve as generators for all functions sending elements to zero in the ring.

Setting, Construction, and Properties

Herein we take $(R, \mathfrak{m})$ to be a finite local ring with maximal ideal $\mathfrak{m}$ having a finite residue field $\overline{R} = R/\mathfrak{m}$. If there is a function f such that $f(r) = 0$ for every $r \in R$ then we say that f is a *zero function*. The set of polynomials that send elements of S to elements of J where S is a subset of the ring R and J an ideal of R, denoted $\mathcal{Z}_R(S, J)$, is an ideal of $R[x]$. If the ring containing S is clear from context the subscript is abandoned as is J whenever $J = 0$. Thus $\mathcal{Z}(R)$ is the set of all polynomials which map all elements of R to zero (Definition 2.1)[5].

Now if the local ring $(R, \mathfrak{m})$ has finite residue field $\overline{R}$ with cardinality q and $c_1, c_2, \ldots, c_q$ are any representatives of the congruence classes of $R/\mathfrak{m}$, then the polynomial $\pi(x) = \prod_{i=1}^{q}(x - c_i)$ is called a *π-polynomial* (Definition 2.4)[5]. As a brief example consider the ring $\mathbb{Z}/49\mathbb{Z}$ which has $\mathfrak{m} = (7)$. Then, for simplicity, we can use the elements $0, 1, 2, 3, 4, 5, 6$ as our representatives from each of the distinct congruence classes

and so by taking the product

$$(x-0)(x-1)(x-2)(x-3)(x-4)(x-5)(x-6)$$

we obtain the π-polynomial

$$x^7 + 28x^6 + 28x^5 + 7x^3 + 34x.$$

There is also an associated function for π-polynomials $p(x) = \pi(x) + x$. We will denote applying this function in succession n times by declaring that $p^{(n+1)}(x) = p(p^{(n)}(x))$ with $p^{(1)}(x) = p(x)$. This deviates from the authors' original notation but provides more consistent notation in the present setting as we will use the same notation for the function $\varphi_\alpha(x)$ associated with α-polynomials.

Some of the properties of π-polynomials shown in the paper are:

- $\mathcal{Z}(R, \mathfrak{m}) = (\pi(x), \mathfrak{m})$,
- if $\pi(x)$ is a π-polynomial then $\pi(x)$ is a monic polynomial,
- if $\pi(x)$ is a π-polynomial then $\pi(x)$ maps to $x^q - x$ in $\overline{R}[x]$.
- if $\pi(x)$ is any polynomial mapping to $x^q - x$ in $\overline{R}[x]$, and $p^{(n)}(x)$ is defined as above, then $p^{(n)}(x) - p^{(n-1)}(x) \in \mathcal{Z}(R, \mathfrak{m}^n)$,
- if $\pi(x)$ is any polynomial mapping to $x^q - x$ in $\overline{R}[x]$, then $\pi(x)$ is a π-polynomial.

One can recover the original roots of $\pi(x)$ by applying $p^{(e)}(x)$ where e is the index of nilpotency of $\mathfrak{m}$, that is, e such that $\mathfrak{m}^e = 0$. The practical upshot is that if one were to know that a given polynomial were a π-polynomial by reducing modulo $\mathfrak{m}$, then the roots, and hence the factorization, of the polynomial can be recovered via this method giving the precise roots from each congruence class in $R/\mathfrak{m}$. Next we will consider a particular example.

Example in $\mathbb{Z}/27\mathbb{Z}$

In this example we will consider a π-polynomial over $\mathbb{Z}/27\mathbb{Z}$. If we list the elements of $R = \mathbb{Z}/27\mathbb{Z}$ as $\{0, 1, \ldots, 26\}$, then R is local with maximal ideal $\mathfrak{m} = 3\mathbb{Z}/27\mathbb{Z} = (3)$ and residue field $\overline{R} \cong \mathbb{Z}/3\mathbb{Z}$. Then the elements of $\overline{R}$ are those found in Table 1. Then we can construct a π-polynomial by using the first representative from

Table 1: Elements of $\overline{R}$, $R = \mathbb{Z}/27\mathbb{Z}$

Residue Class	Coset	Elements
$\bar{0} =$	$\mathfrak{m}$	$= \{0, 3, 6, 9, 12, 15, 18, 21, 24\}$
$\bar{1} =$	$1 + \mathfrak{m}$	$= \{1, 4, 7, 10, 13, 16, 19, 22, 25\}$
$\bar{2} =$	$2 + \mathfrak{m}$	$= \{2, 5, 8, 11, 14, 17, 20, 23, 26\}$

each congruence class as a root: $\pi(x) = (x - 0)(x - 1)(x - 2) = x^3 - 3x^2 + 2x$, which reduced modulo $\mathfrak{m}$ indeed yields $x^3 - x$.

If we evaluate the polynomial $p(x)$ for each element in $\mathbb{Z}/27\mathbb{Z}$, then we see in Table 2 that each value maps after no more than two successive applications to an element from its congruence class, the original root of $\pi(x)$.

Table 2: $p(x)$ and $p^{(n)}(x)$ for $x \in \mathbb{Z}/27\mathbb{Z}$

$x \in R$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	...
$p(x)$	0	1	2	9	1	11	18	1	20	0	1	2	9	1	...
$p^{(2)}(x)$	0	1	2	0	1	2	0	1	2	0	1	2	0	1	...

A graph for a function can be made by defining a directed graph such that a is connected to b if and only if $p(a) = n$. For further details on constructing a graph from a function see Appendix A. The resulting graph is shown in Figure 1. The computational exploration of π-polynomials, and subsequently of polynomials constructed in a similar manner, provided the basis for the results we consider presently. The similarity lies principally in their construction except where π-polynomials use an element of each residue class, α-polynomials use all of the elements of just one congruence class. In the next section we build a more specific kind of α-polynomial over rings $\mathbb{Z}/p^2\mathbb{Z}$ as we considered for π-polynomials.

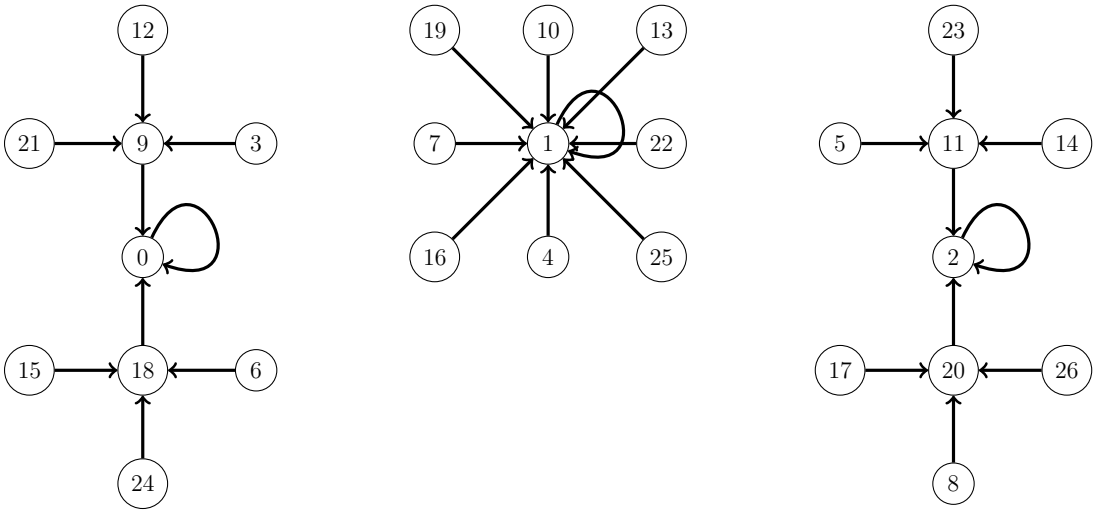


Figure 1: A π-polynomial graph.

ALPHA-POLYNOMIALS IN $\mathbb{Z}/p^2\mathbb{Z}$

Let $\mathbb{Z}$ be the set of integers and $p \in \mathbb{Z}$ be prime. We will take $R = \mathbb{Z}/p^2\mathbb{Z}$ as a local ring with maximal ideal $\mathfrak{m}$ generated by p. Previously we used q and t to denote $|R/\mathfrak{m}|$ and $|\mathfrak{m}|$ respectively, but here we note that $q = p$ and $t = p$; this will give rise to a particular case of α-polynomial. If we take $\alpha = \{\alpha_1, \alpha_2, \ldots, \alpha_p\} \in R/\mathfrak{m}$, then in this setting, the construction of an α-polynomial will be $f_\alpha(x) = \prod_{i=1}^{p}(x - \alpha_i)$ and in turn we obtain $\varphi_\alpha(x)$ as $\varphi_\alpha(x) = f_\alpha(x) + x$. The fixed points of $\varphi_\alpha(x)$ in this case are exactly the elements $\alpha_i \in \alpha$.

Suppose now that we wish to apply $\varphi_\alpha(x)$ n times in succession. We will denote this similarly to the function $p^{(n)}(x)$ associated with π-polynomials by writing $\varphi_\alpha^{(n)}(x)$, and define it as follows. We say $\varphi_\alpha^{(1)}(x) = \varphi_\alpha(x)$, then $\varphi_\alpha^{(n+1)}(x) = \varphi_\alpha(\varphi_\alpha^{(n)}(x))$, i.e., $\varphi_\alpha^{(n)}(x)$ applies the function n times to an element and its successive images. This provides notational brevity in many instances throughout.

As a brief example demonstrating the construction of all α-polynomials in the ring $\mathbb{Z}/9\mathbb{Z}$, note that $\mathfrak{m} = (3)$ and we have $\alpha \in \{\overline{0}, \overline{1}, \overline{2}\}$, hence we obtain the following polynomials:

$$f_0(x) = x(x-3)(x-6),$$
$$f_1(x) = (x-1)(x-4)(x-7), \textit{and}$$
$$f_2(x) = (x-2)(x-5)(x-8).$$

While this example is fairly simple, its purpose is simply to exemplify the construction of α-polynomials in a particular local ring. We turn now to an example of one particular α-polynomial in a slightly larger ring which will allow us to explore the more interesting properties of α-polynomials more generally.

Example in $\mathbb{Z}/25\mathbb{Z}$

The observation of α-polynomials in a particular setting will demonstrate some particular features of this class of polynomials. We are in particular motivated by the way in which sets of elements are partitioned under the action of $\varphi_\alpha^{(n)}(x)$, which when translated to the corresponding graph theoretic setting yields cycles of distinct lengths dependent upon the value of p.

In the local ring $R = \mathbb{Z}/25\mathbb{Z}$, the maximal ideal is generated by 5, i.e., $\mathfrak{m} = (5)$. This gives us the equivalence classes shown in Table 3.

Table 3: Elements of $R/\mathfrak{m}$, $R = \mathbb{Z}/25\mathbb{Z}$

Equivalence Class	Coset	Elements
$\bar{0}$	$\mathfrak{m}$	$= \{0, 5, 10, 15, 20\}$
$\bar{1}$	$1 + \mathfrak{m}$	$= \{1, 6, 11, 16, 21\}$
$\bar{2}$	$2 + \mathfrak{m}$	$= \{2, 7, 12, 17, 22\}$
$\bar{3}$	$3 + \mathfrak{m}$	$= \{3, 8, 13, 18, 23\}$
$\bar{4}$	$4 + \mathfrak{m}$	$= \{4, 9, 14, 19, 24\}$

Then in the case $\alpha = \bar{1}$, we get

$$f_\alpha(x) = f_1(x) = \prod_{i=1}^{5}(x - \alpha_i),$$

which we can explicitly calculate as

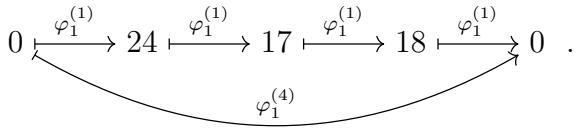
$$\begin{aligned} f_1(x) &= (x-1)(x-6)(x-11)(x-16)(x-21) \\ &= x^5 + 20x^4 + 10x^3 + 15x^2 + 5x + 24 \end{aligned}$$

If we evaluate the polynomial $\varphi_1(x)$ for each element $x \in \mathbb{Z}/25\mathbb{Z}$, then we see in Table 4 and Figure 2 that each element maps, after no more than 4 successive applications of $\varphi_1(x)$, back to itself. This example highlights the main concepts which will be proven in this section. Choose an element from the ring, say 0 for instance. Then we can see that $\varphi_1^{(n)}(0)$ takes on the values $\{24, 17, 18, 0, \dots\}$ in succession, i.e.:

Table 4: $\varphi_1(x)$ for $x \in \mathbb{Z}/25\mathbb{Z}$

$x \in R$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	...
$\varphi_1^{(1)}(x)$	24	1	3	10	22	4	6	8	15	2	9	11	13	20	...
$\varphi_1^{(2)}(x)$	17	1	10	9	23	22	6	15	14	3	2	11	20	19	...
$\varphi_1^{(3)}(x)$	18	1	9	2	5	23	6	14	7	10	3	11	19	12	...
$\varphi_1^{(4)}(x)$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	...

$x \in R$	14	15	16	17	18	19	20	21	22	23	24
$\varphi_1^{(1)}(x)$	7	14	16	18	0	12	19	21	23	5	17
$\varphi_1^{(2)}(x)$	8	7	16	0	24	13	12	21	5	4	18
$\varphi_1^{(3)}(x)$	15	8	16	24	17	20	13	21	4	22	0
$\varphi_1^{(4)}(x)$	7	14	16	18	0	12	19	21	23	5	17



Note that the nontrivial cycles have a length of 4, which is exactly the order of 2 in the unit group of $(\mathbb{Z}/5\mathbb{Z})^\times$, or $\tau(p)$, that is, 4 is the smallest number n such that $2^n = 1$ in $(\mathbb{Z}/5\mathbb{Z})^\times$. We can also clearly see here the connection between $\varphi_1(x)$ and $\varphi_1^{(n)}(x)$. The cyclic behavior of this function is one of the major ideas we work toward in the next section, although several preliminary steps are required including some for which their immediate use is less than apparent.

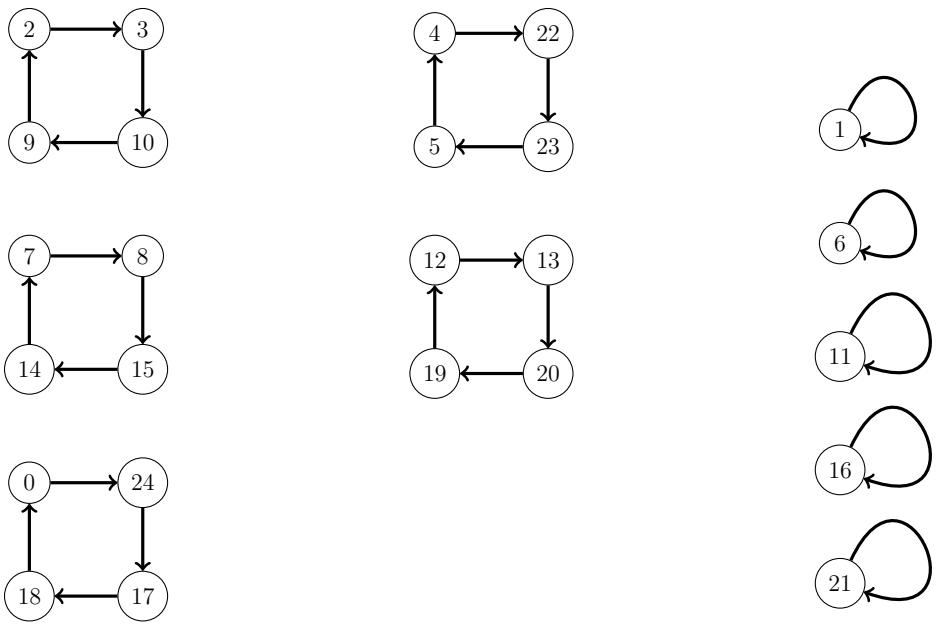


Figure 2: An α-polynomial graph.

Properties of $\varphi_\alpha(x)$ in $\mathbb{Z}/p^2\mathbb{Z}$

Let $R = \mathbb{Z}/p^2\mathbb{Z}$ with $p > 2$ a prime. Then R is a local ring with maximal ideal $\mathfrak{m}$ generated by p and residue field $R/\mathfrak{m} \cong \mathbb{Z}/p\mathbb{Z}$, which we will denote here by $\overline{R}$. Since $\overline{R} \cong \mathbb{Z}/p\mathbb{Z}$ we have $|\overline{R}| = p$ and we can write $\overline{R} = \{\alpha_1, \alpha_2, \ldots, \alpha_{p-1}, \alpha_p\}$. We will denote the groups of units of R and $\overline{R}$ as $R^\times$ and $\overline{R}^\times$ respectively. Then $f_\alpha(x) = \prod_{i=1}^{p}(x - \alpha_i)$ is an α-polynomial in $R[x]$ and we further let $\varphi_\alpha(x) = f_\alpha(x) + x$ as done previously. Note that $f_\alpha(x)$ and $\varphi_\alpha(x)$ retain those properties contained in Theorems 2.7, 2.8, 2.9, and 2.10.

LEMMA 4.1. *Let $R = \mathbb{Z}/p^2\mathbb{Z}$ with p an odd prime. Then for $r \in R$, $f_0(x) = x^p$ and $\varphi_0(x) = x^p + x$.*

Proof. First recall that the maximal ideal $\mathfrak{m}$ of R is generated by p. Then in this case we can write the elements of $\mathfrak{m}$ as $\{i \cdot p \,|\, 0 \leq i \leq p-1\}$. Hence we can write $f_0(r) = \prod_{i=0}^{p-1}(r - i \cdot p)$ as the product:

$$r(r-p)(r-2p)\ldots(r-(p-(j-1))p)(r-(p-j)p)\ldots(r-(p-2)p)(r-(p-1)p).$$

Note that since $2 \nmid |R|$, there is an odd number of elements in the product. If we let $1 \leq k \leq \dfrac{p-1}{2}$, then the product of each pair $(r - k \cdot p), (r - (p-k)p)$ gives us

$$\begin{aligned}
&(r - k \cdot p)(r - (p-k)p) \\
&= r^2 - (p - k + k)pr + (p-k)kp^2 \\
&= r^2 - p^2 r + (p-k)kp^2 = r^2.
\end{aligned}$$

Since there are an even number of elements forming such pairs excluding the $0 \cdot p$ factor,

$$\begin{aligned}
f_0(r) &= \prod_{i=0}^{p-1} (r - i \cdot p) \\
&= r \cdot \prod_{i=1}^{\frac{p-1}{2}} r^2 \\
&= r(r^2)^{\frac{p-1}{2}} = r^p
\end{aligned}$$

and thus $f_0(r) + r = r^p + r$. Hence $f_0(r) = r^p$ and $\varphi_0(r) = r^p + r$ for all $r \in R$. □

At this point it would be helpful to recall a couple of more general ideas. Fermat's Little Theorem tells us that for an integer a, $a^p \equiv a \pmod{p}$ for any prime p [2]. This guarantees for us that $x^p - x$ is a multiple of p for all x if p is a prime. The Binomial Theorem tells us

$$(x + m)^p = \sum_{i=0}^{p} \binom{p}{i} x^i m^{p-i},$$

where $\binom{p}{i} = \frac{p!}{i!(p-i)!}$ is the binomial coefficient and since p is prime, $p \mid \binom{p}{k}$ for each k such that $1 \leq k < p$ [6].

The next lemma is especially useful for simplifying some calculations of products we encounter over rings of the form $\mathbb{Z}/p^2\mathbb{Z}$ when the binomial expansion formula is used in a later proof.

LEMMA 4.2. *Let $R = \mathbb{Z}/p^2\mathbb{Z}$, with p prime, and let k and m be elements of R. Then $f_0(pk + m) = (pk + m)^p = m^p$ for all $m \in R$.*

Proof. By the Binomial Theorem we have $(pk+m)^p = \sum_{i=0}^{p} \binom{p}{i}(pk)^i m^{p-i}$. Then since $p^j = 0$ for any $j \geq 2$, $\binom{p}{i}(pk)^i m^{p-i} = 0$ whenever $i \geq 1$. Hence:

$$\begin{aligned}(pk+m)^p &= \sum_{i=0}^{p} \binom{p}{i}(pk)^i m^{p-i} \\ &= \sum_{i=0}^{0} \binom{p}{i}(pk)^i m^{p-i} \\ &= \binom{p}{0}(pk)^0 m^{p-0} = m^p.\end{aligned}$$

□

This next lemma, like the previous one, will simplify the proof of a later theorem.

LEMMA 4.3. *Let $R = \mathbb{Z}/p^2\mathbb{Z}$ with $p \neq 2$ a prime, $\mathfrak{m}$ be the maximal ideal generated by p, and denote $R/\mathfrak{m} \cong \mathbb{Z}/p\mathbb{Z}$ by $\overline{R}$. Then $2^{np} = 1$ in R if and only if $2^n = 1$ in $\overline{R}$.*

Proof. First, if $2^{np} = 1$ in R then $2^{np} = 1$ in $\overline{R}$, so by Fermat's Little theorem, $2^n = 1$ in $\overline{R}$. Then if $2^n = 1$ in $\overline{R}$ then $2^n = 1 + pk$ in R for some k. Hence $2^{np} = (1+pk)^p = 1^p = 1$. □

The next theorem gives us a formulaic way in which to write the output of repeated applications of $\varphi_\alpha(x)$ to values of $r \in R$. In particular, this theorem brings about the important role of the element 2 as well as a suggestion as to why many properties do not hold if $p = 2$. We will also see later that any finite local ring or finite field having even cardinality is similar in nature.

THEOREM 4.4. *Let $R = \mathbb{Z}/p^2\mathbb{Z}$ with $p > 2$ a prime, $f_\alpha(x) = \prod_{i=1}^{p}(x - m_i)$ with $\mathfrak{m} = \{m_1, m_2, \ldots, m_p\}$, and $\varphi_0(x) = f_0(x) + x$. Then $\varphi_0^{(n)}(r) = r + r^p \sum_{i=0}^{n-1}(2^p)^i$ for all $r \in R$.*

Proof. First, when $n = 1$ the result follows naturally since $(2^p)^0 = 1$. Now we consider the case $n = 2$. We have $\varphi_0^{(2)}(r) = \varphi_0(\varphi_0(r)) = \varphi_0(r^p + r) = \varphi_0(r^p - r + 2r)$. We know

$r^p - r = pk$ for some $k \in \mathbb{Z}$ from above. So by using Lemmas 4.1,4.2, and 4.3, we have:

$$\begin{aligned}
\varphi_0(r^p - r + 2r) &= \varphi_0(pk + 2r) \\
&= (pk + 2r)^p + pk + 2r \\
&= (2r)^p + pk + 2r \\
&= (2r)^p + r^p + r.
\end{aligned}$$

Thus $\varphi_0^{(2)}(r) = (2r)^p + r^p + r = r + \sum_{i=0}^{n-1} (2^i r)^p$.

We proceed by induction. Assume the result is true for some $n \geq 2$. Then:

$$\begin{aligned}
\varphi_0^{(n+1)}(r) &= \varphi_0\left(r + r^p \sum_{i=0}^{n-1} (2^p)^i\right) \\
&= \varphi_0\left(r + \sum_{i=0}^{n-1} \left((2^i r)^p - 2^i r\right) + \sum_{i=0}^{n-1} 2^i r\right) \\
&= \varphi_0\left(r + \sum_{i=0}^{n-1} \left((2^i r)^p - 2^i r\right) + (2^n - 1)x\right) \\
&= \varphi_0\left(\sum_{i=0}^{n-1} \left((2^i r)^p - 2^i r\right) + 2^n r\right) \\
&= \varphi_0\left(2^n r + \sum_{i=0}^{n-1} \left((2^i r)^p - 2^i r\right)\right) \\
&= (2^n r)^p + 2^n r + \sum_{i=0}^{n-1} \left((2^i r)^p - 2^i r\right) \\
&= (2^n r)^p + 2^n r + \sum_{i=0}^{n-1} (2^i r)^p - \sum_{i=0}^{n-1} 2^i r \\
&= \sum_{i=0}^{n} (2^i r)^p + 2^n r - (2^n - 1)r \\
&= r + \sum_{i=0}^{n} (2^i r)^p.
\end{aligned}$$

Therefore, by the principle of mathematical induction, the result is true for all values of n. □

This theorem lies at the core of our results and specifies the restriction on the number (n) of iterations of $\varphi_0(x)$ required such that $\varphi_\alpha(r) = r$ for some $r \in R$.

THEOREM 4.5. *Let $R = \mathbb{Z}/p^2\mathbb{Z}$, with p an odd prime, having its maximal ideal $\mathfrak{m}$ generated by p. Also let $f_0(x)$ be an α-polynomial, and $\varphi_0(x) = f_0(x) + x$. Then for any unit $u \in R$ the smallest value of n such that $\varphi_0^{(n)}(u) = u$ is $n = \tau(p)$.*

Proof. Let $S = \sum_{i=0}^{n-1} x^i$ so that $\sum_{i=1}^{n} x^i = xS$ and hence $1 - x^n = (1-x)S$ as functions. Substituting 2^p for x we see that $1 - (2^p)^n = (1-2^p)S$ in R if $(1-2^p)$ is a unit.

Suppose to the contrary that $1-2^p$ is not a unit, then by Theorem 2.1, $1-2^p \in \mathfrak{m}$. Then $1-2^p = 0$ in the residue field $R/\mathfrak{m}$ and thus we have $2^p = 1$, but we simultaneously have $2^p = 2 \pmod{p}$ by Fermat's Little Theorem and hence $1 = 2$, a contradiction. Therefore $1 - 2^p$ is a unit in R and so we also have

$$\sum_{i=0}^{n-1} (2^p)^i = \frac{1-2^{np}}{1-2^p}.$$

If we combine this result with with that of Theorem 4.4 we obtain

$$\varphi_0^{(n)}(u) = u + u^p \sum_{i=0}^{n-1} (2^p)^i = u + u^p \cdot \frac{1-2^{np}}{1-2^p}.$$

Observe in particular that $\varphi_0^{(n)}(u) = u$ if and only if $u^p \cdot \dfrac{1-2^{np}}{1-2^p} = 0$, and since $1-2^p$ is a unit, if and only if $u^p \cdot (1-2^{np}) = 0$. Then since u is a unit we then have $1 - 2^{np} = 0$, that is, $2^{np} = 1$ in R. By Lemma 4.3, $2^n = 1$ in $\overline{R}$. So n is some multiple of $\tau(p)$. Hence $\varphi_0^{(n)}(u) = u$ where n is a multiple of $\tau(p)$ and $\tau(p)$ is the smallest such n. Suppose to the contrary that there is a smaller n, then we have $2^n = 1$ and $n < \tau(p)$, so $\tau(p)$ is not the order of two in the unit group, a contradiction. Hence the smallest such n is precisely $\tau(p)$. □

We now have the result needed that we can tie everything together and show that α-polynomials exhibit the same behavior we observed in the example in this section, in

particular that α-polynomials create cycles of the elements once connected with a graph theoretic interpretation of the function.

THEOREM 4.6. *For an α-polynomial $f_0(x)$, for every r in $R = \mathbb{Z}/p^2\mathbb{Z}$, either r is a fixed point of $\varphi_0(x)$ or $\varphi_0^{(n)}(r)$ is generates a nontrivial cycle, i.e. every element of R is in a distinct cycle and any cycle containing a fixed point has length 1.*

Proof. By Theorem 2.1, every element of R is either a unit or is in the maximal ideal. For any unit element $r \in R$ we directly apply Theorem 4.5 and have that $\varphi_0^{(n)}(r) = r$ where n is $\tau(p)$, i.e., r is in a cycle of length $\tau(p)$.

For any nonunit element $r \in R$, $r \in \mathfrak{m}$ by Theorem 2.1, so in $\overline{R}$, $r \in \overline{0}$ and thus by Theorem 2.3, r is a fixed point of $\varphi_0(x)$. Then in a graph we have r is adjacent to r and to no other elements, so r is in a cycle with length 1.

Therefore, since every element of R is either a unit or in the maximal ideal, every element of R is in a cycle and any cycle containing a fixed point has length 1. □

COROLLARY 4.7. *For the ring $R = \mathbb{Z}/p^2\mathbb{Z}$ and an α-polynomial $f_0(x)$ in $R[x]$, there are p fixed points and m cycles of length $\tau(p)$ where $m = \dfrac{|R^\times|}{\tau(p)}$.*

We note that the corollary essentially just depends on the calculation of the size of the cyclic subgroup generated by 2 which is $\tau(p)$.

Here we have taken a product of elements belonging to the same congruence class of a ring $\mathbb{Z}/p^2\mathbb{Z}$ modulo its maximal ideal, $f_0(x)$, and shown that the associated function $\varphi_0(x)$ generates cycles of elements partitioning the ring and we can explicitly know the size for any given prime by calculating the appropriate $\tau(p)$ for that ring.

ALPHA-POLYNOMIALS IN LOCAL RINGS

While in $\mathbb{Z}/p^2\mathbb{Z}$ we obtain an interesting connection to graph theory, we can obtain similar results for $\varphi_\alpha(x)$ in a more general setting.

Throughout this section we take R to be a finite local ring with principal maximal ideal $\mathfrak{m}$ such that $\mathfrak{m}^2 = 0$ and $2 \nmid |R|$ and further suppose that R is not a field. We say $|R/\mathfrak{m}| = q$ and note that R is in the scope of Theorems 2.1-2.10.

LEMMA 5.1. *Let R be a local ring as above and assume $|R/\mathfrak{m}| = q$, then $|\mathfrak{m}| = q$ as well.*

Proof. We will consider R and $\mathfrak{m}$ as R-modules and define a function $\psi : R \twoheadrightarrow \mathfrak{m}$ by $r \mapsto rm$ for every $r \in R$ where m is the principal generator of $\mathfrak{m}$. Since we have the preservation of addition and multiplication, by

$$\psi(r_1 + r_2) = (r_1 + r_2)m = r_1m + r_2m = \psi(r_1) + \psi(r_2), \text{ and}$$
$$\psi(rr_1) = (rr_1)m = r(r_1m) = r\psi(r_1),$$

ψ is an R-module homomorphism. Let k be the annihilator of $\mathfrak{m}$, that is, $k = \{r \in R \mid rm = 0\}$. We claim that $k = \mathfrak{m}$ is the kernel of ψ. First, since $\mathfrak{m}^2 = 0$, $\mathfrak{m} \subseteq k$. Conversely, suppose $rm = 0$ for some $r \in R$ such that $r \notin \mathfrak{m}$. Since $r \notin \mathfrak{m}$, r is a unit by Theorem 2.1. Thus $rm = 0$ implies $m = 0$, which is a contradiction, hence we have $r \in \mathfrak{m}$ and $k \subseteq \mathfrak{m}$. Therefore $k = \mathfrak{m}$ and by the First Isomorphism Theorem for modules we have $R/\mathfrak{m} \cong \mathfrak{m}$ and in particular $|\mathfrak{m}| = |R/\mathfrak{m}| = q$. □

As a preliminary to further discussion, we need to ensure that $q \in \mathfrak{m}$ so that a product of $qm = 0$ for any $m \in \mathfrak{m}$ whenever $\mathfrak{m}^2 = 0$. This will be used in particular in Lemma 5.3 and Theorem 5.5.

LEMMA 5.2. *Let R be a local ring with maximal ideal $\mathfrak{m}$ and $q = |R/\mathfrak{m}|$. Then $q \in \mathfrak{m}$.*

Proof. We will consider $R/\mathfrak{m}$ as an additive group temporarily. Since it has cardinality q, we know by Lagrange's theorem that for any $g \neq 0$ in $(R/\mathfrak{m}, +)$, that g generates

some subgroup of $(R/\mathfrak{m}, +)$ and the order of that subgroup divides q since $|R/\mathfrak{m}| = q$ and thus for all g, $gq = 0$. In particular we have $q = 1q = 0$ and thus $q = 0$ in $R/\mathfrak{m}$, hence $q \in \mathfrak{m}$. □

Since $q \in \mathfrak{m}$, we gain a computational advantage in binomial expansions where q then plays an important role as see in the following lemma.

LEMMA 5.3. *Let R be a local ring with maximal ideal $\mathfrak{m}$ and $r \in R$. Then $r^q = 1$ in R if and only if $\overline{r} = 1$ in $R/\mathfrak{m}$.*

Proof. First, if $r^q = 1$ in R then $r^q = 1$ in $R/\mathfrak{m}$ by the natural map. Since $R/\mathfrak{m}$ is a field, by extending Fermat's Little theorem, $\overline{r} = \overline{r}^q = 1$ in $R/\mathfrak{m}$.

Now if $\overline{r} = 1$ in $R/\mathfrak{m}$ then $r = 1 + m$ in R for some $m \in \mathfrak{m}$. Raising both sides to the power q, we see that using a binomial expansion:

$$r^q = (1+m)^q = 1 + qm + \binom{q}{2} m^2 + \cdots + qm^{q-1} + m^q = 1$$

since $q \in \mathfrak{m}$ by Lemma 5.2 so that $qm = 0$ and since $m^i = 0$ for every $i \geq 2$. Therefore $r^q = 1$ in R if and only if $\overline{r} = 1$ in $R/\mathfrak{m}$. □

We have previously defined an α-polynomial for a local ring and explored some related properties. We had for any α in the residue field $R/\mathfrak{m}$ an α-polynomial given by $f_\alpha(x) = \prod_{i=1}^{t}(x - \alpha_i)$ where $t = |\mathfrak{m}|$, which will be q here by Lemma 5.1, and each α_i is a member of α. Of particular interest is the "0" congruence class corresponding to the maximal ideal since we had other properties allowing us to shift from the polynomial for one congruence class to that of another. We also made use of the functions $\varphi_\alpha(x)$ and $\varphi_\alpha^{(n)}(x)$ corresponding to each $f_\alpha(x)$ which we will again see here.

LEMMA 5.4. *Let R be a finite local ring with maximal ideal $\mathfrak{m}$ such that $2 \nmid |R|$ and $\mathfrak{m}^2 = 0$. Then for an α-polynomial $f_0(x) = \prod_{i=1}^{q}(x - m_i)$, where $\mathfrak{m} = \{m_1, m_2, \ldots, m_q\}$, $f_0(x) = x^q$ and $\varphi_0(x) = x^q + x$.*

Proof. By shifting the index we can write $f_0(x) = \prod_{i=0}^{q-1}(x - m_i)$ to obtain the product:

$$x(x - m_1)(x - m_2)(x - m_3)\dots(x - m_{q-2})(x - m_{q-1})$$

where we have taken m_0 to be the zero element of R. Note that since $2 \nmid |R|$, there are an odd number of elements in the product. Since the maximal ideal is a subring and thus a group under addition, excluding the zero element there exist pairs m_i, m_j such that $m_i + m_j = m_0$. Note that if $i = j$, then $m_i + m_j = m_i + m_i = 2m_i = 0$, which implies $2 \in \mathfrak{m}$ and consequently $q = 2^n$ contradicting the condition that $2 \nmid |R|$ and hence $i \neq j$ for all i and j.

If we take k such that $1 \leq k \leq \dfrac{q-1}{2}$ and relabel as necessary to match up the pairs, then similar to the result we obtained in Lemma 4.1, the product of each pair $(x - m_k), (x - m_{q-k})$ yields:

$$\begin{aligned}
&(x - m_k)(x - m_{q-k}) \\
&= x^2 - (m_k + m_{q-k})x + m_k m_{q-k} \\
&= x^2 - 0x + 0 = x^2.
\end{aligned}$$

In other words we get a factor of x^2 for each pair. Since there are also an even number elements forming such pairs after excluding the remaining factor corresponding to 0:

$$\begin{aligned}
f_0(x) &= \prod_{i=0}^{q-1}(x - m_i) \\
&= x \cdot \prod_{i=1}^{\frac{q-1}{2}} x^2 \\
&= x(x^2)^{\frac{q-1}{2}} \\
&= x \cdot x^{q-1} = x^q
\end{aligned}$$

and thus $f_0(x) + x = x^q + x$ as well.

Therefore we have $f_0(x) = x^q$ and $\varphi_0(x) = x^q + x$ as functions. □

What we have gained from this is a simpler form for computation like we had before. We also need to establish some other helpful properties in order to achieve our main result. The following result shows that passing a sum of elements, if one element is an element from the maximal ideal, it essentially falls back out of the function $\varphi_o(x)$ in a similar manner as the additive property of a ring homomorphism since as we saw in Theorem 2.7, the elements of the maximal ideal are roots of $f_0(x)$ and thus are are fixed points of the function $\varphi_0(x)$.

LEMMA 5.5. *Let R be a finite local ring with maximal ideal $\mathfrak{m}$ such that $2 \nmid |R|$ and $\mathfrak{m}^2 = 0$. Further let $a \in \mathfrak{m}$ and $b \in R$. Then $\varphi_0(a + b) = a + \varphi_0(b)$.*

Proof. By Lemma 5.1 we know $|R/\mathfrak{m}| = |\mathfrak{m}| = q$. By Lemma 5.2 $q \in \mathfrak{m}$ so $aq = 0$ since $\mathfrak{m}^2 = 0$. Further, since $a \in \mathfrak{m}$, we have $a^j = 0$ for all $j \geq 2$. Then using a binomial expansion that in a similar manner as Lemma 4.2, we see that:

$$\begin{aligned}
\varphi_0(a+b) &= (a+b)^q + (a+b) \\
&= a^q + qa^{q-1}b + qa^{q-2}b^2 + \cdots + qab^{q-1} + b^q + a + b \\
&= b^q + a + b \\
&= a + (b^q + b)
\end{aligned}$$

Then since $b^q + b = \varphi_0(b)$, we have $\varphi_0(a + b) = a + \varphi_0(b)$. □

Recall that we previously used $\varphi_\alpha^{(n)}(x)$ to denote the application of $\varphi_\alpha(x)$ n times. In the next theorem we find a formula for expressing the value of $\varphi_0^{(n)}$ specifically.

THEOREM 5.6. *Let R be a local ring such that $2 \nmid |R|$ with maximal ideal $\mathfrak{m}$ such that $\mathfrak{m}^2 = 0$. Then $\varphi_0^{(n)}(r) = r + r^q \sum_{i=0}^{n-1} (2^q)^i$ for all $r \in R$.*

Proof. We proceed by induction. First, when $n = 1$ we have $\varphi_0^{(1)}(r) = r^q + r = r + r^q \sum_{0}^{0} (2^q)^i$, so the result holds when $n = 1$. Now we will need to use the fact that $r^q - r$

is in the maximal ideal and apply Lemma 5.5 to $r^q - r$, which we get by rearranging our expression.

$$\begin{aligned}
\varphi_0^{(2)}(r) &= \varphi_0(r^q + r) \\
&= \varphi_0(r^q - r + 2r) \\
&= r^q - r + \varphi_0(2r) \\
&= r + r^q + 2^q r^q \\
&= r + r^q \sum_0^1 (2^q)^i \\
&= r + \sum_0^1 (2^i r)^q
\end{aligned}$$

Now we assume the result is true for some $k \geq 2$. Here we are going to use the fact that $\sum_{i=0}^{k-1} ((2^i r)^q - 2^i r) \in \mathfrak{m}$ since $(2^i r)^q - 2^i r \in \mathfrak{m}$ for each i and so we have a sum of elements in the maximal ideal. Then we have:

$$\begin{aligned}
\varphi_0^{(k+1)}(r) &= \varphi_0 \left(r + r^q \sum_{i=0}^{k-1} (2^q)^i \right) \\
&= \varphi_0 \left(r + \sum_{i=0}^{k-1} (2^i r)^q - \sum_{i=0}^{k-1} 2^i r + \sum_{i=0}^{k-1} 2^i r \right) \\
&= \varphi_0 \left(r + \sum_{i=0}^{k-1} \left((2^i r)^q - 2^i r \right) + r \sum_{i=0}^{k-1} 2^i \right) \\
&= \varphi_0 \left(r + \sum_{i=0}^{k-1} \left((2^i r)^q - 2^i r \right) + (2^k - 1) r \right) \\
&= \varphi_0 \left(\sum_{i=0}^{k-1} \left((2^i r)^q - 2^i r \right) + r 2^k \right) \\
&= \varphi_0 \left(2^k r + \sum_{i=0}^{k-1} \left((2^i r)^q - 2^i r \right) \right) \\
&= (2^k r)^q + 2^k r + \sum_{i=0}^{k-1} \left((2^i r)^q - 2^i r \right)
\end{aligned}$$

$$= (2^k r)^q + 2^k r + \sum_{i=0}^{k-1} (2^i r)^q - \sum_{i=0}^{k-1} 2^i r$$
$$= \sum_{i=0}^{k} (2^i r)^q + 2^k r - (2^k - 1)r$$
$$= r + \sum_{i=0}^{k} (2^i r)^q.$$

Therefore, by the principle of mathematical induction, the result is true for all values of n. □

This result will be of immediate benefit as we use it to determine the size of cycles made by repeated applying $\varphi_0(x)$ to elements of R. We also observe that this is analogous to our main result for rings $\mathbb{Z}/p^2\mathbb{Z}$ in Theorem 4.5 though in a more general setting.

THEOREM 5.7. *Let R be a local ring having maximal ideal $\mathfrak{m}$ with a finite residue field of cardinality $q = p^n$ and such that $\mathfrak{m}^2 = 0$. Also let $f_0(x)$ be an α-polynomial and $\varphi_0(x) = f_0(x) + x$. Then for any unit $u \in R$ the smallest value of n such that $\varphi_0^{(n)}(u) = u$ is $n = \tau(p)$.*

Proof. We begin the proof in a manner similar to Theorem 4.5.

Let $S = \sum_{i=0}^{n-1} x^i$ so that $\sum_{i=1}^{n} x^i = xS$ and hence $1 - x^n = (1 - x)S$ as functions. Substituting 2^q for x we see that $1 - (2^q)^n = (1 - 2^q)S$ in R if $(1 - 2^q)$ is a unit. If $1 - 2^q$ were not a unit, then by Theorem 2.1, $1 - 2^q \in \mathfrak{m}$ and thus $\overline{2^q} = \overline{1}$ in $R/\mathfrak{m}$, but $R/\mathfrak{m}$ is a field and so by way of an extension of Fermat's Little Theorem we have $2^q = 2$, which is a contradiction since then we have $1 = 2$ forcing $R/\mathfrak{m} = \{0\}$. Hence $2^q - 1$ is a unit in R. Then we have

$$\sum_{i=0}^{n-1} (2^q)^i = \frac{1 - 2^{nq}}{1 - 2^q}.$$

If we combine this result with with that of Theorem 5.6 we obtain

$$\varphi_0^{(n)}(u) = u + u^q \sum_{i=0}^{n-1} (2^q)^i = u + u^q \cdot \frac{1 - 2^{nq}}{1 - 2^q}.$$

Observe in particular that $\varphi_0^{(n)}(u) = u$ if and only if $u^q \cdot \dfrac{1-2^{nq}}{1-2^q} = 0$, and since $1-2^q$ is a unit, if and only if $u^p \cdot (1-2^{nq}) = 0$. Then since u is a unit we then have $1-2^{nq} = 0$, that is, $2^{nq} = 1$ in R. By Lemma 5.3, $2^n = 1$ in $\overline{R}$. So $\tau(p) \mid n$. Hence $\varphi_0^{(n)}(u) = u$ where n is a multiple of $\tau(p)$. Suppose there is a smaller n, then $2^n = 1$ and $\tau(p)$ is not the order of two in the unit group, a contradiction. Hence the smallest such n is precisely $\tau(p)$. □

Now we present our more generalised main result. The following theorem combines some of the earlier, and more general, results about $\varphi_\alpha(x)$ with those of the current section to show that $\varphi_0(x)$ generates cycles in any finite local ring where $\mathfrak{m}^2 = 0$.

THEOREM 5.8. *Let R be a local ring having maximal ideal $\mathfrak{m}$ with a finite residue field of cardinality $q = p^n$ and such that $\mathfrak{m}^2 = 0$. Also let $f_0(x)$ be an α-polynomial and $\varphi_0(x) = f_0(x) + x$ Then for every $r \in R$, either r is a fixed point of $\varphi_0(x)$ or $\varphi_0(x)$ generates a cycle of length $\tau(p)$ containing r, namely $(r, \varphi_0(r), \varphi_0^{(2)}(r), \dots)$, i.e. every element of R is in a cycle and any cycle containing a fixed point has length one.*

Proof. By Theorem 2.1, every element of R is either a unit or is in the maximal ideal. For any unit element $r \in R$ we directly apply Theorem 5.7 and have that $\varphi_0^{(\tau(p))}(r) = r$, i.e., r is in a cycle of length $\tau(p)$.

For any nonunit element $r \in R$, $r \in \mathfrak{m}$ by Theorem 2.1, so in $\overline{R}$, $r \in \overline{0}$ and thus by Theorem 2.3, r is a fixed point of $\varphi_0(x)$. Then in a graph we have r is adjacent to r and to no other elements, so r is in a cycle with length one.

Therefore, since every element of R is either a unit or in the maximal ideal, every element of R is in a cycle and any cycle containing a fixed point has length one. □

Thus we conclude our main results, every element of a local ring R having the property $\mathfrak{m}^2 = 0$ is contained in a cycle under $\varphi_0(x)$. Throughout we have assumed that the rings are not fields. The case for fields, as we are about to observe, is simpler since the maximal ideal has a single element. This causes our polynomial to be linear.

The next section answers the question about what happens with $f_\alpha(x)$ and $\varphi_\alpha(x)$ if the maximal ideal is exactly $\{0\}$. It will also serve to establish constructions of finite fields that will be used in the section following it when we examine local rings having even cardinality, another previously excluded case when we required $2 \nmid |R|$.

ALPHA-POLYNOMIALS IN FINITE FIELDS

Up to this point we have precluded the case of finite local rings where the maximal ideal is identically zero, i.e. finite fields. The curious reader may be interested to see how α-polynomials behave over finite fields. Let $\mathbb{F}_q$ be a finite field where $q = p^n$ for some prime p. For the moment we will assume $2 \nmid q$, i.e., $q \neq 2^n$. In this case each maximal ideal has exactly one element, i.e., $\mathfrak{m} = \{0\}$ and so we get

$$f_0(x) = \prod_{i=1}^{1}(x - m_i) = x - 0 = x,$$

so $f_0(x)$ is the identity function on $\mathbb{F}_q$ and hence

$$\varphi_0(x) = f_0(x) + x = x + x = 2x.$$

THEOREM 6.1. *Let $\mathbb{F}_q$ where $q = p^n$ for some odd prime p. Then $\varphi_0^{(p-1)}(x) = x$ and further, $\tau(p)$ is the smallest such value of n such that $\varphi_0^{(n)}(x) = x$.*

Proof. First observe that $\varphi_0^{(2)}(x) = \varphi_0(\varphi_0(x)) = \varphi_0(2x) = 4x$. Then we proceed by induction. Assume $\varphi_0(\varphi_0^{(k)}(x)) = 2^{k+1}x$ is true for some k. Then we have $\varphi_0^{(k+1)}(x) = \varphi_0(\varphi_0^{(k)}(x)) = \varphi_0(2^k x) = 2^{k+1}x$. Therefore by the principle of mathematical induction the result is true for every k. Since 2 is in $\mathbb{F}_q$ and in its prime subfield $\mathbb{F}_p$, it is in the unit groups $\mathbb{F}_q^\times$ of $\mathbb{F}_q$ and $\mathbb{F}_p^\times$ of $\mathbb{F}_p$, hence $2^{p-1} = 1$ in $\mathbb{F}_p$ and so $2^{p-1} = 1$ in $\mathbb{F}_q$ as well since $\mathbb{F}_q$ has characteristic p. Hence $\varphi_0^{(p-1)}(x) = x$. Since $2^{\tau(p)} = 1$ in $\mathbb{F}_p$ and $\tau(p) \leq p - 1$ by definition, $\tau(p)$ divides $p - 1$ by Lagrange's Theorem and so $p - 1$ is some multiple of $\tau(p)$. Suppose that $\tau(p)$ is not the smallest value of n such that $\varphi_0^{(n)}(x) = x$, then there exists some $n \leq \tau(p)$ such that $2^n = 1$ in $\mathbb{F}_p$, but this is a contradiction by the definition of $\tau(p)$ and thus $\tau(p)$ is the smallest value of n such that $\varphi_0^{(n)}(x) = x$. □

We consider now the cases of $\mathbb{F}_2$ and $\mathbb{F}_4$, fields with even characteristic. First, since $\mathbb{F}_2 \cong \mathbb{Z}/2\mathbb{Z}$, it can not possibly exhibit the same behavior as those in the pre-

vious theorem since 2 is not even in the unit group. In fact, since any even field has characteristic 2, by Theorem 6.1 we will have $f_0(x)$ is the identity function and $\varphi_0(x)$ is the zero function. We will consider $\mathbb{F}_4$ in full, partly to exemplify this behavior as a particular example, but also to construct $\mathbb{F}_4$ since it will be used again in the next section to construct a particular local ring.

To construct $\mathbb{F}_4$ we use the usual manner of finite field construction [2]. We will take the polynomial ring $\mathbb{F}_2[S]$ and use an irreducible polynomial ideal as a modulus to obtain the construction

$$\mathbb{F}_4 = \frac{\mathbb{F}_2[S]}{(S^2 + S + 1)} = \{0, s, 1, 1 + s\}.$$

Then we observe that under $f_0(r)$ and $\varphi_0(r)$ we get the values found in Table 5.

Table 5: Computation in $\mathbb{F}_4$

r	$f_0(r)$	$\varphi_0(r)$
0	0	0
s	s	0
1	1	0
$1+s$	$1+s$	0

.

What we see is that $f_0(r)$ is again the identity function on the field, but $\varphi_0(r)$ is a zero function. So in at least the first two even-ordered finite fields the same functions behave differently exemplifying the necessity of requiring $2 \nmid q$.

ALPHA-POLYNOMIALS IN LOCAL RINGS OF EVEN CARDINALITY

Previously we have observed the behavior of $\varphi_\alpha(x)$ in local rings R where $2 \nmid |R|$. In this section we present some counterexamples in order to show what happens in some particular local rings with even cardinality and somewhat justify their previous exclusion. In essence we are going to explore what happens when $2 \mid |R|$. We are going to assume that $f_0(x) = x^t$, where $t = |\mathfrak{m}|$, and $\varphi_0(x) = f_0(x) + x$ as we had previously obtained and further assume they are well-defined functions. According to Ganske and McDonald, there are exactly 3 local rings of order 4: $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{F}_4$, and $(\mathbb{Z}/2\mathbb{Z})[Y]/(Y^2)$ [3]. Since we previously examined the case of $\mathbb{F}_4$, this leaves us with two additional rings of order 4 to explore. In addition we will also consider the ring $\mathbb{F}_4[\Theta]/(\Theta^2)$.

Behavior In $\mathbb{Z}/4\mathbb{Z}$

The ring $\mathbb{Z}/4\mathbb{Z}$ has even cardinality and is of the form $\mathbb{Z}/p^2\mathbb{Z}$ which was explored in an earlier section. We denote the elements as $\mathbb{Z}/4\mathbb{Z} = \{0, 1, 2, 3\}$. Observe that here we have $t = |\mathfrak{m}| = 2$ and thus $f_0(x) = x^2$ and $\varphi_0(x) = x^2 + x$. Then for each r in $\mathbb{Z}/4\mathbb{Z}$ compute the results found in Table 6 and Figure 3.

Table 6: Computation in $\mathbb{Z}/4\mathbb{Z}$

r	$f_0(r)$	$\varphi_0(r)$
0	0	0
1	1	2
2	0	2
3	1	0

.

Figure 3: Behavior in $\mathbb{Z}/4\mathbb{Z}$.

Behavior In $\mathbb{F}_2[X]/(X^2)$

Here we have $\mathbb{F}_2[Y]/(Y^2) = \{0, 1, y, 1+y\}$ which has $t = |\mathfrak{m}| = 2$ and so $f_0(x) = x^2$ and $\varphi_0(x) = x^2 + x$. We see then in Table 7 and Figure 4 the resulting values.

Table 7: Computation in $\mathbb{F}_2[Y]/(Y^2)$

r	$f_0(r)$	$\varphi_0(r)$
0	0	0
1	1	0
y	0	y
$1+y$	1	y

.

Figure 4: Behavior in $\mathbb{F}_2[Y]/(Y^2)$.

Behavior In $\mathbb{F}_4[\Theta]/(\Theta^2)$

In the previous section on α-polynomials over finite fields we constructed $\mathbb{F}_4$. Now we will use it as the base ring of a finite local ring having 16 elements. Let $R = \mathbb{F}_4[\Theta]/(\Theta^2)$ so that in this case we have $t = |\mathfrak{m}| = 4$ where each element of $\mathfrak{m}$ has the form $r\theta$ with r being any element of $\mathbb{F}_4$, so $f_0(x) = x^4$ and $\varphi_0(x) = x^4 + x$. This ring is of the same form as those for which our main result was proven, a local ring which is not a field such that $\mathfrak{m}^2 = 0$, except that here we have $2 \mid |R|$.

So what we observe in Table 4 and Figure 5 is that each value under the function $\varphi_0(x)$ collapses to one of 4 values, a behavior more similar to π-polynomials than α-polynomials. Further, the values to which $\varphi_0(x)$ sends all of the elements of the ring are exactly the elements of the maximal ideal and those elements of the maximal ideal remain fixed under $\varphi_0(x)$.

Table 8: Computation in $\mathbb{F}_4[\Theta]/(\Theta^2)$

r	$f_0(r)$	$\varphi_0(r)$
0	0	0
1	1	0
s	s	0
$1+s$	$1+s$	0
θ	0	θ
$s\theta$	0	$s\theta$
$(1+s)\theta$	0	$(1+s)\theta$
$1+\theta$	1	θ
$1+s\theta$	1	$s\theta$
$1+(1+s)\theta$	1	$(1+s)\theta$
$s+\theta$	s	θ
$s+s\theta$	s	$s\theta$
$s+(1+s)\theta$	s	$(1+s)\theta$
$(1+s)+\theta$	$(1+s)$	θ
$(1+s)+s\theta$	$(1+s)$	$s\theta$
$(1+s)+(1+s)\theta$	$(1+s)$	$(1+s)\theta$

.

What we ultimately observe is that none of these rings of even order have the same behavior for an α-polynomial $f_\alpha(x)$ or the associated function $\varphi_\alpha(x)$.

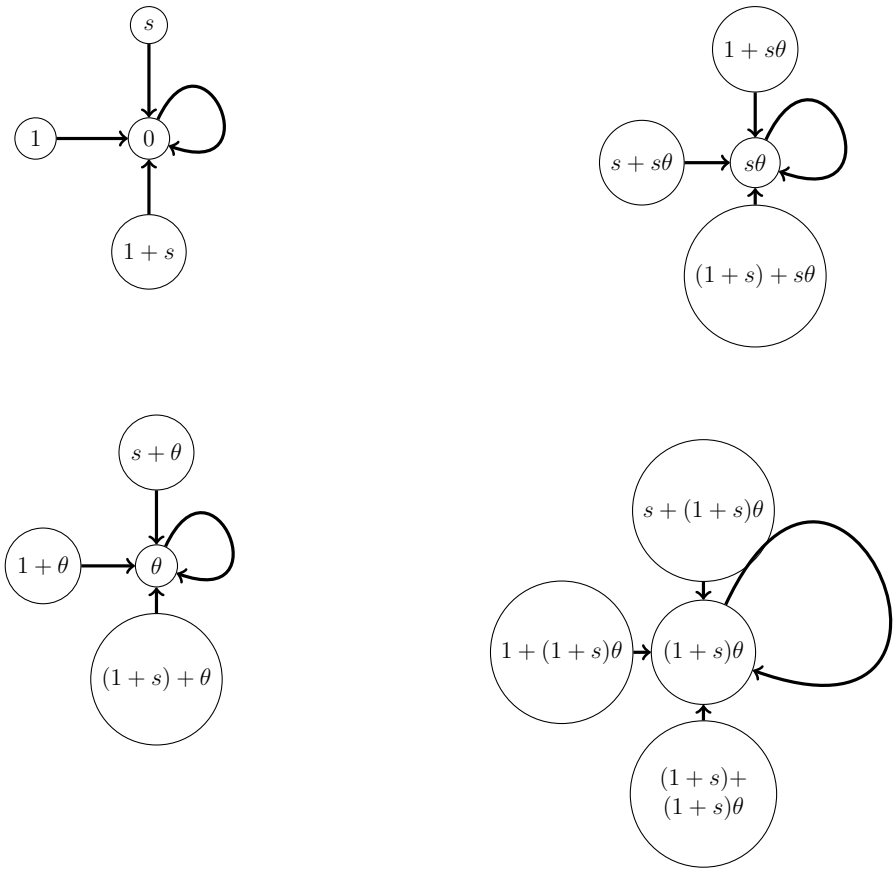


Figure 5: Behavior in $\mathbb{F}_4[\Theta]/(\Theta^2)$.

REFERENCES

[1] Béla Bollobás, *Modern Graph Theory*, Springer, New York, 1998.

[2] David S. Dummit and Richard M. Foote, *Abstract Algebra*, 3rd ed., Wiley, New York, 2004.

[3] G. Ganske and B. R. McDonald, *Finite Local Rings*, Rocky Mountain Journal of Mathematics **3** (1973), no. 4, 521-540, DOI 10.1216/RMJ-1973-3-4-521.

[4] Bernard R. McDonald, *Finite Rings with Identity*, Marcel Dekker, Inc., New York, 1974.

[5] Mark Rogers and Cameron Wickham, *Polynomials Inducing the Zero Function on Local Rings*, Preprint (2016).

[6] Kenneth H. Rosen, *Elementary Number Theory*, 6th ed., Pearson, Boston, 2015.

[7] W. A. Stein et al., *Sage Mathematics Software (Version 7.1)*, 2016. The Sage Development Team.

APPENDICES

Appendix A. Graph Theory

Terminology and Definitions. The following graph theoretic definitions and terminology are based on Bollobás' *Modern Graph Theory* [1].

A (directed) *graph* G is an ordered pair of disjoint sets (V, E) such that $E \subseteq V \times V$. We take by assumption, unless mentioned otherwise, that both V and E are finite sets. The set V is the set of all *vertices* and the set E is the set of *edges*. An edge (v_1, v_2) is said to *join* the vertices v_1 and v_2. For any $v_1, v_2 \in V$, if $(v_1, v_2) \in E$ then we say v_1 and v_2 are *adjacent*.

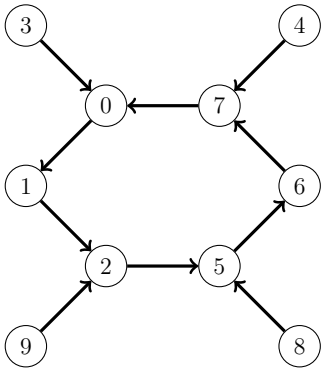
We say that a graph $G' = (V', E')$ is a *subgraph* of $G = (V, E)$ if $V' \subseteq V$ and $E' \subseteq E$, and typically we write $G' \subseteq G$. We define the *order* of G to be the number of vertices in V and we may write $|G| = |V| = n$, where n is the number of vertices in V.

We take a *path* P of the graph $G = (V, E)$ to be a sequence of distinct vertices such that each of the vertices are joined by an edge; that is, a path P is a subgraph of G consisting of a sequence of distinct vertices $V' = \{v_1, \ldots, v_\ell\} \subseteq V$ and edges $E' = \{(v_1, v_2), (v_2, v_3), \ldots, (v_{\ell-1}, v_\ell)\} \subseteq E$. Then $P = (V', E') \subseteq G$. We will often use the abbreviated form $(v_1, \ldots, v_\ell)$ for a path from an *initial* vertex, v_1, to a *terminal* vertex, v_ℓ. If the path includes the edge (v_ℓ, v_1) then we call it a *cycle*.

We further say that two graphs, $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$, are isomorphic if there is a one-to-one correspondence $\phi : V_1 \to V_2$ between their vertex sets that preserves adjacency; in other words, two graphs are isomorphic if $|V_1| = |V_2|$ and an edge $(v_1, v_2) \in E_1$ if and only if $(\phi(v_1), \phi(v_2)) \in E_2$, or put another way, $\forall a, b \in V_1$, a is adjacent to b in G_1 if and only if $\phi(a)$ is adjacent to $\phi(b)$ in G_2.

A function graphing example. As an exercise in using graph theory to visually assess the behavior of functions we can construct a simple example. Let $R = \mathbb{Z}/10\mathbb{Z}$ and $f(x) = x^2 + 1$. In this ring we can quickly calculate the value of several elements, which facilitates its use as an example in connection to graph theory. For instance, we find that $f(0) = 1$, $f(1) = 2$, and $f(2) = 5$. What we then can do is identify the connection made through the mapping of elements by using a 10×10 matrix where each i^{th} row only has a nonzero entry where the image of the value corresponding to i is. This lets us quickly build the graph associated to matrix and so helps us to visualize the behavior of the function on the ring. In general we calculate the adjacency matrix to generate a graph rather than directly observing the matrix itself.

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$



Adjacency matrix and function graph

Appendix B. SAGE CODE FOR EXAMPLES

Here we present the code used to compute the main examples of this thesis. The graphs contained throughout were written in LaTeX using the *Tikz* package, but were based on the graphs obtained from the following code as well as other similar computation.

Example for π-polynomial in $\mathbb{Z}/27\mathbb{Z}$. For the example for a π-polynomial in Section 2 we used the following code:

```
R1 = Integers(27)
elem = list(R1)
P1 = PolynomialRing(R1, 'x')
pi_x = (x-0)*(x-1)*(x-2)+x
pi_x = pi_x.expand()
pi_x =P1(pi_x)
pi_x
A = matrix(27,27,0)
for i in xrange(len(elem)):
        x_val = elem[i]
        x_val = pi_x(x_val)
        A[i,int(x_val)] = int(1)
C = copy(A)
G = DiGraph(C)
H = G.plot(graph_border = True)
H.show(figsize = [15,15])
```

Example for α-polynomial in $\mathbb{Z}/25\mathbb{Z}$. For the α-polynomial example in Section 4 we used the following code:

```
p = 5; n = 2
R0 = Integers(p)
R1 = Integers(p^n)
P0 = PolynomialRing(R0, 'x')
P1 = PolynomialRing(R1, 'x')
elements = list(R1)
cosets = list()
for i in R0:
    cosets.append(list())
for i in R1:
    x_val = i%(R0.characteristic())
    cosets[x_val].append(i)
for i in cosets:
    if P1.one() in i:
        i
        alpha_x = P1.one()
        for j in i:
            alpha_x *= (x-j)
        alpha_x += x
        alpha_x = alpha_x.expand()
        alpha_x = P1(alpha_x)
        alpha_x
        A = matrix(p^n,p^n,0)
        for i in xrange(len(elements)):
            x_val = elements[i]
            x_val = pi_x(x_val)
            A[i,int(x_val)] = int(1)
        G = DiGraph(A)
        H = G.plot(graph_border=True)
        H.show(figsize = [20,10])
```