Polynomial Functions

Over Finite Rings

by

Sara R. Logsdon

(Under the direction of Pete L. Clark)

Abstract

In this thesis, we explore properties of the ring of polynomials $P(R, R)$ over a finite ring R. We examine the kernel of the evaluation map $E : R[t] \to P(R, R)$ to find $\#P(R, R)$, first for when nilpotency index a is at most residue cardinality q, and next when $a = q + 1$. We identify criteria for when all ideals of $P(R, R)$ are principal and look at concrete examples, and we put an R-module structure on $P(R, R)$. Finally, we examine these same questions for the ring $P(R^N, R)$.

Index words: Ring Theory, Polynomials, Commutative Algebra

Polynomial Functions Over Finite Rings

by

Sara R. Logsdon

A Thesis Submitted to the Graduate Faculty
of The University of Georgia in Partial Fulfillment
of the
Requirements for the Degree

Master of Arts

Athens, Georgia

2025

Polynomial Functions

Over Finite Rings

by

Sara R. Logsdon

Major Professor: Pete L. Clark

Committee: Leonard Chastkofsky
Dino Lorenzini

Electronic Version Approved:

Ron Walcott
Dean of the Graduate School
The University of Georgia
May 2025

Acknowledgments

This thesis would not be possible without the support of my professors and peers. I would like to express gratitude to my advisor, Dr. Pete Clark, for his indispensable guidance throughout my thesis. I would also like to thank Dr. Leonard Chastkofsky and Dr. Dino Lorenzini for serving on my committee and for supporting me throughout my academic journey. I am deeply grateful to the University of Georgia Foundation Fellowship for providing financial support that allowed me to attend this institution. I would like to thank my friends, my parents, Mike and Michelle, my brothers, Jacob and Aaron, and my partner, Joseph, for always being in my corner.

Table of Contents

Page

Chapter 1

Introduction

1.1 Background

Suppose we are given a finite ring R (in this thesis, we will assume that all rings are commutative and contain a multiplicative identity). For sets X and Y, we define the notation $Y^X := \{\text{all functions } f : X \to Y\}$. Then $R^R = \{\text{all functions } f : R \to R\}$ is also a ring, under (pointwise) addition and multiplication of maps.

There is a relation between polynomials as viewed purely as formal objects, finite R-linear combinations of monomials $c_0 + c_1 t + \cdots + c_n t^n$ (elements of $R[t]$) and polynomials as viewed as maps (elements of R^R). We define the evaluation map

$$E : R[t] \to R^R$$
$$f(t) \mapsto (x \to f(x))$$

Then we may define the set $P(R, R) \subseteq R^R$ as the image of $R[t]$ under E, and we define two polynomials in $R[t]$ to be equivalent if they induce the same function in $P(R, R) \subseteq R^R$. $P(R, R)$ is then a subring of R^R, and $P(R, R) \cong R[t]/\operatorname{Ker} E$. When R is an infinite domain, E is injective. This is the case that is most familiar. In this thesis, we will consider some questions about $P(R, R)$ when R is finite.

When R is a finite field $\mathbb{F}_q$, we can prove that E is surjective. This comes primarily from the fact that for all $\alpha \in \mathbb{F}_q$,

$$\alpha^q - \alpha = 0 \tag{1.1}$$

This fact is trivial if $\alpha = 0$, and when $\alpha \neq 0$, it is sufficient to prove that $\alpha^{q-1} = 1$. Lagrange's Theorem for multiplicative groups states that if G is a finite group of order n and $g \in G$, then the order of g divides n. In our case, $\mathbb{F}_q^\times = \mathbb{F}_q \setminus \{0\}$ is a multiplicative group of order $q-1$, thus for all $\alpha \in \mathbb{F}_q$, the order of α divides $q-1$, so $\alpha^{q-1} = 1$. Then for every polynomial $f(t)$ in $\mathbb{F}_q[t]$, we can divide it by $(t^q - t)$ to get an equivalent representative $g \in \mathbb{F}_q[t]$ such that $\deg(g) \leq q-1$. There are q^q polynomials in $\mathbb{F}_q[t]$ with degree $\leq q-1$, so

$$\#(\mathbb{F}_q[t]) \leq q^q.$$

But

$$\#({\mathbb{F}_q}^{\mathbb{F}_q}) = q^q$$

So we conclude that E must be surjective in this case, meaning every map $\mathbb{F}_q \to \mathbb{F}_q$ can be represented by a polynomial in $\mathbb{F}_q[t]$.

In fact, the converse is also true: if E is surjective, then R is a finite field ([4], Corollary 2.36). Since $\alpha^q - \alpha = 0$ for all $\alpha \in \mathbb{F}_q$ (we showed this in (1.1)), for every polynomial in $\mathbb{F}_q[t]$, we can divide the polynomial by $t^q - t$ to get an equivalent (induces the same function) polynomial in $\mathbb{F}_q[t]$ with degree $\leq q-1$, say $c_0 + c_1 t + \cdots + c_{q-1}t^{q-1}$, where $c_i \in \mathbb{F}_q[t]$ for all $i = 0, \ldots, q-1$. Now we have a map

$$\{f \in \mathbb{F}_q[t] | \deg(f) \leq q-1\} \to \mathbb{F}_q^{\mathbb{F}_q}$$

$$f \mapsto (c_0, \ldots, c_{q-1})$$

This is a ring homomorphism, and both sides have cardinality q^q. Further, by the Root-Factor Theorem, if f has degree at most $q-1$ and vanishes at every point of $\mathbb{F}_q$, then it must be the zero polynomial. Thus the map above is injective and must be an isomorphism.

For any finite ring R, E fails to be injective, since $R[t]$ will be infinite and $P(R,R) \subset R^R$ will not be. Another way to see this is using the fact that polynomial functions preserve congruences modulo ideals; if I is an ideal of R and $x, y \in R$ are such that $x \equiv y \pmod{I}$, then also $f(x) \equiv f(y) \pmod{I}$. But if $0 \neq I \subsetneq R$, then the delta function at 0

$$\delta_0(x) = \begin{cases} 1, & x = 0 \\ 0, & x \neq 0 \end{cases}$$

does not have this property. $0 \neq I \subsetneq R \implies 0 \in I, 1 \notin I$, and there is a nonzero element $x \in I$. But then $x \equiv 0 \pmod{I}$ but $\delta_0(0) = 1 \not\equiv 0 = \delta_0(x) \pmod{I}$. So for any finite ring R, $R[t]$ is not isomorphic to $P(R, R)$.

Since $P(R, R) \cong R[t]/\operatorname{Ker} E$, and E is not injective for all finite rings R, it is a useful question to ask for a nice set of generators for $\operatorname{Ker} E$. When R is a field $\mathbb{F}_q$, Chevalley [3] gave a nice set of generators: for $E : R[t] \to R^R$, $\operatorname{Ker} E = \langle t^q - t\rangle$. This generalizes to N variables too; if N is a positive integer, for $E : R[t_1, \ldots, t_N] \to R^{R^N}$, $\operatorname{Ker} E$ is generated by $\{t_i^q - t_i\}_{i=1}^N$.

It is a fact ([5], Theorem 8.35) that any finite ring R has a canonical local decomposition

$$R = \prod_{i=1}^{s} R_i \tag{1.2}$$

where s is the number of maximal ideals in R and R_i is a finite local ring of prime power order. For $1 \leq k \leq s$, let $\pi_k : R \to R_i$ be the kth projection map. Then (1.2) induces the canonical isomorphism

$$R[t] \to \bigoplus_{i=1}^{s} R_i[t], f \mapsto (\pi_1(f), \ldots \pi_s(f)) \tag{1.3}$$

By applying the evaluation map E to (1.3), we obtain a ring isomorphism

$$P(R, R) \cong \prod_{i=1}^{s} P(R_i, R_i)$$

so we are reduced to the local case.

When $(R, \mathfrak{m})$ is a finite local ring, Rogers-Wickham [14] gives an explicit set of generators for the kernel of $E : R[t] \to R^R$. They do this by finding a set of generators for the ideal $Z(\mathfrak{m})$ of $R[t]$ consisting of polynomials f such that $f(x) = 0$ for all $x \in \mathfrak{m}$, then showing that if $\{f_i\}_{i=1}^n$ is a set of generators of $Z(\mathfrak{m})$, then $\{f_i(t^q - t)\}_{i=1}^n$ is a set of generators for $\operatorname{Ker} E$.

When $R = \mathbb{Z}/p^a\mathbb{Z}$, Kempner [8] determined that when $a \leq p$, the kernel of the evaluation map $E : \mathbb{Z}/p^a\mathbb{Z}[t] \to \mathbb{Z}/p^a\mathbb{Z}^{(\mathbb{Z}/p^a\mathbb{Z})}$ is $\langle p, t^p - t\rangle^a$. Then:

$$P(\mathbb{Z}/p^a\mathbb{Z}, \mathbb{Z}/p^a\mathbb{Z}) \cong (\mathbb{Z}/p^a\mathbb{Z}[t])/\langle p, t^p - t\rangle^a. \tag{1.4}$$

From (1.4) we can get:

$$\#(P(\mathbb{Z}/p^a\mathbb{Z},\mathbb{Z}/p^a\mathbb{Z})) = \#((\mathbb{Z}/p^a\mathbb{Z}[t])/\langle p, t^p - t\rangle^a) = p^{p^{\frac{a(a+1)}{2}}}.$$

The result above was reproved by Carlitz [2] and Rosenberg [15]. Kempner also found a (more complicated) formula for $\#P((\mathbb{Z}/p^a\mathbb{Z}),\mathbb{Z}/p^a\mathbb{Z})$ when $a > p$, during which $\#(\mathbb{Z}/p^a\mathbb{Z}^{(\mathbb{Z}/p^a\mathbb{Z})}) < p^{p^{\frac{a(a+1)}{2}}}$ and thus $\langle p, t^p - t\rangle^a \subsetneq \operatorname{Ker} E$. And Bandini [1] showed that when $a = p+1$, $\operatorname{Ker} E = \langle I, (t^p - t)^p - p^{p-1}(t^p - t)\rangle$. For the next results, we define some terminology:

Definition 1.1. For a local ring $(R, \mathfrak{m})$, the **residue field** is the field $R/\mathfrak{m}$, and the **residue cardinality** is $\#(R/\mathfrak{m})$.

Definition 1.2. For a finite local ring $(R, \mathfrak{m})$, the **nilpotency index** is the smallest positive integer a such that $\mathfrak{m}^a = 0$.

For a finite local principal ring R with residue field $R/\mathfrak{m} \cong \mathbb{F}_q$, nilpotency index a, and $a \leq q$, Clark [4] (the result seems to appear for the first time here) found that the kernel of the evaluation map $E : R[t] \to R^R$ is $\langle \pi, (t^q - t)\rangle^a$. So we have:

$$P(R,R) \cong R[t]/\langle \pi, (t^q - t)\rangle^a \tag{1.5}$$

Lemma 1.3. *If $(R, \mathfrak{m} = (\pi))$ is a finite local principal ring with nilpotency index a and residue cardinality q, then*

$$\langle \pi, (t^q - t)\rangle^a \subseteq \operatorname{Ker} E.$$

Proof. Let $\alpha \in R$. Let $\bar{\alpha}$ denote the image of α under the quotient map $R \to R/\mathfrak{m}$. Then since $R/\mathfrak{m} \cong \mathbb{F}_q$, (1.1) $\implies \bar{\alpha}^q - \bar{\alpha} = 0$, and thus, lifting back to R, $\alpha^q - \alpha \in \mathfrak{m} = (\pi)$. So π divides $\alpha^q - \alpha$ for all $\alpha \in R$.

Every element of $\langle \pi, (t^q - t)\rangle^a$ is of the form $f(t) := \pi^i (t^q - t)^{a-i}$ for some $i \in \{0, \dots, a\}$. By the conclusion of the last paragraph, $f(\alpha)$ is divisible by π^a for every $\alpha \in R$. Since $(\pi)^a = \mathfrak{m}^a = 0$, we can conclude that f vanishes identically on R. □

We can also determine the cardinality in this case. Jiang-Peng-Sun-Zhang ([7], Theorem 3) represents every $f \in P(R,R)$ by an element of

$$\mathcal{G} := \prod_{i=1}^{a} (R/\mathfrak{m}^i)^{T_i}$$

where: $\omega : \mathbb{F}_q^\times \to R^\times$ is the Teichmüller character ([4], Appendix Section 2) $T := \omega(\mathbb{F}_q^\times) \cup \{0\}$, and T_i is the image of the T under the quotient map $R \to R/\mathfrak{m}^i$. So we get a surjective map

$$\mathcal{E} : \mathcal{G} \to P(R,R)$$

that is a homomorphism of additive groups. We see that

$$\#\mathcal{G} = \prod_{i=1}^{a} \#(R/\mathfrak{m}^i)^{T_i} = \left(\prod_{i=1}^{a} \#(R/\mathfrak{m}^i)\right)^q$$

so

$$\#P(R,R) \leq \left(\prod_{i=1}^{a} \#(R/\mathfrak{m}^i)\right)^q$$

with equality if and only if $\mathcal{E}$ is injective. ([4], Theorem A.3) shows then that $\mathcal{E}$ is injective when $a \leq q$, so

$$\#(P(R,R)) = \left(\prod_{i=1}^{a} \#(R/\mathfrak{m}^i)\right)^q = (q^q) \cdot (q^2)^q \cdot (q^3)^q \dots (q^a)^q = q^{q^{\frac{a(a+1)}{2}}}$$

whenever $a \leq q$.

Progress has been made for the general case, which includes all values of a and not just $a \leq q$: Maxson-van der Merwe [12] found an upper bound for $\#P(R,R)$ when R is a finite local ring, and Necaev [13] found a formula for $\#P(R,R)$ when R is moreover principal.

1.2 Results Covered

In Chapter 2, we will examine Bandini's [1] proof of Ker E for when $R = \mathbb{Z}/p^a\mathbb{Z}$ and $a = p+1$ and generalize this result, proving that when R is a finite local principal ring with residue cardinality q and nilpotency index a such that $a = q+1$, Ker $E = \langle\langle \pi, t^q - t\rangle^{q+1}, (t^q-t)^q - \pi^{q-1}(t^q-t)\rangle$ (Theorem 2.4).

In Chapter 3, we determine the maximal ideals of $P(R,R)$ for finite local principal rings $(R,\mathfrak{m})$ finding that for each $x \in R$, $m_x = \{f \in P(R,R) | f(x) \in \mathfrak{m}\}$ is a maximal ideal of $P(R,R)$ and that $m_x = m_y$ if and only if x and y represent the same class in $R/\mathfrak{m}$ (Corollary 3.5).

In Chapter 4, we analyze criteria under which every ideal of $P(R,R)$ may be generated by a single element. We find that for a finite local principal ring R, if nilpotency index $a \geq 2$, then $P(R,R)$ contains ideals that are not principal (Theorem 4.2).

In Chapter 5, we use our results from Chapter 4 to find a local decomposition for $P(R,R)$, proving Theorem 5.1, which states that for a finite local principal ring R with residue cardinality q, $P(R,R) \cong \mathcal{R}^q$ for some local ring $\mathcal{R}$. We then look at what $\mathcal{R}$ is when $R = \mathbb{Z}/p^2\mathbb{Z}$ (Proposition 5.2) or when R is finite local principal with nilpotency index $a \leq$ residue cardinality q (Theorem 5.3).

In Chapter 6, we ask many of these same questions for the ring

$$P(R^N, R) = \{\text{polynomial maps } f : R^N \to R\} \subseteq R^{R^N}$$

for when $N > 1$ and highlight some important results from the literature.

Chapter 2

Generalization of Bandini's computation of $\operatorname{Ker}\phi_{p+1}$

As already mentioned, Kempner [8] (and then Carlitz [2] and Rosenberg [15]) found that $\operatorname{Ker} E = \langle p, t^p - t\rangle^a$ when $R = \mathbb{Z}/p^a\mathbb{Z}$ and $a \leq p$. Bandini [1] extended these results to the immediate next case, showing that when $R = \mathbb{Z}/p^a\mathbb{Z}$ and $a = p+1$, if $I := \langle p, t^p - t\rangle$, we have

$$\operatorname{Ker} E = \langle I^{p+1}, (t^p - t)^p - p^{p-1}(t^p - t)\rangle$$

In this section, we generalize Bandini's results to all finite local principal rings.

Lemma 2.1. (Generalization of Bandini's Lemma 1.3)
Let R be a finite local principal ring with maximal ideal $\mathfrak{m} = (\pi)$, residue field $R/\mathfrak{m} \cong \mathbb{F}_q$ and nilpotency index a. Then:

1. For all $\alpha \in R$, $\alpha^q - \alpha$ is an element of $\mathfrak{m}$.
2. For all $\beta \in \mathfrak{m}$, there exists $\alpha \in R$ such that $\alpha^q - \alpha = \beta$. In fact, for every $A \in R$, α can be chosen such that $\alpha \equiv A \pmod{\mathfrak{m}}$.

Proof. To prove (1), we refer to (1.1): the fact that for all $x \in \mathbb{F}_q$, $x^q - x = 0$. Let $\bar{\alpha} \in R/\mathfrak{m}$. Since we know that $R/\mathfrak{m} \cong \mathbb{F}_q$, we have that $\bar{\alpha}^q - \bar{\alpha} = 0$. Then lifting back to $R, \alpha^q - \alpha \in \mathfrak{m}$.

To prove (2), we proceed by induction on a. If $a = 1$, then $\mathfrak{m} = (0)$, and $R = \mathbb{F}_q \cong R/\mathfrak{m}$. For any $\bar{\alpha} \in R/\mathfrak{m} \cong \mathbb{F}_q$, $\bar{\alpha}^q - \bar{\alpha} = 0$. $\bar{\alpha}^q - \bar{\alpha} = 0 \in R/\mathfrak{m} \implies$ lifting back to $R, \alpha^q - \alpha \in \mathfrak{m}$. Moreover we can choose α to be any value $\pmod{\mathfrak{m}}$, since the previous logic holds for all $\bar{\alpha} \in \mathbb{F}_q$.

Now suppose that $a \geq 1$ and that the statement holds for nilpotency index $a-1$. Let $\beta \in \mathfrak{m}$. Then $\beta = \pi k$ for some k. By induction, there exists $\alpha_{a-1} \in R$ such that ${\alpha_{a-1}}^q - \alpha_{a-1} \equiv \pi k \pmod{\pi^{a-1}}$. Then ${\alpha_{a-1}}^q - \alpha_{a-1} = \pi k + l\pi^{a-1}$ for some $l \in R$. Then letting $\alpha_a := \alpha_{a-1} + l\pi^{a-1}$,

$$\alpha_a^q - \alpha_a \equiv$$

$$(\alpha_{a-1} + l\pi^{a-1})^q - (\alpha_{a-1} + l\pi^{a-1}) \equiv$$

$${\alpha_{a-1}}^q + q{\alpha_{a-1}}^{q-1} l\pi^{a-1} - \alpha_{a-1} - l\pi^{a-1} \pmod{\pi^a}.$$

But recall that because $q = 0$ in $R/\mathfrak{m}$, we have $\pi | q$. So in R,

$${\alpha_{a-1}}^q + q{\alpha_{a-1}}^{q-1} l\pi^{a-1} - \alpha_{a-1} - l\pi^{a-1} = {\alpha_{a-1}}^q - \alpha_{a-1} - l\pi^{a-1} = \pi k = \beta \in \mathfrak{m},$$

where the last step holds by the inductive hypothesis. Note also that $\alpha_a = \alpha_{a-1} + l\pi^{a-1} \equiv \alpha_{a-1} \pmod{\pi}$, and by the inductive hypothesis, for any $A \in R$, we can choose α_{a-1} such that $\alpha_{a-1} \equiv A \pmod{\pi}$. $\square$

Lemma 2.2. (Generalization of Bandini's Lemma 1.4)
Let R be a finite local principal ring with maximal ideal $\mathfrak{m} = (\pi)$, residue field $R/\mathfrak{m} \cong \mathbb{F}_q$ and nilpotency index $a \geq q+1$. Let $H_2(t) := (t^q - t)^q - \pi^{q-1}(t^q - t)$. Then

1. For all $\beta \in R$, there exists some $\alpha \in R$ such that $H_2(\alpha) = \beta\pi^{q+1}$.

2. The image of the map $H_2 : R \to R$ is $\mathfrak{m}^{q+1}$.

Proof. Proof of (1): Using Lemma 2.1, take $t_0 \in R$ such that ${t_0}^q - t_0 \equiv \pi\beta \pmod{\pi^{a-q}}$. Now applying Lemma 2.1 once more, take $\alpha \in R$ such that $\alpha^q - \alpha \equiv \pi t_0 \pmod{\pi^{a-q+1}}$. Then:

$$\alpha^q - \alpha = \pi t_0 + \pi^{a-q+1} y \implies$$

$$H_2(\alpha) = (\pi t_0 + \pi^{a-q+1} y)^q - \pi^{q-1}(\pi t_0 + \pi^{a-q+1} y)$$

$$= (\pi t_0)^q + q(\pi t_0)^{q-1}(\pi^{a-q+1} y)^q + \cdots + q(\pi t_0)(\pi^{a-q+1} y)^{q-1} + (\pi^{a-q+1} y)^q - \pi^q t_0 + \pi^a y$$

$$= \pi^q({t_0}^q - t_0)$$

$$= \pi^{q+1}\beta$$

So for all $\beta \in R$, there exists some $\alpha \in R$ such that $H_2(\alpha) = \pi^{q+1}\beta$.

Proof of (2): We can write $H_2(\alpha) = (\alpha^q - \alpha)((\alpha^q - \alpha)^{q-1} - \pi^{q-1})$.

If $\alpha^q - \alpha \in (\pi)^2$, since $((\alpha^q - \alpha)^{q-1} - \pi^{q-1}) \in (\pi^{q-1})$, we're done.

Otherwise, $\alpha^q - \alpha \notin (\pi^2)$. We know $\pi|(\alpha^q - \alpha)$ so $\alpha^q - \alpha = C\pi$ for some $C \in R^\times$. Then $\bar{C} \neq 0$ in $R/\mathfrak{m} \cong \mathbb{F}_q$, so $q|(C^{q-1} - 1)$. Hence $C^{q-1} - 1 \in (\pi)$. Then we have that:

$$\begin{aligned} &(\alpha^q - \alpha)^{q-1} - \pi^{q-1} \\ &\qquad = \pi^{q-1}C^{q-1} - \pi^{q-1} \\ &\qquad = \pi^{q-1}(C^{q-1} - 1) \in (\pi)^q. \end{aligned}$$

So $H_2(\alpha) \in (\pi^{q+1}) = \mathfrak{m}^{q+1}$. □

In [1], Bandini defines the following notation: If $P(X)$ is a non-zero polynomial with integer coefficients and p a fixed prime in $\mathbb{Z}$, we define $d_p(P)$ as the largest integer k such that $P(a) \equiv 0 \pmod{p^k}$ for any integer a.

He then shows that: If I^n is the ideal $(X^p - X, p)^n$ for any positive integer n, and $I^0 = \mathbb{Z}[X]$, when we have a polynomial $Q(X) \in I^n \setminus I^{n+1}$ we can write

$$Q(X) = \sum_{i=0}^{n} Q_i(X)(X^p - X)^i p^{n-i} + R(X) \tag{2.1}$$

with $R(X) \in I^{n+1}$, all coefficients of the $Q_i(X)$ prime with p and $\deg Q_i(X) < p$ for any i.

Then, finally, he proves the following ([1], Proposition 1.5): Let $Q(X) \in I^n \setminus I^{n+1}$. Then $d_p(Q) \geq n+1 \iff H_2(X)$ divides $Q(X) \pmod{I^{n+1}}$ i.e. H_2 divides $Q(X) - R(X)$.

We will generalize this to our context of a finite local principal ring R with residue cardinality q and nilpotency index $a = q+1$. First, we can generalize Bandini's (2.1): When we have a polynomial $Q(t) \in I^a$ ($I := \langle \pi, t^q - t \rangle$), we can write

$$Q(t) = \sum_{i=0}^{a} Q_i(t)(t^q - t)^i \pi^{a-i} + r(t) \tag{2.2}$$

where $r(t) \in I^{a+1}$, all coefficients of the $Q_i(t)$ are units in R and $\deg Q_i(t) < q$ for any i. We can do this in the following way: Let $Q \in I^a$. We take our

$$Q(t) = \sum_{i=0}^{a} G_i(t)(t^q - t)^i \pi^{a-i}$$

where $G_i(t) \in R[t]$ for all $i = 0, \ldots, a$. Using the division algorithm, we rewrite each $G_i(t)$ as $G_i(t) = P_i(t)(t^q - t) + R_i(t)$, where $\deg(R_i(t)) \leq q - 1$. Then we have

$$Q(t) = \sum_{i=0}^{a} P_i(t)(t^q - t)^{i+1} \pi^{a-i} + \sum_{i=0}^{a} R_i(t)(t^q - t)^i \pi^{a-i}.$$

Observe that this first term $\sum_{i=0}^{a} P_i(t)(t^q - t)^{i+1} \pi^{a-i}$ is in I^{a+1}. Now in order to take the second term and rewrite it in a special way, consider the injective group homomorphism

$$\omega : \mathbb{F}_q^{\times} \cup \{0\} \to R^{\times} \cup \{0\}$$

$$0 \neq x \mapsto x^{q^{a-1}}, 0 \mapsto 0$$

known as the Teichmüller character (mentioned on Page 5). If $q : R^{\times} \to \mathbb{F}_q^{\times}$ is the quotient map restricted to the unit groups, then $q \circ \omega = 1_{\mathbb{F}_q^{\times}}$.

For any $x \in R$, we can write $x = \omega(q(x)) + (x - \omega(q(x)))$. Then $\omega(q(x))$ is either 0 or an element of $R^{\times}$, and $x - \omega(q(x)) \in \mathfrak{m}$; so every element x of R may be written $x = A + B$ where A is either 0 or a unit in R, and B is divisible by π.

It is this fact that we will use to rewrite the second term $\sum_{i=0}^{a} R_i(t)(t^q - t)^i \pi^{a-i}$. For each $i = 0, \ldots, a$, we can write

$$R_i(t) = A_i(t) + B_i(t),$$

where $A_i(t)$ has coefficients that are either 0 or units in R, and $B_i(t)$ has coefficients that are divisible by π. Thus

$$\sum_{i=0}^{a} R_i(t)(t^q - t)^i \pi^{a-i} = \sum_{i=0}^{a} A_i(t)(t^q - t)^i \pi^{a-i} + \sum_{i=0}^{a} B_i(t)(t^q - t)^i \pi^{a-i}.$$

But we observe now that term $\sum_{i=0}^{a} B_i(t)(t^q - t)^i \pi^{a-i}$ is in I^{a+1}. So we end up with

$$Q(t) = \left(\sum_{i=0}^{a} P_i(t)(t^q - t)^{i+1} \pi^{a-i} + \sum_{i=0}^{a} B_i(t)(t^q - t)^i \pi^{a-i} \right) + \left(\sum_{i=0}^{a} A_i(t)(t^q - t)^i \pi^{a-i} \right)$$

where the first term $(\sum_{i=0}^{a} P_i(t)(t^q-t)^{i+1}\pi^{a-i} + \sum_{i=0}^{a} B_i(t)(t^q-t)^i\pi^{a-i})$ is in I^{a+1} and the second term $(\sum_{i=0}^{a} A_i(t)(t^q-t)^i\pi^{a-i})$ has coefficients that are either 0 or units in R.

Proposition 2.3. (Partial generalization of Bandini's Proposition 1.5)
Let R be a finite local principal ring with maximal ideal $\mathfrak{m} = (\pi)$, residue field $R/\mathfrak{m} \cong \mathbb{F}_q$, and nilpotency index $a = q+1$. Let $I = \langle \pi, t^q - t\rangle$. Then if $Q(t) \in I^q$ and $Q(t)$ vanishes identically on R, $\exists r(t) \in I^{q+1}$ such that H_2 divides $Q(t) - r(t)$ in $R[t]$.

Proof. Assume $Q(t)$ vanishes identically on R. First, decompose $Q(t)$ in the way described in (2.2):

$$Q(t) = \sum_{i=0}^{q} Q_i(t)(t^q-t)^i\pi^{q-i} + r_1(t),$$

so that $r_1(t) \in I^{q+1}$, all coefficients of the $Q_i(t)$ are units in R, and $\deg Q_i(t) < q$ for all i.

Since $r_1(t) \in I^{q+1}$, $r_1(t)$ vanishes identically on R, and thus so does $Q(t) - r_1(t)$. Then

$$Q(t) - r_1(t) = \sum_{i=0}^{q} Q_i(t)(t^q-t)^i\pi^{q-i} \implies \sum_{i=0}^{q} Q_i(t)(t^q-t)^i\pi^{q-i} \text{ vanishes identically on } R.$$

Let $\beta \in R$. By Lemma 2.1, there is $\alpha \in R$ such that $\alpha^q - \alpha = \pi\beta$. Then: $\forall \beta \in R$, there exists $\alpha \in R$ (which, in particular, we may choose to be anything we wish modulo π) such that:

$$Q(\alpha) = \pi^q\beta^q Q_q(\alpha) + \pi \cdot \pi^{q-1}\beta^{q-1}Q_{q-1}(\alpha) + \cdots + \pi^q Q_0(\alpha) \implies$$
$$Q_0(\alpha) + \sum_{i=1}^{q} Q_i(\alpha)\beta^i \equiv 0 \pmod{\pi}.$$

Now, if x, y are positive integers and $x \equiv y \pmod{q-1}$, then for all $\beta \in R$ (R as above) we have $\beta^x \equiv \beta^y \pmod{\mathfrak{m}}$. This is because $\forall x \in \mathbb{F}_q$, $x^{q-1} = 1 \implies$ for every $x \in \mathbb{F}_q$ and every positive integer n, $x^n = x^{n \pmod{q-1}}$, so x^n depends only on n modulo $q-1$. Define:

$$P_0(t) = Q_0(t)$$
$$P_1(t) = Q_1(t) + Q_q(t)$$
$$P_j(t) = Q_j(t), j = 2, \ldots, q-2$$

Then for all $\alpha, \beta \in R$ we have

$$\sum_{j=0}^{q-1} P_j(\alpha)\beta^j \equiv 0 \pmod{\pi}$$

That is, for all $x, y \in \mathbb{F}_q$,

$$\overline{P}_0(x) + \overline{P}_1(x)y + ... + \overline{P}_{q-1}(x)y^{q-1} = 0 \in \mathbb{F}_q,$$

where $\overline{P}_j$ denotes the reduction of P_j modulo $\mathfrak{m}$.

But then using the fundamental fact that a univariate polynomial over $\mathbb{F}_q$ of degree less than q that evaluates to the zero function must be 0, we find that for each fixed $x \in \mathbb{F}_q$, the polynomial $\overline{P}_0(x) + ... + \overline{P}_{q-1}(x)y^{q-1}$ evaluates to 0 at all $y \in \mathbb{F}_q$, hence $\overline{P}_0(x), ..., \overline{P}_{q-1}(x)$ are all 0. In turn, each $\overline{P}_j$ is a polynomial of degree at most $q-1$, so applying the same fact again we get that $\overline{P}_j = 0$ for all $j = 0, \ldots, q-1$. Thus every coefficient of P_j is divisible by π. So we can write each P_j as $P_j(t) = \pi\tilde{P}_j(t)$, where each $\tilde{P}_j(t)$ is a polynomial in $R[t]$. Note, in particular, that this gives us $Q_0(t) = P_0(t) = 0$, since each Q_j has coefficients that are either zero or units in R.

Using $Q_0(t) = P_0(t) = 0$ and $Q_q(t) = P_1(t) - Q_1(t)$, we have that in $R[t]$,

$$\begin{aligned}
Q(t) - r_1(t) &= \sum_{i=0}^{q} Q_i(t)(t^q - t)^i \pi^{q-i} \\
&= Q_1(t)(t^q - t)\pi^{q-1} + \sum_{j=2}^{q-1} \left(Q_j(t)(t^q - t)^j \pi^{q-j}\right) + Q_q(t)(t^q - t)^q \\
&= Q_1(t)\left((t^q - t)\pi^{q-1} - (t^q - t)^q\right) + \pi\tilde{P}_1(t)(t^q - t)^q + \sum_{j=2}^{q-1} \pi\tilde{P}_j(t)(t^q - t)^j \pi^{q-j} \\
&= Q_1(t) \cdot (-H_2(t)) + \sum_{j=2}^{q-1} \pi\tilde{P}_j(t)(t^q - t)^j \pi^{q-j}
\end{aligned}$$

So if we let $r(t) = r_1(t) + \sum_{j=2}^{q-1} \pi\tilde{P}_j(t)(t^q - t)^j \pi^{q-j} \in I^{q+1}$, $H_2(t)$ divides $Q(t) - r(t)$ in $R[t]$. □

Theorem 2.4. (Generalization of Bandini's Theorem 2.1)
Let R be a finite local principal ring with maximal ideal $\mathfrak{m} = (\pi)$ and residue field $R/\mathfrak{m} \cong \mathbb{F}_q$. Let $\phi_a : R[t] \to R^R$ denote the evaluation map in the case where R has nilpotency index a. Again let $I = \langle \pi, t^q - t \rangle$ and $H_2(t) = (t^q - t)^q - \pi^{q-1}(t^q - t)$. Then $\operatorname{Ker} \phi_{q+1} = (I^{q+1}, H_2)$.

Proof. To see that $(I^{q+1}, H_2) \subset \operatorname{Ker}\phi_{q+1}$, that $H_2 \in \operatorname{Ker}\phi_{q+1}$ follows from (Lemma 2.2, Part 2), and $I^{q+1} \subset \operatorname{Ker}\phi_{q+1}$ by Lemma 1.3.

To prove $\operatorname{Ker}\phi_{q+1} \subset (I^{q+1}, H_2)$, let $Q(t) \in \operatorname{Ker}\phi_{q+1} \subset \operatorname{Ker}\phi_q = I^q$. We may apply Proposition 2.3: there exists $r(t) \in I^{q+1}$ such that H_2 divides $Q(t) - r(t)$ in $R[t]$. Thus $Q(t) = r(t) + H_2(t)f(t)$ for some $f(t) \in R[t]$, so $Q(t) \in (I^{q+1}, H_2)$. $\square$

Chapter 3

Maximal ideals of $P(R, R)$

Let R be a finite local ring with maximal ideal $\mathfrak{m}$, nilpotency index a and residue field $R/\mathfrak{m} \cong \mathbb{F}_q$. We may ask: how many maximal ideals does $P(R, R)$ have? What are they?

In the case of a finite field $R = \mathbb{F}_q$, every map $f : \mathbb{F}_q \to \mathbb{F}_q$ can be written as a polynomial in $\mathbb{F}_q[t]$, since E is surjective. In this case, we see that for all $x \in \mathbb{F}_q$,

$$m_x := \{f \in P(\mathbb{F}_q, \mathbb{F}_q) | f(x) = 0\} \tag{3.1}$$

is a maximal ideal of $P(R, R)$, by being the kernel of the homomorphism $P(R, R) \to R$ defined by evaluating at x (which is surjective since E is surjective).

But now suppose that $(R, \mathfrak{m})$ is a finite local ring and $\mathfrak{m} \neq 0$ (that is, R is not a field). In this case, we define for $x \in R$,

$$m_x := \{f \in P(R, R) | f(x) \in \mathfrak{m}\}. \tag{3.2}$$

These ideals m_x are maximal, this time by being the kernel of the surjective homomorphism

$$F_x : P(R, R) \to R \to R/\mathfrak{m},$$

evaluating at x and then taking the canonical quotient map. Notice that when we plug in $\mathfrak{m} = (0)$ to (3.2) we recover our definition from (3.1) for the case where R is a field.

3.1 Are these maximal ideals distinct?

When $R = \mathbb{F}_q$, the maximal ideals m_x as in (3.1) above are distinct: if $\alpha \neq \beta \in \mathbb{F}_q$ then e.g. $f(x) := x - \alpha$ is such that $f \in m_\alpha$ but $f \notin m_\beta$.

When $R \neq \mathbb{F}_q$, in general, the maximal ideals m_x are not distinct. Take, for example: $R = \mathbb{Z}/p^2\mathbb{Z}$. Let $m_0 := \{f | f(0) \in (p)\}$ and let $m_p := f(p) \in (p)\}$. We see that $0 \equiv p \pmod{p} \implies f(0) \equiv f(p) \pmod{p}$, since polynomials preserve congruences. Then $f(0) \in (p) \iff f(p) \in (p)$, and thus $m_0 = m_p$.

In fact, more generally:

Proposition 3.1. If $(R, \mathfrak{m})$ is a finite local ring, if we let $m_x := \{f : f(x) \in \mathfrak{m}\}$, then for all $x_1, x_2 \in R$, $m_{x_1} = m_{x_2} \iff x_1 \equiv x_2 \pmod{\mathfrak{m}}$.

Proof. ($\impliedby$) Suppose $x_1 \bmod \mathfrak{m} = x_2 \bmod \mathfrak{m}$. Then for all $f \in R[t]$, $f(x_1) \bmod \mathfrak{m} = f(x_1 \bmod \mathfrak{m}) = f(x_2 \bmod \mathfrak{m}) = f(x_2) \bmod \mathfrak{m}$.
($\implies$) Suppose $x_1 \bmod \mathfrak{m} \neq x_2 \bmod \mathfrak{m}$. We will show $m_{x_1} \neq m_{x_2}$ (i.e. there exists $f \in R[t]$ such that $f(x_1) \in \mathfrak{m}$ and $f(x_2) \notin \mathfrak{m}$). Take $f(t) := t - x_1$. Then $f(x_1) = 0 \in \mathfrak{m}$ and $f(x_2) \notin \mathfrak{m}$. □

3.2 Are these m_x all the maximal ideals of $P(R, R)$?

More generally, we may ask: if R is a finite ring and $m_1, \ldots, m_r$ are maximal ideals of R, what is a criterion for these to be all of the maximal ideals? Let's first introduce some definitions.

Definition 3.2. For any ring R,

$$\operatorname{nil} R := \{x \in R : x^k = 0 \text{ for some } k\} = \bigcap_{\text{prime } P \lhd R} P$$

where the second equality can be found in ([5], Proposition 4.12).

Definition 3.3. We say an ideal $I \lhd R$ is **nil** if every $x \in I$ is nilpotent and that $I \lhd R$ is **nilpotent** if $I^k = 0$ for some nonnegative integer k.

Proposition 3.4. For a finite local ring $(R, \mathfrak{m})$, if we define $m_x := \{f \in P(R, R) | f(x) \in \mathfrak{m}\}$, then every maximal ideal of $P(R, R)$ is of the form m_x for some $x \in R$.

Proof. Since R is finite and $P(R,R) \subset R^R$, $P(R,R)$ is also finite and hence Noetherian. So all prime ideals in $P(R,R)$ are maximal. Then

$$\operatorname{nil} P(R,R) = \bigcap_{\text{maximal } M \lhd P(R,R)} M$$

A version ([5], Theorem 4.18) of the Chinese Remainder Theorem tells us in particular that the if $m_1, \ldots, m_r$ is a finite set of pairwise comaximal ideals of $P(R,R)$, then the map

$$P(R,R) \to \prod_{m_i \in \operatorname{MaxSpec} P(R,R)} P(R,R)/m_i$$

$$x \mapsto (x + m_i)_{i=1}^{r}$$

is surjective. This means that for any proper subset $S \subsetneq \operatorname{MaxSpec} P(R,R)$, there is an element $x \in P(R,R)$ such that the set $\{I \in \operatorname{MaxSpec} P(R,R) | x \in I\}$ is precisely S.

Thus, if we intersect over a proper subset of $\operatorname{MaxSpec} P(R,R)$, the intersection will strictly contain $\operatorname{nil} P(R,R)$. That is:

$$S \subsetneq \operatorname{MaxSpec} P(R,R) \implies \operatorname{nil} P(R,R) \subsetneq \bigcap_{I \in S} I \tag{3.3}$$

Define the set

$$A := \bigcap_{x \in R} m_x$$

Then

$$A = \bigcap_{x \in R} m_x = \bigcap_{\bar{x} \in \mathbb{F}_q} m_{\bar{x}} = \{\text{polynomials } f : R \to R | f(x) \equiv 0 \pmod{\pi} \forall x \in R\}.$$

Let $f \in A$. Then $(f(x))^a = 0$ for all $x \in R$, and consequently $f^a = 0$. We may conclude that the set A is nilpotent, and so $A \subset \operatorname{nil} P(R,R)$. We may conclude then, using (3.3), that the set $\{m_x | x \in R\}$ contains all of the maximal ideals of $P(R,R)$. $\square$

Corollary 3.5. Given a finite local ring $(R, \mathfrak{m})$ with residue field $R/\mathfrak{m} \cong \mathbb{F}_q$, $P(R,R)$ has q maximal ideals

$$m_x = \{f \in P(R,R) | f(x) \in \mathfrak{m}\}, x \in R,$$

one for each equivalence class in $R/\mathfrak{m}$.

Chapter 4

Criteria for $P(R, R)$ to be a Principal Ideal Ring

Let R be a finite local principal ring with unique maximal ideal $\mathfrak{m} = (\pi)$, residue field $R/\mathfrak{m} \cong \mathbb{F}_q$, and nilpotency index a. We may then ask: when is every ideal of $P(R, R)$ principal?

Definition 4.1. We call a ring A a **principal ideal ring (PIR)** if every ideal of A is principal.

For the finite field case $R = \mathbb{F}_q$, $P(R, R)$ is, in particular, a principal ideal domain (PID), because $P(\mathbb{F}_q, \mathbb{F}_q) = {\mathbb{F}_q}^{\mathbb{F}_q} \cong {\mathbb{F}_q}^q$ and a finite product of PIDs is a PIR.

We claim that when R is not a field, $P(R, R)$ is no longer a principal ideal ring. To show this, it is sufficient to find an ideal of I of $P(R, R)$ that is not principal.

For a maximal ideal I in $P(R, R)$, if I is principal, then I/I^2 is 1-dimensional as a $R/\mathfrak{m}$-vector space [11]. Thus in order to achieve the above, we will take a maximal ideal I (using our results from Chapter 3) and show that the dimension of I/I^2 over $R/\mathfrak{m}$ is greater than 1.

4.1 The Case $R = \mathbb{Z}/p^2\mathbb{Z}$

Let $R = \mathbb{Z}/p^2\mathbb{Z}$. Recalling the definition from 3.2, we have $m_0 = \{f \in P(R, R) : f(0) \in (p^2)\}$. Observe that

$$m_0^2 \subsetneq \{f \in P(R, R) : f(0) \in (p^2)^2 = (0)\}.$$

Take, for example, $f(t) = t$. We have that $f(0) = 0 \in (0) = (p^2)^2$, but $f(t)$ cannot be written $f = gh$ such that g, h have constant terms in (p^2), so $f(t) = t \notin m_0^2$. This is equivalent to showing the dimension of m_0/m_0^2 over $\mathbb{F}_q$ is > 1. We conclude that when $R = \mathbb{Z}/p^2\mathbb{Z}$, $P(R,R)$ is *not* a principal ideal ring.

4.2 The General Case

We note that for the case of a finite principal local ring R, if nilpotency index $a = 1$, then R is a field and our question is answered: $P(R,R) = \mathbb{F}_q^q$ is a finite principal ring.

Theorem 4.2. Let R be a finite local principal ring with unique maximal ideal $\mathfrak{m} = (\pi)$, residue field $R/\mathfrak{m} \cong \mathbb{F}_q$, and nilpotency index a. Then $P(R,R)$ is not a principal ideal ring whenever $a \geq 2$.

Proof. The elements t and π both lie in the maximal ideal $m_0 \subseteq P(R,R)$. We should show that t and π give $\mathbb{F}_q$-linearly independent elements in m_0/m_0^2. Because every element of $P(R,R)/m_0 \cong \mathbb{F}_q$ is represented by a constant function (because the residue field of R is also $\mathbb{F}_q$), it is enough to show that if $a_1, a_2 \in R$ are such that $a_1 t + a_2 \pi \in m_0^2$, then both a_1 and a_2 lie in m_0 :

In general, if I is generated by $\langle x_1, ..., x_n \rangle$ then I^2 is generated by $\langle x_i x_j | 1 \leq j \leq n \rangle$. We know that m_0 is generated by t and π: every polynomial function f such that $f(0)$ lies in $\mathfrak{m}$ can be written as a multiple of t plus a constant polynomial, and the fact that $f(0)$ lies in $\mathfrak{m}$ means that the constant lies in $\mathfrak{m}$ and thus is a multiple of π. So m_0^2 is generated by $t^2, \pi t$, and π^2. Thus our assumption is that there are polynomials f_1, f_2, f_3 such that

$$a_1 t + a_2 \pi \equiv f_1 \cdot t^2 + f_2 \cdot t \cdot \pi \cdot + f_3 \cdot \pi^2,$$

where $\equiv$ means equal as polynomial functions: i.e., plugging in each x in R gives an equality.

Evaluating at $x = 0$ gives $a_2 \cdot \pi = \pi^2 \cdot f_3(0) \in R$, so π divides a_2, as desired. Evaluating at $x = \pi$ and reducing modulo π^2, we get $a_1 \cdot \pi = 0 \in (R/\pi^2)$, so π divides a_1, as desired. Thus $\dim(m_0/m_0^2) > 1$, so even in the general case, $P(R,R)$ is never a principal ideal ring.

Note that we are also using that every element of $P(R, R)$ differs from an element of m_0 by a constant function,which is why we can assume that a_1 and a_2 lie in R: this assumption does not change them modulo m_0. $\square$

Chapter 5

Local Decomposition of $P(R,R)$

Let $(R,\mathfrak{m})$ be a finite local ring with nilpotency index a and residue cardinality q. Recall that since $P(R,R)$ is itself a finite ring, and we now know from Chapter 3 that $P(R,R)$ has q maximal ideals, (1.2) gives:

$$P(R,R) \cong \prod_{i=1}^{q} R_i$$

where each R_i is a finite local ring.

Theorem 5.1. Let R be a finite local principal ring with residue cardinality q. Then

$$P(R,R) \cong \prod_{i=1}^{q} \mathcal{R},$$

for some local ring $\mathcal{R}$ and so $P(R,R) \cong \mathcal{R}^q$. That is, $R_i = \mathcal{R}$ for all $i = 1,\dots,q$. (We call this $\mathcal{R}$ the "isotypic ring.")

Proof. Suppose $P(R,R)$ has distinct maximal ideals $m_1,\dots,m_q$ (as defined in (3.2)). Because $P(R,R)$ is Artinian, $P(R,R)$ satisfies the descending chain condition. That is, there is no infinite sequence of ideals $\{A_i\}$ such that $A_{i+1} \subsetneq A_i$ for all $i \in \mathbb{Z}^+$ ([5], p.140). Then the chain $m_i \supset m_i^2 \supset m_i^3 \supset \dots$ must stabilize, so for $1 \le i \le q$ there is some nonnegative integer l_i such that $m_i^{l_i} = m_i^{l_i+k}$ for all $k \ge 0$. Also, $l_i \ne 0$ because no power of a maximal ideal contains any other maximal ideal.

But now the ideals $m_1^{l_1},...,m_q^{l_q}$ are pairwise comaximal (because their radicals are), so $I := m_1^{l_1} \cdot ... \cdot m_q^{l_q} = m_1^{l_1} \cap ... \cap m_q^{l_q}$. And $I \subset m_i$ for $1 \le i \le q$, so (the ring is Artinian, hence Noetherian) I is a nilpotent ideal: thus there is some nonnegative integer n such that

$I^n = 0$. On the other hand, if you raise I to any power n, then because $((m_i)^{l_i})^n = m_i^{l_i}$ we find that $I = I^n$. It follows that $I = 0$.

Then the Chinese Remainder Theorem gives an isomorphism:

$$P(R, R) = P(R, R)/I \to \prod_{i=1}^{q} R/m_i^{l_i}$$

so the local factors we are looking for are $P(R, R)/m_i^{l_i}$.

Claim 1: We may take l_x to equal a.

Proof: We have $P(R, R) = \mathcal{R}^q$. So if f is an element of the maximal ideal of $\mathcal{R}$, then $F = (f, 0, ..., 0)$ is a nilpotent element of $P(R, R)$. The elements of $P(R, R)$ that are nilpotent are the elements that map every element of R into (π), in which case the a-th power of the element is 0. So

$$0 = F^a = (f^a, 0, ..., 0),$$

so $f^a = 0$. Thus indeed $m_x^a = m_x^{a+j}$ for all $j \geq 0$, for all $x \in R$. Further, a is the minimum such value: the polynomial $f(t) = \pi(t - x + 1)$ lies in m_x and evaluates at x to π, so the polynomial f^{a-1} lies in $m_x^{a-1} \setminus m_x^a$. Let $\mathcal{R}_x := P(R, R)/m_x^a$. Observe that the ring R embeds in $P(R, R)$ as the subring of constant functions. This induces a map $\phi : R \to P(R, R) \to \mathcal{R}_x$.

Claim 2: ϕ is injective.

Proof: Because $m_0 = \{f : R \to R | f(0) \in \mathfrak{m}\}$, elements of m_0^a evaluate to 0 at 0, and the only constant function for which this is true is 0 itself. So $R \cap m_x^a = (0)$. Thus for all x in R, the map $R \to P(R, R) \to \mathcal{R}_x$ is injective (so each $\mathcal{R}_x$ should be a faithful R-algebra). The embedding of R is injective.

Claim 3: For all $x, y \in R$, the local rings $\mathcal{R}_x$ and $\mathcal{R}_y$ are isomorphic.

Proof: For all x in R, translation by x is an automorphism of the ring $P(R, R)$. For a polynomial function f, define

$$\tau_x(f) : y \to f(x + y)$$

Observe that τ_x is a ring homomorphism whose inverse is τ_{-x}. For x, y in R and k in $\mathbb{Z}^+$ we should have

$$\tau_{y-x} m_x^k = m_y^k$$

Thus τ_{y-x} induces an isomorphism from $\mathcal{R}_x = P(R, R)/m_x^a$ to $\mathcal{R}_y = P(R, R)/m_y^a$. $\square$

5.0.1 The Case $R = \mathbb{Z}/p^2\mathbb{Z}$

Proposition 5.2. Let $R = \mathbb{Z}/p^2\mathbb{Z}$. Then $P(R, R) = \mathcal{R}^p$ where $\mathcal{R} \cong \mathbb{Z}/p^2\mathbb{Z}[pt]$.

Proof. As we mentioned, if $R = \mathbb{Z}/p^2\mathbb{Z}$, then $P(R, R) = \mathcal{R}^p$ where each $\mathcal{R}$ is be a faithful $\mathbb{Z}/p^2\mathbb{Z}$-algebra of order p^3. Our candidate for $\mathcal{R}$ is $\mathbb{Z}/p^2\mathbb{Z}[pt]$.

As a first check, $\mathbb{Z}/p^2\mathbb{Z}[pt]$ has order p^3: if $f \in \mathbb{Z}/p^2\mathbb{Z}[pt]$ then $f(pt) = c_0 + c_1 pt + \cdots + c_n (pt)^n$ with $c_i \in \mathbb{Z}/p^2\mathbb{Z}[pt]$ for all $i = 0, \ldots, n$ but $p^2 = 0$ so we have $f(pt) = c_0 + c_1 pt$, where $c_0 \in \mathbb{Z}/p^2\mathbb{Z}$ and $c_1 \in \{p, p+1, \ldots, p^2 - 1\} \subset \mathbb{Z}/p^2\mathbb{Z}$ so there are $p^2 \cdot p = p^3$ choices for c_0 and c_1.

Claim 1: $S := \mathbb{Z}/p^2\mathbb{Z}[pt] \cong \mathbb{Z}/p^2\mathbb{Z}[x]/(px, x^2)$.

Proof: Consider the homomorphism $\psi : \mathbb{Z}/p^2\mathbb{Z}[x] \to \mathbb{Z}/p^2\mathbb{Z}[pt]$ defined uniquely by $x \mapsto pt$. $\operatorname{Ker}\psi = \{\text{polynomials } P \in \mathbb{Z}/p^2\mathbb{Z}[x] | P(pt) = 0 \text{ in } S\}$, so $(px, x^2) \subset \operatorname{Ker}\psi$. Also, in $\mathbb{Z}/p^2\mathbb{Z}[x]/(px, x^2)$, $x^2 = 0$, so every polynomial can be written as $ax + b$ with $a, b \in \mathbb{Z}/p^2\mathbb{Z}$. There are p^2 choices for b but only p choices $\{0, 1, \ldots, p-1\}$ for a, since in this quotient, $px = 0$. This gives $p \cdot p^2 = p^3$ options for $ax + b$. So $\#(\mathbb{Z}/p^2\mathbb{Z}[x]/(px, x^2)) = p^3$.

Claim 2: Let $\mathcal{R}$ be a local ring of order p^3 that is a faithful $\mathbb{Z}/p^2\mathbb{Z}$-algebra and has nilpotency index 2. Then we claim that $\mathcal{R} \cong S$.

Proof: There is an isomorphism from the additive group of $\mathcal{R}$ to $\mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ that carries 1 to $(1, 0)$; this comes from the classification of finite abelian groups. Let y be the element of $\mathcal{R}$ that maps to $(0, 1)$ under the isomorphism, so $y \notin \mathbb{Z}/p^2\mathbb{Z}$ and y has order p, so $\mathcal{R} = \mathbb{Z}/p^2\mathbb{Z}[y]$.

Since $\mathcal{R}$ has characteristic p^2 and y has order p, y cannot be a unit in $\mathcal{R}$: if $yz = 1$, then $p = pyz = 0 \cdot z = 0$, contradiction. So y must lie in the maximal ideal of $\mathcal{R}$ and thus $y^2 = 0$. Thus we have a surjective $\mathbb{Z}/p^2\mathbb{Z}$-algebra homomorphism

$$\begin{aligned} \mathbb{Z}/p^2\mathbb{Z}[t]/(t^2, pt) &\to \mathcal{R}, \\ t &\mapsto y \end{aligned}$$

Since both rings have order p^3, this is an isomorphism. Thus the properties we wrote for $\mathcal{R}$ indeed characterize it up to isomorphism, so it must be isomorphic to $\mathbb{Z}/p^2\mathbb{Z}[pt]$, although the representation $\mathbb{Z}/p^2\mathbb{Z}[t]/(t^2, pt)$ may be more useful. □

5.0.2 The Case $a \leq q$

Theorem 5.3. Let R be a finite local principal ring with maximal ideal $\mathfrak{m} = (\pi)$, residue field $R/\mathfrak{m} \cong \mathbb{F}_q$, and nilpotency index a. Suppose $a \leq q$. Then

$$R^q \times (R/\pi)^q \times \cdots \times (R/\pi^{a-1})^q \cong P(R, R).$$

Proof. Recall that [4] proves that

$$P(R, R) \cong R[t]/\langle \pi^a, \pi^{a-1}(t^q - t), \ldots, (t^q - t)^a \rangle.$$

We know that $(t^q - t)^a = 0$ in $P(R, R)$ so we can divide any polynomial by this monic degree aq polynomial to get a remainder of degree at most $aq - 1$. Thus

$$\begin{aligned} &\{1, t, \ldots t^{q-1}, \\ &(t^q - t), t(t^q - t), \ldots t^{q-1}(t^q - t), \\ &(t^q - t)^2, t(t^q - t)^2, \ldots, t^{q-1}(t^q - t)^2, \\ &\ldots \\ &(t^q - t)^{a-1}, t(t^q - t)^{a-1}, \ldots, t^{q-1}(t^q - t)^{a-1}\} \end{aligned}$$

is an R-module spanning set for $P(R, R)$ (we have just to choose one monic polynomial for each degree $0, 1, \ldots aq - 1$).

But $(t^q-t)^{a-1}$ is killed by π so we have a surjective R-module homomorphism:

$$\begin{aligned}\Phi : R^{aq} &\to P(R,R)\\ (a_0,\dots,a_{aq-1}) &\mapsto\\ a_0\cdot 1+\dots a_{q-1}\cdot t^{q-1}\\ +a_q\cdot(t^q-t)+a_{q+1}\cdot t(t^q-t)+\dots+a_{2q-1}\cdot t^{q-1}(t^q-t)+\\ \dots\\ +a_{(a-1)q}\cdot(t^q-t)^{a-1}+\dots+a_{aq-1}\cdot t^{q-1}(t^q-t)^{a-1}\end{aligned}$$

Letting $J := (0)^q\times(\pi R)^q\times\dots\times(\pi^{a-1}R)^q$, then $J\subset \operatorname{Ker}\Phi$. So Φ induces a surjective R-module map

$$R^{aq}/J\to P(R,R)$$

But since $R^{aq}/J\cong R^q\times(R/\pi)^q\times\dots\times(R/\pi^{a-1})^q$, we have a surjective map

$$R^q\times(R/\pi)^q\times\dots\times(R/\pi^{a-1})^q\to P(R,R)$$

However,

$$\#P(R,R)=q^{q\frac{a(a+1)}{2}}$$

and

$$\begin{aligned}\#(R^q\times(R/\pi)^q\times\dots\times(R/\pi^{a-1})^q) &= (\#R)^q\cdot(\#R/\pi)^q\cdot\dots\cdot(\#R/\pi^{a-1})^q\\ &= (q^a)^q\cdot(q)^q\cdot(q^2)^q\cdot\times\cdot(q^{(a-1)})^q = q^{q\frac{a(a+1)}{2}}\end{aligned}$$

so this map is an isomorphism, and $R^q\times(R/\pi)^q\times\dots\times(R/\pi^{a-1})^q\cong P(R,R)$. $\square$

Remark. Since we have

$$P(R,R)\cong\mathcal{R}^q,$$

we can deduce that when $a\le q$,

$$\mathcal{R}\cong R\oplus R/(\pi)\oplus\dots\oplus R/(\pi^{a-1}).$$

Kempner's formula [8] shows that $\#P(\mathbb{Z}/p^a\mathbb{Z})) < p^{p^{\frac{a(a+1)}{2}}}$ when $a > p$, and thus in this case the ideal $\operatorname{Ker} E$ properly contains $I = \langle p, t^p - t\rangle^a$. Then when $a > q$, we still have an R-module surjection

$$R \oplus R/(\pi) \oplus \cdots \oplus R/(\pi^{a-1}) \to \mathcal{R}$$

since the argument we used for the surjectivity did not use $a \leq q$; we used only that the elements $\pi^{a-i}(t^q - t)^i$ all lie in $\operatorname{Ker} E$, which still holds when $a > q$. But this map is no longer an isomorphism. Why is this? Define, for $1 \leq n \leq \#R$,

$$\alpha(n) := \sum_{i=1}^{a} \left\lfloor \frac{n}{q^i} \right\rfloor \tag{5.1}$$

and for $1 \leq i \leq q$,

$$\beta(i) := \text{ the least } n \text{ such that } \alpha(n) \geq i. \tag{5.2}$$

When $a > q$, Necaev's result [13] says that

$$\#P(R, R) = q^{\sum_{i=1}^{a} \beta(i)}$$

One can show that for all $1 \leq i \leq q$, $\beta(i) = qi$, so when $a > q$,

$$\#P(R, R) > q^{\sum_{i=1}^{q} \beta(i)} = q^{q(\sum_{i=1}^{a} i)} = q^{q\frac{a(a+1)}{2}}$$

So $\#P(R, R) \neq \#(R \oplus R/(\pi) \oplus \cdots \oplus R/(\pi^{a-1}))^q$, meaning we cannot have an isomorphism.

Remark. One can compute that for a finite local principal ring $(R, \mathfrak{m})$ with nilpotency index $a = 2$ and residue field $R/\mathfrak{m} \cong \mathbb{F}_q$, the dimension $\dim(m_0/m_0^2)$ (which we looked at in Chapter 4) is equal to 2. Though it is not true in general that $m_0^2 = 0$, we may pass to the local ring. That is, inside of $(\mathcal{R}, m_0), m_0^2 = 0$. Then

$$\#P(R, R) = q^{3q} = (q^3)^q = \#(\mathcal{R})^q \implies \#R = q^3$$

and so

$$\#(m_0) = \frac{\#(\mathcal{R})}{q} = \frac{q^3}{q} = q^2 = (\#(\mathbb{F}_q))^2$$

So the dimension over $\mathbb{F}_q$ of the local version of m_0 is 2, but localization leaves this dimension unchanged, meaning $\dim(m_0/m_0^2) = 2$.

In fact, we can compute $\dim(m_0/m_0^2)$ for any nilpotency index a. As mentioned in Chapter 4, m_0 is generated by π and t. Since m_0 can be generated by two elements, certainly m_0/m_0^2 can be generated by 2 elements, so $\dim(m_0/m_0^2) \leq 2$. But from Theorem 4.2, we found $\dim(m_0/m_0^2) > 1$. So in general, $\dim(m_0/m_0^2) = 2$.

Chapter 6

Generalizations to N Variables

Let R be a finite ring. Then we may also examine the ring $P(R^N, R) \subseteq R^{R^N}$ for finite rings R, when $N > 1$. Just as in the $N = 1$ case, we have an analogous evaluation map

$$E : R[t_1, \ldots, t_N] \to R^{R^N}$$

$$f(t_1, \ldots, t_N) \mapsto ((a_1, \ldots, a_N) \mapsto f(a_1, \ldots, a_N))$$

We define $P(R^N, R)$ as the image of $R[t_1, \ldots, t_N]$ under E, and consider two polynomials in $R[t_1, \ldots, t_N]$ equivalent if they induce the same function $R^N \to R$.

We may once again ask the same questions as in the $N = 1$ case: what are the maximal ideals of $P(R^N, R)$? When is every ideal of $P(R^N, R)$ principal? What is the local decomposition of $P(R^N, R)$?

We can immediately reduce to the local case, just as before.

6.0.1 Maximal ideals of $P(R^N, R)$

Let $(R, \mathfrak{m})$ be a finite local ring with nilpotency index a and $R/\mathfrak{m} \cong \mathbb{F}_q$. We can ask: what are the maximal ideals of $P(R^N, R)$? In this case, we define (analogously to the $N = 1$ case), for all $(a_1, \ldots, a_N) \in R^N$:

$$m_{(a_1,\ldots,a_N)} := \{f \in P(R^N, R) | f(a_1, \ldots, a_N) \in \mathfrak{m}\}. \tag{6.1}$$

These ideals $m_{(a_1,\ldots,a_N)}$ are maximal, again by being the kernel of the surjective homomorphism

$$F_{(a_1,\ldots,a_N)} : P(R^N, R) \to R \to R/\mathfrak{m},$$

evaluating at $(a_1, \ldots, a_N)$ and then taking the canonical quotient map.

Are these maximal ideals distinct?

Recall that for the case $N = 1$ we proved that if $(R, \mathfrak{m})$ is a finite local ring, if we let $m_x := \{f : f(x) \in \mathfrak{m}\}$, then for all $x_1, x_2 \in R$, $m_{x_1} = m_{x_2} \iff x_1 \equiv x_2 \bmod \pmod{\mathfrak{m}}$. We claim the same is true for all $N \geq 1$, and the proof is analogous to the $N = 1$ case:

Lemma 6.1. If $(R, \mathfrak{m})$ is a finite local ring, if we let $m_{(a_1,\ldots,a_N)} := \{f \in P(R^N, R) | f(a_1, \ldots, a_N) \in \mathfrak{m}\}$, then for all $(a_1, \ldots, a_N)$ and $(b_1, \ldots, b_N) \in R$, $m_{(a_1,\ldots,a_N)} = m_{(b_1,\ldots,b_N)} \iff (a_1, \ldots, a_N) \equiv (b_1, \ldots, b_N) \pmod{\mathfrak{m}}$.

Proof. ($\Longleftarrow$) Suppose $(a_1, \ldots, a_N) \pmod{\mathfrak{m}} = (b_1, \ldots, b_N) \pmod{\mathfrak{m}}$. Then for all $f \in R[t_1, \ldots, t_N]$, $f(a_1, \ldots, a_N) \pmod{\mathfrak{m}} = f((a_1, \ldots, a_N) \pmod{\mathfrak{m}})$ (polynomials preserve congruences) $= f((b_1, \ldots, b_N) \pmod{\mathfrak{m}}) = f(b_1, \ldots, b_N) \pmod{\mathfrak{m}}$.

($\Longrightarrow$) Suppose $(a_1, \ldots, a_N) \pmod{\mathfrak{m}} \neq (b_1, \ldots, b_N) \pmod{\mathfrak{m}}$. We will show $m_{(a_1,\ldots,a_N)} \neq m_{(b_1,\ldots,b_N)}$ by showing there exists $f \in R[t_1, \ldots, t_N]$ such that $f((a_1, \ldots, a_N)) \in \mathfrak{m}$ and $f((b_1, \ldots, b_N)) \notin \mathfrak{m}$).

By hypothesis, for some $r \in \{1, \ldots, N\}$, $a_r \pmod{\mathfrak{m}} \neq b_r \pmod{\mathfrak{m}}$. Take $f(t_1, \ldots, t_N) := t_r - a_r$. Then $f(a_1, \ldots, a_N) = 0 \in \mathfrak{m}$ and $f(b_1, \ldots, b_N) \notin \mathfrak{m}$. □

Are these all of the maximal ideals of $P(R^N, R)$?

Yes, by a proof analogous to the result for $N = 1$:

Proposition 6.2. If we define

$$m_{(a_1,\ldots,a_N)} := \{f \in P(R^N, R) | f(a_1, \ldots, a_N) \in \mathfrak{m}\} \tag{6.2}$$

then every maximal ideal of $P(R^N, R)$ is of the form $m_{(a_1,\ldots,a_N)}$ for some $(a_1, \ldots, a_N) \in R^N$.

Proof. Since R is finite and $P(R^N, R) \subset R^{R^N}$, $P(R^N, R)$ is also finite and hence Noetherian. So all prime ideals in $P(R^N, R)$ are maximal. Then

$$\operatorname{nil} P(R^N, R) = \bigcap_{\text{maximal } M \lhd P(R^N,R)} M$$

A version ([5], Theorem 4.18) of the Chinese Remainder Theorem tells us that if $m_1, \ldots, m_r$ is a finite set of pairwise comaximal ideals of $P(R^N, R)$, then the map

$$P(R^N, R) \to \prod_{m_i \in \operatorname{MaxSpec} P(R^N,R)} P(R^N, R)/m_i$$
$$x \mapsto (x + m_i)_{i=1}^r$$

is surjective. This means that for any proper subset $S \subsetneq \operatorname{MaxSpec} P(R^N, R)$, there is an element $x \in P(R^N, R)$ such that the set $\{I \in \operatorname{MaxSpec} P(R^N, R) | x \in I\}$ is precisely S. Thus, if we intersect over a proper subset of $\operatorname{MaxSpec} P(R^N, R)$, the intersection will strictly contain $\operatorname{nil} P(R^N, R)$. That is:

$$S \subsetneq \operatorname{MaxSpec} P(R^N, R) \implies \operatorname{nil} P(R^N, R) \subsetneq \bigcap_{I \in S} I \tag{6.3}$$

Define the set

$$A := \bigcap_{(a_1,\ldots,a_N) \in R^N} m_{(a_1,\ldots,a_N)}$$

Then

$$\begin{aligned} A = & \\ & \bigcap_{(a_1,\ldots,a_N) \in R^N} m_{(a_1,\ldots,a_N)} = \\ & \bigcap_{(\overline{a_1,\ldots,a_N}) \in \mathbb{F}_q} m_{(\overline{a_1,\ldots,a_N})} = \\ & \bigcap_{(\bar{a_1},\ldots,\bar{a_N}) \in \mathbb{F}_q} m_{(\bar{a_1},\ldots,\bar{a_N})} = \\ & \{f \in P(R^N, R) | f(a_1, \ldots, a_N) \equiv 0 \pmod{\pi} \forall (a_1, \ldots, a_N) \in R^N\}. \end{aligned}$$

Let $f \in A$. Then $(f(x))^a = 0$ for all $x \in R^N$, and consequently $f^a = 0$. We may conclude that the set A is nilpotent, and so $A \subset \operatorname{nil} P(R^N, R)$. We may conclude then, using (6.3), that the set $\{m_{(a_1,\ldots,a_N)} | (a_1, \ldots, a_N) \in R^N\}$ contains all of the maximal ideals of $P(R^N, R)$. □

Corollary 6.3. Given a finite local ring $(R, \mathfrak{m})$ with residue field $R/\mathfrak{m} \cong \mathbb{F}_q$, $P(R^N, R)$ has q^N maximal ideals

$$m_{(a_1,\ldots,a_N)} = \{f \in P(R^N, R) | f(a_1, \ldots, a_N) \in \mathfrak{m}\}, (a_1, \ldots, a_N) \in R^N,$$

one for each equivalence class in $(R/\mathfrak{m})^N$.

6.1 Computing $\#P(R^N, R)$

For a finite local principal ring R, we know the cardinality of $P(R, R)$ in many cases. How does the size of $P(R^N, R)$ change when $N > 1$?

The result for the case when R is a field $\mathbb{F}_q$ is as one would expect. Since $\mathbb{F}_q^N$ is again a field, we have $\#P(R^N, R) = q^{q^N}$.

Kempner [9] found the formula for $\#P((\mathbb{Z}/p^a\mathbb{Z})^N, \mathbb{Z}/p^a\mathbb{Z})$. Specker-Hungerbühler-Wasem reproved this in [16], giving the formula

$$\#P((\mathbb{Z}/p^a\mathbb{Z})^N, \mathbb{Z}/p^a\mathbb{Z}) = \prod_{\mathbf{k}\in\mathbb{N}_0^d, e_p(\mathbf{k})<m} p^{m-e_p(\mathbf{k})}$$

where for $\mathbf{k} = (k_1, \ldots, k_d) \in \mathbb{N}^d$ and $\mathbf{x} = (x_1, \ldots, x_d) \in \mathbb{N}^d$ we let

$$\mathbf{x}^{\mathbf{k}} := \prod_{i=1}^{d} {x_i}^{k_i} \;,\; \mathbf{k!} := \prod_{i=1}^{d} k_i! \;,\text{ and } e_p(\mathbf{k}) := \max\{\mathbf{x} \in \mathbb{N}^k | p^{\mathbf{x}} | \mathbf{k!}\}.$$

Li-Sha [10] gives a formula for $\#P(R^N, R)$ for all finite principal rings R. When R is local, it reduces to the following:

Theorem 6.4. (Li-Sha) Let R be a finite, local principal ring with residue cardinality q and nilpotency index a. Then

$$\#P(R^N, R) = q^{\sum(a-\sum_{i=1}^{N}\alpha(k_i))},$$

where $\alpha(n) = \sum_{i=1}^{a} \lfloor \frac{n}{q^i} \rfloor$ (note that this is the same α we defined in Equation 5.1) and the outer sum ranges over N-tuples of non-negative integers $(k_1, ..., k_N)$ such that $\alpha(k_1) + ... + \alpha(k_N) < a$.

6.2 Criteria for $P(R^N, R)$ to be a Principal Ideal Ring

For a finite local principal ring $(R, \mathfrak{m} = (\pi))$, we can again ask: when are all ideals of $P(R^N, R)$ principal? An important observation is that we may think of the 1-variable polynomial ring

$R[t]$ as a quotient of the N-variable polynomial ring $R[t_1, \ldots, t_N]$. We let Φ denote the projection map $R[t_1, \ldots, t_N] \to R[t_1, \ldots, t_N]/\langle t_2, \ldots, t_N \rangle \cong R[t]$, and let $\tilde{\Phi}$ denote the map induced on $P(R, R)$ by Φ ($\tilde{\Phi}(f(t_1, \ldots, t_N)) = f(t, 0, \ldots, 0)$). Then we have the following diagram:

$$\begin{tikzcd} R[t_1, \ldots, t_N] \arrow[r, "\Phi"'] \arrow[d, "E"'] & R[t] \arrow[d, "E"'] \\ P(R^N, R) \arrow[r, "\tilde{\Phi}"'] & P(R, R) \end{tikzcd}$$

$\tilde{\Phi}$ is a ring homomorphism, so we must have that if an ideal I of $P(R^N, R)$ is principal, $\tilde{\Phi}_*(I) := \langle \tilde{\Phi}(f) | f \in I \rangle$ is principal. But $\tilde{\Phi}$ is a quotient map, so $\tilde{\Phi}_*(I) = \tilde{\Phi}(I)$.

Then we immediately have that there are ideals in $P(R^N, R)$ that are not principal. Take, for example, $m_{(0,\ldots,0)} \subseteq P(R^N, R)$ as in (6.2). We have that

$$\tilde{\Phi}(m_{(0,\ldots,0)}) = m_0,$$

where m_0 is as in (3.2). We showed that m_0 is not principal in $P(R, R)$, so $m_{(0,\ldots,0)}$ is not principal in $P(R^N, R)$.

Remark. Just as in the $N = 1$ case, we can compute bounds for the dimension of m_0/m_0^2. In N variables, the analogous upper bound would come from the fact that the natural set of generators for $m_{(0,\ldots,0)}$ is $(t_1, ..., t_N, \pi)$, so we get that the dimension is at most $N + 1$.

6.3 Local Decomposition of $P(R^N, R)$

Let $(R, \mathfrak{m})$ be a finite local ring with nilpotency index a and residue cardinality q. Since $P(R^N, R)$ is itself a finite ring, and we showed that $P(R^N, R)$ has q^N maximal ideals, (1.2) again gives

$$P(R^N, R) \cong \prod_{i=1}^{q^N} R_i$$

where each R_i is a finite local ring.

Theorem 6.5. If R is a finite local ring with residue cardinality q, then $P(R^N, R) \cong \mathcal{R}^{q^N}$ for some finite local ring $\mathcal{R}$.

Proof. Suppose $P(R^N, R)$ has distinct maximal ideals $m_1, \ldots, m_{q^N}$ (recall that these maximal ideals correspond to the ideals $m_{(a_1,\ldots,a_N)}, (a_1, \ldots, a_N) \in R^N$, with notation matching that of (6.2)).

Because $P(R^N, R)$ is Artinian, for $1 \leq i \leq q^N$ there is some l_i such that $m_i^{l_i} = m_i^{l_i+k}$ for all $k \geq 0$. Also, $l_i \neq 0$ because no power of a maximal ideal contains any other maximal ideal.

But now the ideals $m_1^{l_1}, ..., m_r^{l_{q^N}}$ are pairwise comaximal (because their radicals are), so $I := m_1^{l_1} \cdot ... \cdot m_1^{l_{q^N}} = m_1^{l_1} \cap ... \cap m_1^{l_{q^N}}$. And $I \subset m_i$ for $1 \leq i \leq q^N$, so (the ring is Artinian, hence Noetherian) I is a nilpotent ideal: thus there is some n such that $I^n = 0$. On the other hand, if you raise I to any power n, then because $((m_i)^{l_i})^n = m_i^{l_i}$ we find that $I = I^n$. It follows that $I = 0$.

Then the Chinese Remainder Theorem gives an isomorphism:

$$P(R^N, R) = P(R^N, R)/I \to \prod_{i=1}^{q^N} R/m_i^{l_i}$$

so the local factors we are looking for are $P(R^N, R)/m_i^{l_i}$.

Claim 1: We may take l_i to equal a.

Proof: We have $P(R^N, R) = \mathcal{R}^{q^N}$. So if f is an element of the maximal ideal of $\mathcal{R}$, then $F = (f, 0, ..., 0)$ is a nilpotent element of $P(R^N, R)$. The elements of $P(R^N, R)$ that are nilpotent are the elements that map every element of R into (π), in which case the a-th power of the element is 0. So

$$0 = F^a = (f^a, 0, ..., 0),$$

so $f^a = 0$. Thus indeed $m^a_{(a_1,\ldots,a_N)} = m^{a+j}_{(a_1,\ldots,a_N)}$ for all $j \geq 0$, for all $x \in R$. Further, a is the minimum such value: if $x = (a_1, \ldots, a_N) \in R^N$, the polynomial $f(t_1, \ldots, t_N) = \pi((t_1 - a_1) \ldots (t_N - a_N) + 1)$ lies in $m_{(a_1,\ldots,a_N)}$ and evaluates at $(a_1, \ldots, a_N)$ to π, so the polynomial f^{a-1} lies in $m^{a-1}_{(a_1,\ldots,a_N)} \backslash m^a_{(a_1,\ldots,a_N)}$. Let $\mathcal{R}_{(a_1,\ldots,a_N)} := P(R^N, R)/m^a_{(a_1,\ldots,a_N)}$. Observe that the ring R embeds in $P(R^N, R)$ as the subring of constant functions. This induces a map $\phi : R \to P(R^N, R) \to \mathcal{R}_{(a_1,\ldots,a_N)}$.

Claim 2: ϕ is injective.

Proof: Because $m_{(0,\ldots,0)} = \{f : R^N \to R | f(0,\ldots,0) \in \mathfrak{m}\}$, elements of $m^a_{(0,\ldots,0)}$ evaluate to 0 at $(0,\ldots,0)$, and the only constant function for which this is true is 0 itself. So $R \cap m^a_{(a_1,\ldots,a_N)} = (0)$. Thus for all $(a_1,\ldots,a_N)$ in R^N, the map $R \to P(R^N, R) \to \mathcal{R}_{(a_1,\ldots,a_N)}$ is injective (so each $\mathcal{R}_{(a_1,\ldots,a_N)}$ should be a faithful R-algebra). The embedding of R is injective.

Claim 3: For all $(a_1,\ldots,a_N), (b_1,\ldots,b_N) \in R^N$, the local rings $\mathcal{R}_{(a_1,\ldots,a_N)}$ and $\mathcal{R}_{(b_1,\ldots,b_N)}$ are isomorphic.

Proof: For all $(a_1,\ldots,a_N)$ in R^N, translation by $(a_1,\ldots,a_N)$ is an automorphism of the ring $P(R^N, R)$. For a polynomial function f, define

$$\tau_{(a_1,\ldots,a_N)}(f) : (b_1,\ldots,b_N) \to f((a_1,\ldots,a_N) + (b_1,\ldots,b_N))$$

Observe that $\tau_{(a_1,\ldots,a_N)}$ is a ring homomorphism whose inverse is $\tau_{-(a_1,\ldots,a_N)}$. For $(a_1,\ldots,a_N), (b_1,\ldots,b_N)$ in R^N and l in $\mathbb{Z}^+$ we should have

$$\tau_{y-(a_1,\ldots,a_N)} m^l_{(a_1,\ldots,a_N)} = m^l_{(b_1,\ldots,b_N)}$$

Thus $\tau_{(b_1,\ldots,b_N)-(a_1,\ldots,a_N)}$ induces an isomorphism from $\mathcal{R}_{(a_1,\ldots,a_N)} = P(R^N, R)/m^a_{(a_1,\ldots,a_N)}$ to $\mathcal{R}_{(b_1,\ldots,b_N)} = P(R^N, R)/m^a_{(b_1,\ldots,b_N)}$. $\square$

Chapter 7

Open Problems

1. Can we extend Li-Sha's results [10] to give the R-module structure of $P(R^N, R)$ for any finite local principal ring R? Note that when $N = 1$ this generalizes the work of Necaev [13].

2. Extend Rosenberg's work [15] from $\mathbb{Z}$- algebras to R-algebras for a finite local principal ring R.

3. For a ring R, define $\mu_*(R) := \sup\{\mu(I) | I \lhd R\}$, where $\mu(I)$ = the least number of generators of I. When $(R, \mathfrak{m})$ is a finite local principal ring with nilpotency index a, it turns out that $\mu_*(R[t]) = a$ ([6], Corollary 4.6).

   (a) What is $\mu_*(P(R^N, R))$? When $N = 1$, for example, we found in Chapter 3 that $\mu(m_x) = 2$, so $\mu_*(P(R, R)) \geq 2$. But what about other cases?

   (b) If S surjects onto T, then $\mu_*(T) \leq \mu_*(S)$, so since $P(R, R)$ is a quotient of $R[t]$, $\mu_*(P(R, R)) \leq \mu_*(R[t]) = a$. Is there ever equality? When $N \geq 2$, $\mu_*(R[t_1, \ldots, t_N]) = \infty$. But $\mu_*(P(R^N, R)) < \infty$ so in this case the answer is no, but what about when $N = 1$?

4. Let R_1, R_2 be finite local principal rings. If $P(R_1, R_1) \cong P(R_2, R_2)$, does that imply $R_1 \cong R_2$? If R is a finite local principal ring, then from the isomorphism class of $P(R, R)$ we can determine three invariants of R:

   (a) The residue cardinality q, since q is the residue cardinality of the localization of $P(R, R)$ at any maximal ideal.

(b) The nilpotency index a, since a is the nilpotency index of the localization of $P(R,R)$ at any maximal ideal. (Note that (1) and (2) give that the order $\#R = q^a$ is also an invariant).

(c) The characteristic (this is the least positive integer n such that $n \cdot 1 = 0 \in R$), since we have ring inclusions

$$R \subseteq P(R,R) \subseteq R^{\#R}$$

and the characteristics of R and $R^{\#R}$ are the same.

We observe that since the characteristic of R is also the unique positive integer n such that R is a faithful $\mathbb{Z}/n\mathbb{Z}$-algebra, in particular, $\mathbb{Z}/n\mathbb{Z}$ is a subring of R. Applying Lagrange's Theorem to the additive groups, we get that $n|\#R = q^a$ (but q must be a power of p; say $q = p^r$ for a positive integer r) so $q^a = p^{ra}$, so n is also a power of p, say $n = p^b$. Moreover, because p lies in the maximal ideal of R, we have $p^a = 0 \in R$ and thus $b \leq a$.

Then to a finite local principal ring we have associated four parameters: a prime number p that is the residue characteristic and positive integers r and $b \leq a$. In what cases do these invariants completely determine our ring R? Are there any other invariants?

5. Are there any cases other than $a = 1$ or $R = \mathbb{Z}/p^2\mathbb{Z}$ where $\mathcal{R}$ and $P(R,R)$ can be determined explicitly?

6. For a finite local principal ring $(R, \mathfrak{m} = (\pi))$ with nilpotency index a and residue cardinality q such that $a = q+1$, again letting $H_2(t) = (t^q - t)^q - \pi^{q-1}(t^q - t)$, what is the structure of $R[t]/\langle H_2 \rangle$?

Bibliography

[1] A. Bandini. Functions $f : \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$ Induced by Polynomials of $\mathbb{Z}[x]$. *Annali di Matematica Pura ed Applicata*, March 2002.

[2] L. Carlitz. Functions and polynomials $\pmod{p^n}$. *Acta Arithmetica*, 9(1):67–78, 1964.

[3] C. Chevalley. Démonstration d'une hypothèse de M. Artin. Abh. Math. Sem. Univ. Hamburg, 1935.

[4] P. L. Clark. Around the Chevalley–Warning Theorem (monograph manuscript).

[5] P. L. Clark. Commutative Algebra. http://alpha.math.uga.edu/ pete/integral.pdf, 2015.

[6] P.L. Clark. A note on rings of finite rank. *Communications in Algebra*, 46(10):4223–4232, 2018.

[7] J.J. Jiang, G.H. Peng, Q. Sun, and Q.F. Zhang. On polynomial functions over finite commutative rings. Acta Math. Sin. (Engl. Ser.), 2006.

[8] A. J. Kempner. Polynomials and Their Residue Systems. *Transactions of the American Mathematical Society*, 22(2):240–266, 1921.

[9] A. J. Kempner. Polynomials of Several Variables and Their Residue Systems. https://doi.org/10.2307/1989105, 1925.

[10] X. Li and M. Sha. Polynomial functions in the residue class rings of dedekind domains. *International Journal of Number Theory*, 15(07):1473–1486, July 2019. ISSN 1793-7310.

[11] H. Matsumura. *Commutative Ring Theory.* Cambridge University Press, January 1987. ISBN 9781139171762.

[12] C.J. Maxson and A.B. van der Merwe. Functions and polynomials over finite commutative rings, 2001.

[13] A.A. Necaev. Polynomial transformations of finite commutative local rings of principal ideals. Mathematical Notes of the Academy of Sciences of the USSR, 1980.

[14] M. Rogers and C. Wickham. Polynomials inducing the zero function on chain rings. 17, 2018.

[15] I.G. Rosenberg. Polynomial functions over finite rings. Glasnik Mat. Ser., 1975.

[16] E. Specker, N. Hungerbühler, and M. Wasem. The ring of polyfunctions over z/nz. *Communications in Algebra*, 51(1):116–134, July 2022. ISSN 1532-4125.