1-1-2017

Polynomials inducing the zero function on local rings

Mark W. Rogers
Missouri State University

Cameron Wickham
Missouri State University

Recommended Citation

Rogers, Mark W., and Cameron Wickham. "Polynomials inducing the zero function on local rings." arXiv preprint arXiv:1607.02482 (2016).

International Electronic Journal of Algebra
Volume 22 (2017) 170-186
DOI: 10.24330/ieja.325942

POLYNOMIALS INDUCING THE ZERO FUNCTION ON LOCAL RINGS

Mark W. Rogers and Cameron Wickham

Received: 21 February 2017; Revised: 15 May 2017
Communicated by A. Çiğdem Özcan

Abstract. For a Noetherian local ring $(R, \mathfrak{m})$ having a finite residue field of cardinality q, we study the connections between the ideal $\mathrm{N}(R)$ of $R[x]$, which is the set of polynomials that vanish on R, and the ideal $\mathrm{N}(\mathfrak{m})$, the polynomials that vanish on $\mathfrak{m}$, using polynomials of the form $\pi(x) = \prod_{i=1}^{q}(x - c_i)$, where $c_1, \ldots, c_q$ is a set of representatives of the residue classes of $\mathfrak{m}$. In particular, when R is Henselian we show that a generating set for $\mathrm{N}(R)$ may be obtained from a generating set for $\mathrm{N}(\mathfrak{m})$ by composing with $\pi(x)$.

Mathematics Subject Classification (2010): 13M10, 13B25, 11C08, 13J15, 13E10, 13F20
Keywords: Finite ring, polynomial function, vanishing polynomial, Artinian ring, null ideal

1. Introduction

One of the surprising facts about finite rings is that a polynomial can be nonzero and yet induce the zero function. An interesting first example is provided by Fermat's Little Theorem: If p is prime, then the nonzero polynomial $x^p - x$ induces the zero function on $\mathbb{Z}_p$. Using this we can build obvious examples, such as $p(x^p - x)$ and $(x^p - x)^2$ on $\mathbb{Z}_{p^2}$, and more surprising examples, such as $(x^p - x)^p - p^{p-1}(x^p - x)$ on $\mathbb{Z}_{p^{p+1}}$; see Corollary 4.5 for more information on these examples. For a ring R, it's easy to see that the set of polynomials in $R[x]$ that induce the zero function on R is an ideal of $R[x]$; we call this the *null ideal* of R, denoted $\mathrm{N}(R)$. The null ideal has been studied, often with particular focus on the rings $R = \mathbb{Z}_{p^n}$, for its connection with integer-valued polynomials and functions induced by polynomials [3,5,10,13] and coding theory [6].

For most of our paper, $(R, \mathfrak{m})$ is a Noetherian local ring; we will see that $\mathrm{N}(R)$ is nonzero only when the residue field $\overline{R} = R/\mathfrak{m}$ is finite, so we focus most of our attention on this case and let $q = |\overline{R}|$. Many authors have studied the problem of finding a generating set for $\mathrm{N}(R)$, most often in the case $R = \mathbb{Z}_{p^n}$ [1,2,3,7,9,10,11]. In this paper, we argue that in many cases, focus should be shifted from $\mathrm{N}(R)$ to the simpler ideal $\mathrm{N}(\mathfrak{m})$, which is the set of polynomials that induce the zero function on $\mathfrak{m}$. The connection between the two is the ideal $\mathrm{N}(R, \mathfrak{m})$, the set of polynomials that take elements of R into $\mathfrak{m}$; it's easy to show that $\mathrm{N}(R, \mathfrak{m}) = (x^q - x, \mathfrak{m})$. Certainly polynomials in $\mathrm{N}(R, \mathfrak{m})$ can be composed with those in $\mathrm{N}(\mathfrak{m})$ to obtain polynomials in $\mathrm{N}(R)$; visually, $\mathrm{N}(\mathfrak{m}) \circ \mathrm{N}(R, \mathfrak{m}) \subseteq \mathrm{N}(R)$. One of the main themes of this paper is to show that in some sense the opposite is true: A generating set for $\mathrm{N}(R)$ can be obtained by composing generators of $\mathrm{N}(R, \mathfrak{m})$ with generators of $\mathrm{N}(\mathfrak{m})$ (see Theorem 4.2).

Example 1.1. *Let $R = \mathbb{Z}_9$, so that $\mathfrak{m} = (3)$ and $\overline{R} \cong \mathbb{Z}_3$. By direct computation or by Theorem 4.4,* $\mathrm{N}(\mathfrak{m}) = (x, \mathfrak{m})^2$. *In Lemma 2.5 we easily find that with $\pi(x) = x^3 - x$, $\mathrm{N}(R, \mathfrak{m}) = (\pi(x), \mathfrak{m}) = (x^3 - x, 3)$; from this, according to Theorem 4.2, we deduce*

$$\mathrm{N}(R) = \mathrm{N}(\mathfrak{m}) \circ \mathrm{N}(R, \mathfrak{m}) = (x^3 - x, 3)^2.$$

This makes it clear that the simpler ideal $\mathrm{N}(\mathfrak{m})$ *controls the structure of the generating set of the more complicated ideal* $\mathrm{N}(R)$.

The polynomial $x^q - x$ has played an important role in the research on null ideals, due primarily to the fact that the image of $x^q - x$ generates $\mathrm{N}(\overline{R})$ and, to a lesser extent, the fact that when R is finite, $x^q - x$ maps R surjectively onto $\mathfrak{m}$; see A. Bandini's paper [1] for applications of surjectivity when $R = \mathbb{Z}_{p^n}$. We generalize the surjectivity result in Corollary 2.11 and apply it in Theorem 3.3 and Proposition 4.1. A secondary theme of this paper is that there is actually a class of polynomials with these properties that can play the role of $x^q - x$; we call these *π-polynomials*, defined to be polynomials of the form $\pi(x) = \prod_{i=1}^{q}(x - c_i)$ where $c_1, \ldots, c_q$ is any set of representatives of the residue classes of $\mathfrak{m}$. As we will see, $x^q - x$ is a π-polynomial when R is Henselian (which holds true in the common case where R is finite). If R is complete, we also provide a computational way of obtaining the factorization of any π-polynomial, such as $x^q - x$ itself. In the case of $x^q - x$, this method is as simple as choosing any element of R and repeatedly taking the qth power; the results converge to a root of $x^q - x$. (See Theorems 2.10, 5.2.)

The ideal $\mathrm{N}(R)$ for $R = \mathbb{Z}_{p^n}$ was studied as early as 1929 by L. E. Dickson [2, Theorem 27]; in that work, the polynomials in $\mathrm{N}(R)$ were referred to as *residual polynomials*. Dickson found a generating set for $\mathrm{N}(\mathbb{Z}_{p^n})$ when $n \leqslant p$. In our notation, he found $\mathrm{N}(R) = (\pi(x), \mathfrak{m})^n$, where $\pi(x) = x^p - x$ and $\mathfrak{m} = pR$. We generalize and recover this work as another application of our Theorem 4.2: We show in Theorem 4.4 and its corollary that if $(R, \mathfrak{m})$ is an Artinian local ring with a principal maximal ideal having index of nilpotency $e \leqslant q$, then $\mathrm{N}(\mathfrak{m}) = (x, \mathfrak{m})^e$, and thus $\mathrm{N}(R) = (\pi(x), \mathfrak{m})^e$ for any π-polynomial. When $e > q$, the situation is more complicated, but we take care of the case $e = q + 1$; the result is related to results on $\mathrm{N}(R)$ for specific rings R ([1, Theorem 2.1] and [7, Theorem II]).

As further indication of the importance of π-polynomials and $\mathrm{N}(\mathfrak{m})$, we provide two additional results. Under suitable conditions, we prove in Proposition 2.7 that $\mathrm{N}(R)$ is the intersection of the principal ideals generated by the π-polynomials, and in Proposition 2.9 we provide a minimal primary decomposition of $\mathrm{N}(R)$ as the intersection of the ideals $\mathrm{N}(c_i + \mathfrak{m})$, where $c_1, \ldots, c_q$ is a set of representatives of the residue classes of $\mathfrak{m}$. Since generators for $\mathrm{N}(c_i + \mathfrak{m})$ may be obtained from generators for $\mathrm{N}(\mathfrak{m})$ by composition with $x - c_i$, this shows that a primary decomposition for $\mathrm{N}(R)$ may be obtained from knowing only a generating set for $\mathrm{N}(\mathfrak{m})$. This result on primary decomposition is a generalization of results from the paper [10] of G. Peruginelli, which was concerned with the ring $R = \mathbb{Z}_{p^n}$.

The remaining theme of our paper is provided in Theorem 3.3, Theorem 3.4, and Corollary 3.5, where we identify conditions under which $\mathrm{N}(R)$ is nonzero, principal, and regular, and the same for $\mathrm{N}(\mathfrak{m})$; these results explain why we often focus our attention on finite rings. The results generalize, have some overlap with, and were inspired by R. Gilmer's paper [4].

2. Null ideals and π-polynomials

We begin with a precise definition of the null ideal of a ring, and we define a class of polynomials that plays an important role in the study of null ideals.

Definition 2.1. Let R be a commutative ring with identity, let S be a subset of R, and let J be an ideal of R. The set $\mathrm{N}(S, J)$ of polynomials in $R[x]$ which map S into J is easily seen to be an ideal of $R[x]$. When the ideal J is omitted, it is assumed to be zero. The focus of this paper is on $\mathrm{N}(R)$, which we call the *null ideal* of R.

Definition 2.2. Suppose the local ring $(R, \mathfrak{m})$ has a finite residue field and let $f(x) \in R[x]$. If $f(x) = \prod_{i=1}^{q}(x - c_i)$ for some set of representatives $c_1, \ldots, c_q$ of the residue classes of $\mathfrak{m}$, then we call the polynomial $f(x)$ a *π-polynomial* for R.

Example 2.3. *We mentioned in the introduction that for $R = \mathbb{Z}_9$, $\mathrm{N}(\mathfrak{m}) = (x, 3)^2$. However, for $R = \mathbb{Z}_8$, $\mathrm{N}(\mathfrak{m}) \supsetneq (x, 2)^3$. In fact, according to Theorem 4.4 and a few brief calculations, $\mathrm{N}(\mathfrak{m}) = (x, 2)^3 + (x^2 - 2x) = (x^2 - 2x, 4x)$. We may then use*

Theorem 4.2 to compose with the π-polynomial $\pi(x) = x^2 - x$ and conclude that $\mathrm{N}(R) = ((x^2 - x)^2 - 2(x^2 - x), 4(x^2 - x))$.

The following basic result is a generalized factor theorem that will be useful in a few proofs. This result appeared in Gilmer's proof of Theorem 4 in [4], albeit restricted to units rather than regular elements. We omit the trivial proof of this result.

Lemma 2.4. *Let R be a commutative ring with identity. If $f(x) \in R[x]$ is a polynomial with roots $c_1, c_2, \ldots, c_n$ such that each difference $c_i - c_j$ $(i \neq j)$ is a regular element, then $(x - c_1)(x - c_2) \cdots (x - c_n)$ divides $f(x)$ in $R[x]$.*

Convention. Throughout this paper, we let R be a local ring with maximal ideal $\mathfrak{m}$; we do not automatically assume that R is Noetherian. Unless otherwise specified, the residue field $R/\mathfrak{m}$ will be denoted by $\overline{R}$. The image in $\overline{R}$ of an element $r \in R$ will be denoted by $\overline{r}$. If the residue field is finite, $c_1, \ldots, c_q$ will denote a set of representatives of the residue classes of $\mathfrak{m}$ and $\pi(x)$ will denote the π-polynomial $\pi(x) = \prod_{i=1}^{q}(x - c_i)$.

The following lemma may be viewed as a generalization of Fermat's Little Theorem; it is well-known, at least in special cases, as remarked by D. J. Lewis in [7]. A simple but important consequence of this lemma is that $\pi(R) \subseteq \mathfrak{m}$. Later in Corollary 2.11 we will show that if R is Henselian, then $\pi(R) = \mathfrak{m}$.

Lemma 2.5. *If $(R, \mathfrak{m})$ is a local ring with finite residue field of cardinality q and $\pi(x)$ is any π-polynomial, then* $\mathrm{N}(R, \mathfrak{m}) = (\pi(x), \mathfrak{m})$.

Proof. Let $f(x) \in \mathrm{N}(R, \mathfrak{m})$; then $\overline{f}(x) \in \mathrm{N}\left(\overline{R}\right)$. By Lemma 2.4, $\overline{f}(x)$ is in the ideal generated by $\overline{\pi}(x)$ in $\overline{R}[x]$; pull this back to $R[x]$ to get $f(x) \in (\pi(x), \mathfrak{m})$.

For the opposite containment, certainly the constant polynomials in $\mathfrak{m}$ are in $\mathrm{N}(R, \mathfrak{m})$. Now suppose $\pi(x) = \prod_{i=1}^{q}(x - c_i)$. Since any element in R is congruent modulo $\mathfrak{m}$ to one of the c_i, the polynomial $\pi(x)$ is in $\mathrm{N}(R, \mathfrak{m})$, as desired. □

Example 2.6. *Let $R = \mathbb{Z}_{(5)}$ ($\mathbb{Z}$ localized at the prime ideal (5)), so that $\mathfrak{m} = (5)$, $\overline{R} = \mathbb{Z}_5$, and $q = 5$. The polynomial $x^q - x$ is not a π-polynomial since it doesn't factor completely over $R \subseteq \mathbb{Q}$: $x^5 - x = x(x-1)(x+1)(x^2+1)$. However, as we shall see in Theorem 2.10, this polynomial is a π-polynomial for the Henselian ring $\hat{R}$ of 5-adic integers. In this case, this is due to the existence of a square root of -1 in $\hat{R}$.*

By Lagrange's Theorem applied to the group of units of $\overline{R}$, it is true that $x^5 - x \in \mathrm{N}(R, \mathfrak{m})$. According to the lemma, we expect $x^5 - x \in (\pi(x), \mathfrak{m})$ for any π-polynomial. In fact, if for example we let $\pi(x) = (x-2)(x+1)x(x-1)(x+2)$, then $x^5 - x = \pi(x) + 5(x^3 - 1) \in (\pi(x), \mathfrak{m})$.

In the next result we show that the polynomials in the null ideal are precisely those polynomials that are multiples of each π-polynomial.

Proposition 2.7. *Let $(R, \mathfrak{m})$ be a local ring with finite residue field $\overline{R}$ of cardinality q. The null ideal of R is the intersection of the principal ideals generated by the π-polynomials. That is, $\mathrm{N}(R) = \bigcap(\pi(x))$, where the intersection is taken over all π-polynomials $\pi(x)$ for R.*

Proof. The fact that any polynomial $f(x) \in \mathrm{N}(R)$ is a multiple of any π-polynomial $\pi(x)$ follows immediately from Lemma 2.4. This shows $\mathrm{N}(R) \subseteq \bigcap(\pi(x))$.

Let $f(x) \in \bigcap(\pi(x))$ and let $r \in R$; we show $f(r) = 0$. We may extend r to a set $r, c_2, \ldots, c_q$ of representatives of the residue classes of $\mathfrak{m}$, and thus the polynomial $\pi(x) = (x-r)(x-c_2)\cdots(x-c_q)$ is a π-polynomial having r as a root. Since $f(x)$ is a multiple of $\pi(x)$, $f(r) = 0$. Thus $f(x) \in \mathrm{N}(R)$. □

In the following result we give a minimal primary decomposition of $\mathrm{N}(R)$ if R is finite. First, we give a simple example:

Example 2.8. *For $R = \mathbb{Z}_9$, as mentioned in the introduction, we have $\mathrm{N}(\mathfrak{m}) = (x, 3)^2 = (x^2, 3x)$, so the proposition below gives the following minimal primary decomposition of $\mathrm{N}(R)$:*

$$((x^3 - x)^2, 3(x^3 - x)) = (x^2, 3x) \cap ((x-1)^2, 3(x-1)) \cap ((x-2)^2, 3(x-2)),$$

where the ideals on the right are primary for the maximal ideals $(x, 3)$, $(x-1, 3)$, and $(x-2, 3)$, respectively.

Proposition 2.9. *Let $(R, \mathfrak{m})$ be a finite local ring with residue field $\overline{R}$ of cardinality q. Let $c_1, \ldots, c_q$ be a set of representatives of the residue classes of $\mathfrak{m}$. Then $\mathrm{N}(R) = \bigcap_{i=1}^{q} \mathrm{N}(c_i + \mathfrak{m})$ is a minimal primary decomposition of $\mathrm{N}(R)$. For each i, the associated prime of $\mathrm{N}(c_i + \mathfrak{m})$ is the maximal ideal $(x - c_i, \mathfrak{m})$.*

Proof. For the minimality of the decomposition, let j be an integer between 1 and q; we show that $\mathrm{N}(R) \subsetneq \bigcap_{i \neq j} \mathrm{N}(c_i + \mathfrak{m})$. Let $h(x) = \prod_{i \neq j}(x - c_i)^e$; then $h(x) \in \bigcap_{i \neq j} \mathrm{N}(c_i + \mathfrak{m})$ since $\mathfrak{m}^e = 0$. To see that $h(x)$ does not induce the zero function, note that $h(c_j) = \prod_{i \neq j}(c_j - c_i)^e$ is a product of units, and is thus nonzero. The proofs of the remaining assertions are straightforward and thus omitted. □

Next we provide an equivalent way to view π-polynomials, provided the ring is Henselian; of course, this holds for the finite local rings in which we are mainly interested. For an example where the two conditions below are not equivalent, see Example 2.6. This theorem is also needed in our proof that π-polynomials map R surjectively onto $\mathfrak{m}$. (A Henselian local ring is a local ring satisfying Hensel's Lemma.)

Theorem 2.10. *Let R be a Henselian local ring with finite residue field $\overline{R}$ of cardinality q. For any polynomial $p(x) \in R[x]$, the following statements are equivalent:*

(i) *The polynomial $p(x)$ is a π-polynomial.*

(ii) *The polynomial $p(x)$ is monic and maps to $x^q - x$ in $\overline{R}[x]$.*

Proof. Let $p(x)$ be any π-polynomial. Since $\overline{R}$ is a field with q elements, by Lagrange's theorem on the group of units of $\overline{R}$, $x^q - x$ induces the zero function on $\overline{R}$. By Lemma 2.4, $\overline{p}(x)$ divides $x^q - x$ in $\overline{R}[x]$. Since these are monic polynomials of the same degree, they are equal.

For the converse, suppose $p(x)$ is any monic polynomial with $\overline{p}(x) = x^q - x$. Let $\overline{R} = \{\overline{d_1}, \ldots, \overline{d_q}\}$; as discussed in the previous paragraph, $x^q - x = \prod_{i=1}^{q}(x - \overline{d_i})$ in $\overline{R}[x]$. By Hensel's Lemma, this factorization of $\overline{p}(x)$ can be pulled back to a factorization in $R[x]$: There exist c_i in R with $\overline{c_i} = \overline{d_i}$ such that $p(x) = \prod_{i=1}^{q}(x - c_i)$. Thus $p(x)$ is a π-polynomial. □

In the following corollary, we improve upon part of Lemma 2.5 by showing that the induced function $\pi\colon R \to \mathfrak{m}$ is actually surjective when R is Henselian. This generalizes Lemma 1.3 of [1], where A. Bandini proved that, for any prime p, $\pi(R) = \mathfrak{m}$ in case $R = \mathbb{Z}_{p^n}$ and $\pi(x) = x^p - x$. We use this corollary in our Theorem 3.3, where we characterize finite rings with principal null ideals, expanding upon Gilmer [4]. It is used again in Proposition 4.1, which is fundamental for our Theorem 4.2, which shows that generators for $\mathrm{N}(R)$ may be obtained by composing generators for $\mathrm{N}(\mathfrak{m})$ with a π-polynomial.

Corollary 2.11. *If $(R, \mathfrak{m})$ is a Henselian local ring with finite residue field $\overline{R}$ of cardinality q, then $\pi(R) = \pi(\mathfrak{c}) = \mathfrak{m}$ for any π-polynomial $\pi(x)$ and any coset $\mathfrak{c}$ of $\mathfrak{m}$.*

Proof. We show that $\pi(\mathfrak{c}) \subseteq \pi(R) \subseteq \mathfrak{m} \subseteq \pi(\mathfrak{c})$. The first containment is clear since $\mathfrak{c} \subseteq R$, and we saw the second containment in Lemma 2.5. For the final containment, let $m \in \mathfrak{m}$. By Theorem 2.10, the polynomial $\pi(x) - m$ is still a π-polynomial, and thus it factors over R: $\pi(x) - m = (x - c_1)(x - c_2) \cdots (x - c_q)$.

This shows that for each i, $\pi(c_i) = m$. Since $c_1, c_2, \ldots, c_q$ is a set of representatives of the residue classes of $\mathfrak{m}$, one of them, say c_j, is in $\mathfrak{c}$. Thus $m = \pi(c_j) \in \pi(\mathfrak{c})$, as desired. □

3. When $\mathrm{N}(R)$ and $\mathrm{N}(\mathfrak{m})$ are nonzero, regular, or principal

In the upcoming Theorems 3.3 and 3.4 we will use the following result from B. R. McDonald. McDonald states and proves the theorem for any finite local ring $(R, \mathfrak{m})$, but the theorem and proof still hold when R is just Artinian. The notation McDonald uses is different from ours but the part we will use is that over an Artinian local ring, any regular polynomial is an associate of a monic polynomial. McDonald writes μf where we would write $\overline{f}$, the image of f in $\overline{R}[x]$.

Theorem 3.1. [8, Theorem XIII.6, p. 259] *Let f be a regular polynomial in $R[x]$. Then there is a monic polynomial f^* with $\mu f = \mu f^*$ and, for an element a in R, $f(a) = 0$ if and only if $f^*(a) = 0$. Furthermore, there is a unit v in $R[x]$ with $vf = f^*$.*

One of the motivations for the current paper is Theorem 4 from [4], which states that if $(R, \mathfrak{m})$ is a zero-dimensional local ring, then $\mathrm{N}(R)$ is principal if and only if either $\overline{R}$ is infinite (when $\mathrm{N}(R) = 0$) or R is a finite field (when $\mathrm{N}(R)$ is generated by $x^q - x$.) The upcoming theorem ($2 \Rightarrow 1$) recovers the sufficiency in Gilmer's result, using some of the same ideas but a few different ones as well. For example, Gilmer used a result of E. Snapper; instead we use the result of McDonald mentioned above. Also, we make the connection with π-polynomials and $\mathrm{N}(\mathfrak{m})$. The necessity in Gilmer's result is recovered in Theorem 3.4, Statements 2 and 6. (In considering the connection between our results and Gilmer's Theorem, one should keep in mind that a zero-dimensional (Noetherian) local ring is finite if and only if it has a finite residue field.)

It should be noted that in Gilmer's result, local rings are assumed to be Noetherian. This is clear for several reasons, including his reference to Zariski-Samuel [12], and due to the following, which would be a counterexample to Gilmer's Theorem 4 if the local ring were not assumed to be Noetherian.

Example 3.2. *Let*

$$R = \mathbb{Z}_2[T_1, T_2, \ldots]/(T_1^2, T_2^2, \ldots) = \mathbb{Z}_2[t_1, t_2, \ldots],$$

a zero-dimensional non-Noetherian local ring with maximal ideal $\mathfrak{m} = (t_1, t_2, \ldots)$. We claim that $\mathrm{N}(R)$ is principal even though $\overline{R}$ is not infinite and R is not a finite field.

Since R has characteristic 2, $x^2 \in \mathrm{N}(\mathfrak{m})$; thus $f \in R[x]$ is in $\mathrm{N}(\mathfrak{m})$ if and only if its linear term, say f_1x, is in $\mathrm{N}(\mathfrak{m})$, and this is true if and only if $f_1\mathfrak{m} = 0$. However, the annihilator of $\mathfrak{m}$ is 0, so $\mathrm{N}(\mathfrak{m}) = (x^2)$. One may now prove directly that $\mathrm{N}(R) = ((x^2 - x)^2)$, but it's easier to note that R is Henselian and apply our main theorem, Theorem 4.2.

Theorem 3.3. *Let $(R, \mathfrak{m})$ be a finite local ring and let $\pi(x)$ be any π-polynomial for R. The following statements are equivalent:*

(1) *R is a field.*
(2) *$\mathrm{N}(R)$ is principal.*
(3) *$\mathrm{N}(R) = (\pi(x))$.*
(4) *$\mathrm{N}(\mathfrak{m})$ is principal.*
(5) *$\mathrm{N}(\mathfrak{m}) = (x)$.*

Proof. (1) ⇒ (2) If R is a field, then $R[x]$ is a principal ideal domain, so $\mathrm{N}(R)$ is principal.

(2) ⇒ (3) Assume $\mathrm{N}(R)$ is principal. Since $\pi(R) \subseteq \mathfrak{m}$ and $\mathfrak{m}^e = 0$ for some $e \geqslant 1$, $\mathrm{N}(R)$ contains regular polynomials, such as $\pi(x)^e$; thus, the generator of $\mathrm{N}(R)$ must be regular. According to Theorem 3.1, we may assume the generator is monic: $\mathrm{N}(R) = (f(x))$ for some monic polynomial in $R[x]$. Let r be a nonzero element in the annihilator of $\mathfrak{m}$, so that, by Lemma 2.5, $r\pi(x)$ is a polynomial of degree q in $\mathrm{N}(R) = (f(x))$. This forces $f(x)$ to have degree at most q, and since we know that all polynomials in $\mathrm{N}(R)$ are multiples of $\pi(x)$ (Proposition 2.7), the degree of $f(x)$ is exactly q. Since $f(x)$ is a monic multiple of $\pi(x)$ with the same degree, $f(x) = \pi(x)$.

(3) ⇒ (4) If $\mathrm{N}(R) = (\pi(x))$, then according to Corollary 2.11, $0 = \pi(R) = \mathfrak{m}$. From this we easily conclude that $\mathrm{N}(\mathfrak{m}) = (x)$, and thus $\mathrm{N}(\mathfrak{m})$ is principal.

(4) ⇒ (5) If $\mathrm{N}(\mathfrak{m})$ is principal, we use an argument similar to the part where we assumed $\mathrm{N}(R)$ is principal. Since $\mathrm{N}(\mathfrak{m})$ contains x^e for some $e \geqslant 1$, $\mathrm{N}(\mathfrak{m})$ contains regular elements, so the generator of $\mathrm{N}(\mathfrak{m})$ is regular, and we may assume it is monic: $\mathrm{N}(\mathfrak{m}) = (f(x))$ for some monic $f(x) \in R[x]$. Let r be a nonzero element in the annihilator of $\mathfrak{m}$, so that $rx \in \mathrm{N}(\mathfrak{m})$. This forces $f(x)$ to have degree at most 1. Since $f(x)$ is monic and $f(0) = 0$, $f(x) = x$, as desired.

(5) ⇒ (1) If $\mathrm{N}(\mathfrak{m}) = (x)$, then $\mathfrak{m} = 0$, so R is a field. □

In the next proposition it becomes clear how the conditions of being Artinian or having a finite residue field affect $\mathrm{N}(R)$ and $\mathrm{N}(\mathfrak{m})$. We will use the concept of the *embedding dimension* of R, denoted $\operatorname{edim} R$; this is the minimal number of generators of the maximal ideal. Recall that $\operatorname{depth} R \leqslant \dim R \leqslant \operatorname{edim} R$.

Theorem 3.4. *Let $(R, \mathfrak{m})$ be a Noetherian local ring.*

(1) $\mathrm{N}(\mathfrak{m})$ *contains nonzero polynomials if and only if* $\operatorname{depth} R = 0$.

(2) $\mathrm{N}(R)$ *contains nonzero polynomials if and only if* $\operatorname{depth} R = 0$ *and $\overline{R}$ is finite.*

(3) $\mathrm{N}(\mathfrak{m})$ *contains regular polynomials if and only if* $\dim R = 0$.

(4) $\mathrm{N}(R)$ *contains regular polynomials if and only if* $\dim R = 0$ *and $\overline{R}$ is finite.*

(5) $\mathrm{N}(\mathfrak{m})$ *is generated by a regular polynomial if and only if* $\operatorname{edim} R = 0$.

(6) $\mathrm{N}(R)$ *is generated by a regular polynomial if and only if* $\operatorname{edim} R = 0$ *and $\overline{R}$ is finite.*

In order to make the similarity with the other parts more clear, parts (4), (5), and (6) of the previous proposition were not stated as concisely as possible. Before we present the proof, we state a corollary to clarify those three parts; the proof of the corollary is straightforward and is thus omitted. In the development of this paper, we were particularly interested in the monic polynomials in $\mathrm{N}(R)$, so this corollary explains why we were mainly focused on finite rings.

Corollary 3.5. *Let $(R, \mathfrak{m})$ be a Noetherian local ring.*

(3) $\mathrm{N}(\mathfrak{m})$ *contains regular polynomials if and only if R is Artinian.*

(4) $\mathrm{N}(R)$ *contains regular polynomials if and only if R is a finite ring.*

(5) $\mathrm{N}(\mathfrak{m})$ *is generated by a regular polynomial if and only if R is a field.*

(6) $\mathrm{N}(R)$ *is generated by a regular polynomial if and only if R is a finite field.*

Proof of Theorem 3.4. (1) If R has depth 0 then since R is Noetherian, there is a nonzero element m that annihilates $\mathfrak{m}$; thus $mx \in \mathrm{N}(\mathfrak{m})$.

If R does not have depth 0, then R contains a regular element t. Let $g(x) = g_0 + g_1 x + \cdots + g_n x^n \in \mathrm{N}(\mathfrak{m})$. Since $g(t) = g(t^2) = g(t^3) = \cdots = g(t^{n+1}) = 0$, there is a matrix equation

$$\begin{bmatrix} 1 & t^1 & t^2 & \cdots & t^n \\ 1 & t^2 & t^4 & \cdots & t^{2n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & t^{n+1} & t^{(n+1)2} & \cdots & t^{(n+1)n} \end{bmatrix} \begin{bmatrix} g_0 \\ g_1 \\ \vdots \\ g_n \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

The determinant of this Vandermonde matrix is

$$\prod_{1 \leqslant i < j \leqslant n+1} (t^j - t^i) = \prod_{1 \leqslant i < j \leqslant n+1} t^i (t^{j-i} - 1).$$

Since each $t^{j-i}-1$ is a unit, this determinant is an associate of a power of t; namely t^k where $k = n(n+1)(n+2)/6$. After multiplying both sides of the matrix equation by the adjugate and dividing by the unit, we find that $t^k g_i = 0$ for each i. Since t^k is regular, the polynomial $g(x)$ is zero, as desired.

(2) Assume $\overline{R} = \{\overline{c_1}, \ldots, \overline{c_q}\}$ and R has depth 0. Since R is Noetherian with depth 0, there is a nonzero element m that annihilates $\mathfrak{m}$. By Lemma 2.5, the polynomial $\pi(x) = \prod_{i=1}^{q}(x - c_i)$ is in $\mathrm{N}\,(R, \mathfrak{m})$, so the polynomial $m\pi(x)$ is a nonzero element of $\mathrm{N}\,(R)$.

For the converse, if $\overline{R}$ is not finite, then there is an infinite sequence of elements $\{c_n\}_{n \geqslant 1}$ such that no two come from the same residue class of $\mathfrak{m}$; thus each difference $c_j - c_i$ $(j \neq i)$ is a unit. On the other hand, if R does not have depth 0, then there is a regular element $t \in \mathfrak{m}$. Consider the sequence $\{t^n\}_{n \geqslant 1}$; for $i > j$ we have $t^i - t^j = t^j(t^{i-j} - 1)$. Since t^j is regular and $t^{i-j} - 1$ is a unit, each difference $t^i - t^j$ $(i \neq j)$ is regular.

In either case, we may apply Lemma 2.4 to conclude that any nonzero polynomial in the null ideal has arbitrarily high degree. This is a contradiction, so the null ideal contains only the zero polynomial, as desired.

(3) If R has dimension 0, then $\mathfrak{m}^e = 0$ for some $e \geqslant 1$. Thus $x^e \in \mathrm{N}\,(\mathfrak{m})$.

Conversely, if R has positive dimension, then for any minimal prime ideal $\mathfrak{p}$ of R, $R/\mathfrak{p}$ is an integral domain of positive dimension; in particular, it has positive depth. According to Part (1), $\mathrm{N}\,(\mathfrak{m}/\mathfrak{p})$ is the zero ideal of $R/\mathfrak{p}$. The image of any $f(x) \in \mathrm{N}\,(\mathfrak{m})$ in $(R/\mathfrak{p})[x]$ is in $\mathrm{N}\,(\mathfrak{m}/\mathfrak{p})$, and thus $f(x) \in \mathfrak{p}[x]$. Since the coefficients of $f(x)$ are in every minimal prime, they are all nilpotent, so $f(x)$ is not regular.

(4) Suppose $\overline{R}$ is finite and $\dim R = 0$. Let e be such that $\mathfrak{m}^e = 0$ and let $\overline{R} = \{\overline{c_1}, \ldots, \overline{c_q}\}$. By Lemma 2.5, the polynomial $\pi(x) = \prod_{i=1}^{q}(x - c_i)$ is in $\mathrm{N}\,(R, \mathfrak{m})$, so the regular polynomial $\pi(x)^e$ is in $\mathrm{N}\,(R)$.

Conversely, suppose either $\overline{R}$ is infinite or $\dim R \geqslant 1$. If $\overline{R}$ is infinite, then $\mathrm{N}\,(R)$ does not contain regular polynomials since it is the zero ideal, by Part (2). If $\dim R \geqslant 1$, the proof continues as in the "conversely" part of the proof of (3), replacing $\mathrm{N}\,(\mathfrak{m}/\mathfrak{p})$ with $\mathrm{N}\,(R/\mathfrak{p})$.

(5) If $\operatorname{edim} R = 0$, then R is a field, so $\mathfrak{m} = 0$ and $\mathrm{N}\,(\mathfrak{m}) = (x)$.

Conversely, assume $\mathrm{N}\,(\mathfrak{m}) = (f(x))$ for some regular polynomial $f(x) \in R[x]$. By Part (3), $\dim R = 0$, so $\mathfrak{m}^e = 0$ for some $e \geqslant 1$. Due to this and the result from McDonald (our Theorem 3.1), we may assume $f(x)$ is monic. By Part (1), $\operatorname{depth} R = 0$, so there is an element $m \in \mathfrak{m}$ with $mx \in \mathrm{N}\,(\mathfrak{m})$. This shows that the monic polynomial $f(x)$ must have degree 1; the only choice is $f(x) = x$. From this we see that $\mathfrak{m} = 0$ so R is a field.

(6) If $\operatorname{edim} R = 0$ and $\overline{R}$ is finite, then R is a finite field, so $\mathrm{N}(R) = (\pi(x))$ for any π-polynomial, by Lemma 2.5.

Conversely, assume $\mathrm{N}(R) = (f(x))$ for some regular polynomial $f(x)$. From Part (4) we know that $\dim R = 0$ and $\overline{R}$ is finite; this implies that R is finite. By Theorem 3.3, R is a finite field, so $\operatorname{edim} R = 0$. □

In the following example we illustrate the use of this theorem and contrast the behavior of the null ideals over rings with finite and infinite residue fields.

Example 3.6. *The ring $R = \mathbb{Z}_2[\![S,T]\!]/(S^2, ST)$ is a complete Noetherian local ring with depth zero, dimension one, and a finite residue field with $q = 2$ elements; let s and t be the images of S and T in R. According to Theorem 3.4, $\mathrm{N}(\mathfrak{m})$ is nonzero but does not contain regular polynomials, and the same goes for $\mathrm{N}(R)$. We argue that $\mathrm{N}(\mathfrak{m}) = (sx)$ and conclude that $\mathrm{N}(R) = (s(x^2 - x))$ by applying Theorem 4.2. Certainly $\mathrm{N}(\mathfrak{m}) \supseteq (sx)$, since the annihilator of the maximal ideal of R is sR. For the opposite containment, let $\tilde{R} = R/sR \cong \mathbb{Z}_2[\![T]\!]$, a local Noetherian ring of positive depth. If $f(x) \in \mathrm{N}(\mathfrak{m})$, then $\tilde{f} \in \mathrm{N}(\tilde{\mathfrak{m}})$, where $\tilde{\mathfrak{m}}$ and $\tilde{f}$ are the images of $\mathfrak{m}$ and f in $\tilde{R}$ and $\tilde{R}[x]$. By Theorem 3.4 (1), $\mathrm{N}(\tilde{\mathfrak{m}}) = 0$, so we conclude that $f \in (s)$. Since $f(0) = 0$, $f \in (s) \cap (x) = (sx)$, as desired.*

If we switch to an infinite coefficient ring and residue field, say, $\mathbb{Q}$ instead of $\mathbb{Z}_2$, we still have $\mathrm{N}(\mathfrak{m}) = (sx)$ (nonzero but containing no regular polynomials). However, Theorem 4.2 does not apply (for one thing, π-polynomials don't exist). In fact, Theorem 3.4 (2) guarantees $\mathrm{N}(R) = 0$ instead of $\mathrm{N}(R) = (s(x^2 - x))$.

4. Obtaining $\mathrm{N}(R)$ from $\mathrm{N}(m)$; applications

The following proposition is the key to our main result, Theorem 4.2.

Proposition 4.1. *Let $(R, \mathfrak{m})$ be a Henselian local ring with finite residue field $\overline{R}$ and let $\pi(x)$ be an arbitrary π-polynomial. Any $f(x) \in \mathrm{N}(R)$ may be written in the form*

$$f(x) = p_0(\pi(x)) + xp_1(\pi(x)) + x^2p_2(\pi(x)) + \cdots + x^{q-1}p_{q-1}(\pi(x))$$

with each $p_i(x) \in \mathrm{N}(\mathfrak{m})$.

Proof. Let $f(x) \in \mathrm{N}(R)$. In the polynomial ring $R[x,y] = R[y][x]$, f may be divided by the monic polynomial $\pi(x) - y$, so that $f(x) = Q(x,y)(\pi(x) - y) + G(x,y)$ for some $Q(x,y), G(x,y) \in R[x,y]$ with $G(x,y) = 0$ or the degree of $G(x,y)$ with respect to x is less than q. Now set $y = \pi(x)$ to obtain $f(x) = p_0(\pi(x)) + xp_1(\pi(x)) + x^2p_2(\pi(x)) + \cdots + x^{q-1}p_{q-1}(\pi(x))$ where the polynomials $p_i(y) \in R[y]$ are the coefficients of the powers of x in $G(x, y)$.

It remains to see that each $p_i(x) \in \mathrm{N}(\mathfrak{m})$. Let $m \in \mathfrak{m}$. Since (according to Corollary 2.11) π maps each coset of $\mathfrak{m}$ onto $\mathfrak{m}$, there exists a set $c_1, c_2, \ldots, c_q$ of representatives of the residue classes of $\mathfrak{m}$, with $\pi(c_i) = m$ for each c_i; each difference $c_i - c_j$ $(i \neq j)$ is a unit. Since $f(x) \in \mathrm{N}(R)$, we may evaluate $f(x)$ at c_i for each i from 1 to q to obtain

$$0 = p_0(m) + c_ip_1(m) + c_i^2p_2(m) + \cdots + c_i^{q-1}p_{q-1}(m).$$

In matrix form, this system becomes

$$\begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix} = \begin{bmatrix} 1 & c_1 & c_1^2 & \cdots & c_1^{q-1} \\ 1 & c_2 & c_2^2 & \cdots & c_2^{q-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & c_q & c_q^2 & \cdots & c_q^{q-1} \end{bmatrix} \begin{bmatrix} p_0(m) \\ p_1(m) \\ \vdots \\ p_{q-1}(m) \end{bmatrix}.$$

The matrix is a Vandermonde matrix, and its determinant is $\prod_{1 \leqslant i < j \leqslant q}(c_j - c_i)$, which is a unit since it is a product of units. Thus, the matrix is invertible, so each $p_i(m) = 0$, as desired. □

An application of the previous result, we come to our main theorem, which states that generators for $\mathrm{N}(R)$ can be obtained by composing generators for $\mathrm{N}(\mathfrak{m})$ with any π-polynomial, which we could roughly describe by writing $\mathrm{N}(R) = \mathrm{N}(\mathfrak{m}) \circ \mathrm{N}(R, \mathfrak{m})$, if one keeps in mind Lemma 2.5 which states that $\mathrm{N}(R, \mathfrak{m}) = (\pi(x), \mathfrak{m})$. An obvious consequence of the next theorem is that the minimal number of generators of $\mathrm{N}(R)$ is less than or equal to the minimal number of generators of $\mathrm{N}(\mathfrak{m})$.

Theorem 4.2. *Suppose $(R, \mathfrak{m})$ is a Henselian local ring with finite residue field $\overline{R}$ of cardinality q and let $\pi(x)$ be an arbitrary π-polynomial. If $\mathrm{N}(\mathfrak{m}) = (F_1(x), \ldots, F_n(x))$, then $\mathrm{N}(R) = (F_1(\pi(x)), \ldots, F_n(\pi(x)))$.*

Proof. Since $\pi(R) \subseteq \mathfrak{m}$, certainly $\mathrm{N}(R) \supseteq (F_1(\pi(x)), \ldots, F_n(\pi(x)))$. Now let $f(x) \in \mathrm{N}(R)$. Use Proposition 4.1 to write $f(x) = p_0(\pi(x)) + xp_1(\pi(x)) + x^2p_2(\pi(x)) + \cdots + x^{q-1}p_{q-1}(\pi(x))$ with each $p_i(x) \in \mathrm{N}(\mathfrak{m})$. Since each $p_i(x)$ is an $R[x]$-linear combination of $F_1(x), \ldots, F_n(x)$, each $p_i(\pi(x))$ is an $R[x]$-linear (actually $R[\pi(x)]$-linear) combination of $F_1(\pi(x)), \ldots, F_n(\pi(x))$. Since $f(x)$ is an $R[x]$-linear combination of the $p_i(\pi(x))$, the proof is complete. □

Remark 4.3. *The equality* $\mathrm{N}(R) = \mathrm{N}(\mathfrak{m}) \circ \mathrm{N}(R, \mathfrak{m})$ *should not be taken too literally. Certainly polynomials in* $\mathrm{N}(\mathfrak{m})$ *composed with polynomials in* $\mathrm{N}(R, \mathfrak{m})$ *are in* $\mathrm{N}(R)$*, but it's not true that every polynomial in* $\mathrm{N}(R)$ *can be obtained in that way. For example,* $x(x^2 - x) \in \mathrm{N}(\mathbb{Z}_2)$*, but since its degree is not even, it does not equal* $f(x^2 - x)$ *for any polynomial* $f(x)$*.*

As mentioned in the introduction, the theorem below is a version of results of Dickson [2, p. 22, Theorem 27], Bandini [1, Theorem 2.1], and Lewis [7, Theorem II], adapted for $\mathrm{N}(\mathfrak{m})$ rather than $\mathrm{N}(R)$, and for finite local rings rather than specific rings. We then recover the results for $\mathrm{N}(R)$ in Corollary 4.5 as an application of our main theorem, Theorem 4.2.

Theorem 4.4. *Let* $(R, \mathfrak{m})$ *be a finite local ring with principal maximal ideal* $\mathfrak{m} = (m)$*; set* $q = |R/\mathfrak{m}|$*. Suppose* e *is the index of nilpotency of* $\mathfrak{m}$*. If* $e \leqslant q$*, then* $\mathrm{N}(\mathfrak{m}) = (x, m)^e$*; if* $e = q + 1$*, then* $\mathrm{N}(\mathfrak{m}) = (x, m)^e + (x^q - m^{q-1}x)$*.*

Proof. We prove the first result using induction on e. The base case $e = 1$ is clear, since then R is a field, $\mathfrak{m} = 0$, and $\mathrm{N}(\mathfrak{m}) = (x)$. Assume the result is true for rings whose maximal ideal has index of nilpotency $e - 1 \leqslant q$; we prove the result for a ring whose maximal ideal has index of nilpotency $e \leqslant q$. The containment $\supseteq$ is clear. Let $f(x) \in \mathrm{N}(\mathfrak{m})$; then $\overline{f}(x) \in \mathrm{N}\left(\mathfrak{m}/\mathfrak{m}^{e-1}\right)$. By induction, $\overline{f}(x) \in \overline{(x, m)^{e-1}}$, and thus $f(x) \in (x, m)^{e-1}$. We have $f(x) = \sum_{k=0}^{e-1} x^k m^{e-1-k} f_k(x)$ for some $f_k(x) \in R[x]$; it remains to see that each $f_k(x) \in (x, m)$, i.e. that $f_k(0) \in \mathfrak{m}$.

For each $r \in R$,

$$0 = f(rm) = \sum_{k=0}^{e-1} (rm)^k m^{e-1-k} f_k(rm) = m^{e-1} \sum_{k=0}^{e-1} r^k f_k(rm).$$

Since the annihilator of m^{e-1} is $\mathfrak{m}$, $\sum_{k=0}^{e-1} r^k f_k(rm) \in \mathfrak{m}$, and thus $\sum_{k=0}^{e-1} r^k f_k(0) \in \mathfrak{m}$. This shows that $\sum_{k=0}^{e-1} \overline{f_k(0)} x^k \in \mathrm{N}\left(\overline{R}\right)$. Since by Lemma 2.5 $\mathrm{N}\left(\overline{R}\right) = (x^q - x)$, this polynomial with degree less than q must be the zero polynomial. Therefore each $f_k(0) \in \mathfrak{m}$, as desired.

For the second result, the only part of the containment $\mathrm{N}(\mathfrak{m}) \supseteq (x, m)^e + (x^q - m^{q-1}x)$ that is not clear is $x^q - m^{q-1}x \in \mathrm{N}(\mathfrak{m})$; for this, take any $rm \in \mathfrak{m}$ and compute $(rm)^q - m^{q-1}(rm) = m^q(r^q - r) \in \mathfrak{m}^{q+1} = 0$. For the opposite containment, assume $f(x) \in \mathrm{N}(\mathfrak{m})$ and reduce module $\mathfrak{m}^{e-1}$ as above to obtain a similar expression for $f(x)$, and again deduce that $\sum_{k=0}^{e-1} \overline{f_k}(0) x^k \in \mathrm{N}\left(\overline{R}\right) = (x^q - x)$. Since $e - 1 = q$, we must have $\sum_{k=0}^{e-1} \overline{f_k}(0) x^k = \overline{u}(x^q - x)$ for some unit $u \in R$; thus each $\overline{f_k(0)} = 0$ except for $\overline{f_q(0)} = \overline{u}$ and $\overline{f_1(0)} = -\overline{u}$. Define polynomials $g_k(x)$ identical to $f_k(x)$ except for $g_q(x) = f_q(x) - u$ and $g_1(x) = f_1(x) + u$. Now the constant term of each $g_k(x)$ is in $\mathfrak{m}$ and we have

$$f(x) = \sum_{k=0}^{e-1} x^k m^{e-1-k} f_k(x) = u(x^q - m^{q-1}x) + \sum_{k=0}^{e-1} x^k m^{e-1-k} g_k(x)$$

so that $f(x) \in (x, m)^e + (x^q - m^{q-1}x)$, as desired. □

The following corollary follows immediately from the theorem and Theorem 4.2.

Corollary 4.5. *Let $(R, \mathfrak{m})$ be a finite local ring with principal maximal ideal $\mathfrak{m} = (m)$; set $q = |R/\mathfrak{m}|$. Suppose e is the index of nilpotency of $\mathfrak{m}$, and let $\pi(x)$ be any π-polynomial. If $e \leqslant q$ then $\mathrm{N}(R) = (\pi(x), m)^e$; if $e = q + 1$ then $\mathrm{N}(R) = (\pi(x), m)^e + (\pi(x)^q - m^{q-1}\pi(x))$.*

5. Factoring π-polynomials

The following lemma is the heart of a more constructive approach (Theorem 5.2) to the converse part of the proof of Theorem 2.10, which gave two equivalent conditions for π-polynomials. Note that according to this lemma, if $\mathfrak{m}^e = 0$, then for any $r \in R$, the sequence $\{p_n(r)\}$ stabilizes at $n = e - 1$.

Lemma 5.1. *Let $(R, \mathfrak{m})$ be a Noetherian local ring with finite residue field $\overline{R}$ of cardinality q, and let $p(x)$ be any polynomial mapping to $x^q - x$ in $\overline{R}[x]$. Let $p_0(x) = x$ and $p_n(x) = p(p_{n-1}(x)) + p_{n-1}(x)$, so that $p_n(x)$ denotes the function obtained by successively applying the function $p(x) + x$, n times. For every $n \geqslant 1$,*

$$p_n(x) - p_{n-1}(x) \in \mathrm{N}(R, \mathfrak{m}^n).$$

Proof. We use induction on n. For the base case ($n = 1$) just note that $p_1(x) - p_0(x) = (p(x) + x) - x = p(x) \in \mathrm{N}\left(R, \mathfrak{m}^1\right)$ by Lemma 2.5.

Now assume the induction hypothesis: For some $n \geqslant 1$, $p_n(x) - p_{n-1}(x) \in \mathrm{N}(R, \mathfrak{m}^n)$. We show that $p_{n+1}(x) - p_n(x) \in \mathrm{N}\left(R, \mathfrak{m}^{n+1}\right)$. Since $p(x)$ is a polynomial mapping to $x^q - x$ modulo $\mathfrak{m}[x]$, there is some $m(x) \in \mathfrak{m}[x]$ such that $p(x) = x^q - x - m(x)$; thus $p_n(x)$ may also be viewed as applying $x^q - m(x)$, n times. For simplicity of notation, set $c = p_n(x)$, $a = p_{n-1}(x)$, and $b = c - a$, so that

$c = p(a) + a = a^q - m(a)$. We have

$$\begin{aligned} p_{n+1}(x) - p_n(x) &= p(p_n(x)) + p_n(x) - p_n(x) \\ &= p(c) \\ &= c^q - c - m(c) \\ &= (a+b)^q - c - m(c) \\ &= a^q + qa^{q-1}b + \binom{q}{2} a^{q-2}b^2 + \cdots + b^q - c - m(c) \\ &= qa^{q-1}b + \binom{q}{2} a^{q-2}b^2 + \cdots + b^q + m(a) - m(c) \end{aligned}$$

since $a^q - c = m(a)$. By induction, $b \in \mathrm{N}(R, \mathfrak{m}^n)$, and since $q \in \mathfrak{m}$, we see that the first term is in $\mathrm{N}\left(R, \mathfrak{m}^{n+1}\right)$. Since $b \in \mathrm{N}(R, \mathfrak{m}^n)$ and $n \geqslant 1$, $b^2 \in \mathrm{N}\left(R, \mathfrak{m}^{n+1}\right)$, which takes care of all but the last two terms: $m(a) - m(c)$.

Now $m(a) - m(c) = \sum_{i=1}^{\deg m(x)} m_i(a^i - c^i)$, where m_i is the coefficient of x^i in $m(x)$, and is thus in $\mathfrak{m}$. Since $-b = a - c$ is a factor of $a^i - c^i$ for all positive integers i and $-b \in \mathrm{N}(R, \mathfrak{m}^n)$, it follows that $m(a) - m(c) \in \mathrm{N}\left(R, \mathfrak{m}^{n+1}\right)$, as desired. □

The following theorem provides, in particular, a more constructive approach to the proof of the result in Theorem 2.10 which states that any monic polynomial $p(x)$ mapping to $x^q - x$ is actually a π-polynomial. In a ring with $\mathfrak{m}^e = 0$, it allows discovery of the roots by successively applying the function $p(x) + x$ ($e - 1$ times) to representatives of the residue classes of $\mathfrak{m}$. When $p(x) = x^q - x$, this amounts to successively taking qth powers. In the case of a finite ring, the resulting roots of $x^q - x$ are called *Teichmüller elements* in Jian Jun Jiang's paper [5].

Theorem 5.2. *Let $(R, \mathfrak{m})$ be a complete Noetherian local ring with finite residue field $\overline{R} = \{\overline{c_1}, \ldots, \overline{c_q}\}$. Let $p(x)$ be any polynomial mapping to $x^q - x$ in $\overline{R}[x]$ and let $p_n(x)$ be the function obtained by applying $p(x) + x$ successively, n times. The limit $\lim_{n\to\infty} p_n(c_i)$ exists. Set $d_i = \lim_{n\to\infty} p_n(c_i)$; then d_i is a root of $p(x)$ and $\overline{d_i} = \overline{c_i}$. If $p(x)$ is monic, then there is a factorization*

$$p(x) = (x - d_1)(x - d_2) \cdots (x - d_q),$$

and thus $p(x)$ is a π-polynomial.

Proof. The limit exists since, by Lemma 5.1, the sequence $\{p_n(c_i)\}_{n \geqslant 1}$ is a Cauchy sequence. For any $r \in R$, $p(r) + r$ and r are in the same coset of $\mathfrak{m}$, since $p(r) = r^q - r - m(r) \in \mathfrak{m}$. We may apply this fact successively, beginning with $r = c_i$, to see that each $p_n(c_i)$ is congruent to c_i modulo $\mathfrak{m}$. Since $\mathfrak{m}$ is closed under the $\mathfrak{m}$-adic topology, we conclude that $\overline{d_i} = \overline{c_i}$.

To see that $p(d_i) = 0$, use the Cauchy sequence mentioned above and the fact that polynomials are continuous under the $\mathfrak{m}$-adic topology:

$$p(d_i) = p(\lim p_n(c_i)) = \lim p(p_n(c_i)) = \lim(p_{n+1}(c_i) - p_n(c_i)) = 0.$$

If $p(x)$ is monic then it must have degree q; an application of Lemma 2.4 completes the proof. □

Example 5.3. *With $R = \mathbb{Z}_{125}$, we have $q = 5$ and $e = 3$. We can choose elements $0, 1, 2, 3, 4$ to be representatives of the elements of $R/\mathfrak{m} = \mathbb{Z}_5$. We factor the polynomial*

$$\pi(x) = x^5 + 5x^4 + 40x^3 + 85x^2 + 24x + 50 = x^5 - x - m(x)$$

where $m(x) = -(5x^4 + 40x^3 + 85x^2 + 25x + 50)$. Applying $p_2(x)$ to $0, 1, 2, 3, 4$ yields $50, 31, 72, 18, 74$. According to the theorem, $\pi(x)$ factors in $R[x]$ as

$$\pi(x) = (x - 50)(x - 31)(x - 72)(x - 18)(x - 74).$$

Acknowledgment. The authors thank Richard Belshoff, Jung-Chen Liu and Les Reid for helpful discussions and suggestions, and the referee for valuable suggestions and comments.

References

[1] A. Bandini, *Functions $f\colon \mathbb{Z}/p^n\mathbb{Z} \longrightarrow \mathbb{Z}/p^n\mathbb{Z}$ induced by polynomials of $\mathbb{Z}[x]$*, Ann. Mat. Pura Appl., 181 (2002), 95-104.

[2] L. E. Dickson, Introduction to the Theory of Numbers, The University of Chicago Press, 1929.

[3] S. Frisch, *Polynomial functions on finite commutative rings*, Advances in commutative ring theory (Fez, 1997), Lecture Notes in Pure and Appl. Math., 205, Dekker, New York, (1999), 323-336.

[4] R. Gilmer, *The ideal of polynomials vanishing on a commutative ring*, Proc. Amer. Math. Soc., 127(5) (1999), 1265-1267.

[5] J. J. Jiang, *On the number counting of polynomial functions*, J. Math. Res. Exposition, 30(2) (2010), 241-248.

[6] J. Lahtonen, J. Ryu and E. Suvitie, *On the degree of the inverse of quadratic permutation polynomial interleavers*, IEEE Trans. Inform. Theory, 58(6) (2012), 3925-3932.

[7] D. J. Lewis, *Ideals and polynomial functions*, Amer. J. Math., 78 (1956), 71-77.

[8] B. R. McDonald, Finite Rings with Identity, Pure and Applied Mathematics, 28, Marcel Dekker, Inc., New York, 1974.

[9] I. Niven and L. J. Warren, *A generalization of Fermat's theorem*, Proc. Amer. Math. Soc., 8 (1957), 306-313.

[10] G. Peruginelli, *Primary decomposition of the ideal of polynomials whose fixed divisor is divisible by a prime power*, J. Algebra, 398 (2014), 227-242.

[11] N. J. Werner, *Polynomials that kill each element of a finite ring*, J. Algebra Appl., 13(3) (2014), 1350111 (12 pp).

[12] O. Zariski and P. Samuel, Commutative Algebra, vol. I, Springer-Verlag, Berlin-Heidelberg, 1958.

[13] Q. Zhang, *Polynomial functions and permutation polynomials over some finite commutative rings*, J. Number Theory, 105(1) (2004), 192-202.

Mark W. Rogers (Corresponding Author) and **Cameron Wickham**
Department of Mathematics
Missouri State University
Springfield, MO 65897, USA
e-mails: markrogers@missouristate.edu (M. W. Rogers)
cwickham@missouristate.edu (C. Wickham)