DE GRUYTER

Mathematica Slovaca

DOI: 10.1515/ms-2021-0039
Math. Slovaca **71** (2021), No. 5, 1063–1088

POLYNOMIAL FUNCTIONS ON RINGS OF DUAL NUMBERS OVER RESIDUE CLASS RINGS OF THE INTEGERS

Hasan Al-Ezeh* — Amr Ali Al-Maktry**, c — Sophie Frisch**

The second and third authors wish to dedicate this paper to the memory of Prof. Al-Ezeh, who died while the paper was under review.

(*Communicated by István Gaál*)

ABSTRACT. The ring of dual numbers over a ring R is $R[\alpha] = R[x]/(x^2)$, where α denotes $x + (x^2)$. For any finite commutative ring R, we characterize null polynomials and permutation polynomials on $R[\alpha]$ in terms of the functions induced by their coordinate polynomials ($f_1, f_2 \in R[x]$, where $f = f_1 + \alpha f_2$) and their formal derivatives on R.

We derive explicit formulas for the number of polynomial functions and the number of polynomial permutations on $\mathbb{Z}_{p^n}[\alpha]$ for $n \le p$ (p prime).

1. Introduction

Let A be a finite commutative ring. A function $F\colon A \longrightarrow A$ is called a polynomial function on A if there exists a polynomial $f = \sum\limits_{k=0}^{n} c_k x^k \in A[x]$ such that $F(a) = \sum\limits_{k=0}^{n} c_k a^k$ for all $a \in A$. When a polynomial function F is bijective, it is called a polynomial permutation of A, and f is called a permutation polynomial on A.

Polynomial functions on A form a monoid $(\mathcal{F}(A), \circ)$ with respect to composition. Its group of units, which we denote by $\mathcal{P}(A)$, consists of all polynomial permutations of A. Unless A is a finite field, not every function on A is a polynomial function and not every permutation of A is a polynomial permutation. Apart from their intrinsic interest in algebra, polynomial functions on finite rings have uses in computer science [4,12].

For any ring R, the ring of dual numbers over R is defined as $R[\alpha] = R[x]/(x^2)$, where x is an indeterminate and α stands for $x + (x^2)$. Rings of dual numbers are used in coding theory [5,7].

In this paper, we investigate the polynomial functions and polynomial permutations of rings of dual numbers over finite rings. Since every finite commutative ring is a direct sum of local rings, and evaluation of polynomial functions factors through this direct sum decomposition, we may concentrate on local rings.

2020 Mathematics Subject Classification: Primary 13F20; Secondary 11T06, 13B25, 12E10, 05A05, 06B10.
Keywords: finite rings, finite commutative rings, dual numbers, polynomials, polynomial functions, polynomial mappings, polynomial permutations, permutation polynomials, null polynomials.
This work was supported by the Austrian Science Fund FWF projects P 27816-N26 and P 30934-N35.

[c] Corresponding author.

Among other things, we derive explicit formulas for $|\mathcal{F}(\mathbb{Z}_{p^n}[\alpha])|$ and $|\mathcal{P}(\mathbb{Z}_{p^n}[\alpha])|$ where $n \leq p$. Here, as in the remainder of this paper, p is a prime number and, for any natural number m, $\mathbb{Z}_m$ stands for the ring of integers modulo m, that is, $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$.

The study of the monoid of polynomial functions and the group of polynomial permutations on a finite ring R essentially originated with Kempner, who, in 1921, determined their orders in the case where R is the ring of integers modulo a prime power:

$$|\mathcal{F}(\mathbb{Z}_{p^n})| = p^{\sum\limits_{k=1}^{n}\mu(p^k)} \qquad \text{and} \qquad |\mathcal{P}(\mathbb{Z}_{p^n})| = p!p^p(p-1)^p p^{\sum\limits_{k=3}^{n}\mu(p^k)} \qquad \text{for } n > 1, \tag{1.1}$$

where $\mu(p^k)$ is the minimal $l \in \mathbb{N}$ such that p^k divides $l!$, that is, the minimal $l \in \mathbb{N}$ for which $\sum\limits_{j\geq 1} \lfloor \frac{l}{p^j} \rfloor \geq k$. (Here $\lfloor z \rfloor$ means the largest integer smaller than or equal to z).

Kempner's proof has been simplified [15, 26, 29] and his formulas shown to hold for more general classes of local rings [3, 9, 20] when p is replaced by the order of the residue field and n by the nilpotency of the maximal ideal. The classes of local rings for which Kempner's formulas hold *mutatis mutandis* have been up to now the only finite local rings (R, M) for which explicit formulas for $|\mathcal{F}(R)|$ and $|\mathcal{P}(R)|$ are known. (By explicit formula, we mean one that depends only on readily apparent parameters of the finite local ring, such as the order of the ring and its residue field, and the nilpotency of the maximal ideal.)

What all the finite local rings (A, M) for which explicit formulas for $|\mathcal{F}(A)|$ and $|\mathcal{P}(A)|$ are known have in common is the following property: If m is the nilpotency of the maximal ideal M of A, and we denote by $w(a)$ the maximal $k \leq m$ such that $a \in M^k$, then, for any $a, b \in A$,

$$w(ab) = \min(w(a) + w(b), m),$$

that is, A allows a kind of truncated discrete valuation, with values in the additive monoid on $\{0, 1, 2, \ldots, m\}$, whose addition is $u \oplus v = \min(u + v, m)$.

Rings of dual numbers over $\mathbb{Z}_{p^n}$, for which we provide explicit formulas for the number of polynomial functions and the number of polynomial permutations in Theorems 8.11 and 8.10, do not have this property, except for $n = 1$, see Proposition 2.9.

Statements about the number of polynomial functions and polynomial permutations that hold for any finite commutative ring A are necessarily less explicit in nature than the counting formulas in Equation (1.1) on one hand and Theorems 8.10 and 8.11 on the other hand.

Görcsös, Horváth and Mészáros [11] provide a formula, valid for any finite local commutative ring that satisfies the condition $M^{|A/M|} = \{0\}$, expressing the number of polynomial permutations in terms of the cardinalities of the annihilators of the ideals M_k generated by the k-th powers of elements of the maximal ideal. We will not make use of this formula, however, but prove our counting formulas from scratch, in a way that yields additional insight into the structure of the monoid of polynomial functions and the group of polynomial permutations on rings of dual numbers. Also for any finite local commutative ring A, Jiang [13] has determined the ratio of $|\mathcal{P}(A)|$ to $|\mathcal{F}(A)|$, see Remark 5.8.

Chen [6], Wei and Zhang [27, 28], Liu and Jiang [18], among others [8, 22] have generalized facts about polynomial functions in one variable to several variables. Starting with polynomial functions over rings of dual numbers, we get a different kind of generalization to several parameters, if we replace $R[\alpha]$ by $R[\alpha_1, \ldots, \alpha_n]$ with $\alpha_i\alpha_j = 0$. The second author has shown that most results of the present paper carry over to this generalization [2].

Beyond number formulas, some structural results about groups of permutation polynomials on $\mathbb{Z}_{p^n}$ are known, due to Nöbauer [21, 24] and others [10, 30].

In this paper, we derive structural results about $\mathcal{F}(R[\alpha])$ and $\mathcal{P}(R[\alpha])$ by relating them to $\mathcal{F}(R)$ and $\mathcal{P}(R)$, and then use these results to prove explicit formulas for $|\mathcal{F}(\mathbb{Z}_{p^n}[\alpha])|$ and $|\mathcal{P}(\mathbb{Z}_{p^n}[\alpha])|$ in the case $n \le p$.

Here is an outline of the paper. After establishing some notation in Section 2, we characterize null polynomials on $R[\alpha]$ in Section 3 and permutation polynomials on $R[\alpha]$ in Section 4, for any finite local ring R. Section 5 relates the pointwise stabilizer of R in the group of polynomial permutations on $R[\alpha]$ to functions induced by the formal derivatives of permutation polynomials. Section 6 relates permutation polynomials on $\mathbb{Z}_{p^n}[\alpha]$ to permutation polynomials on $\mathbb{Z}_{p^n}$. Section 7 contains counting formulas for the numbers of polynomial functions and polynomial permutations on $\mathbb{Z}_{p^n}[\alpha]$ in terms of the order of the pointwise stabilizer of $\mathbb{Z}_{p^n}$ in the group of polynomial permutations on $\mathbb{Z}_{p^n}[\alpha]$. Section 8 contains explicit formulas for $|\mathcal{F}(\mathbb{Z}_{p^n}[\alpha])|$ and $|\mathcal{P}(\mathbb{Z}_{p^n}[\alpha])|$ for $n \le p$. Section 9 gives a canonical representation for polynomial functions on $\mathbb{Z}_{p^n}[\alpha]$ for $n \le p$. The easy special case where R is a finite field is treated en passant in sections 3 and 4.

2. Basics

We recall a few facts about rings of dual numbers and polynomial functions, and establish our notation. Since we are mostly concerned with polynomials over finite rings, we have to distinguish carefully between polynomials and the functions induced by them. All rings are assumed to have a unit element and to be commutative.

Throughout this paper, p always stands for a prime number. We use $\mathbb{N}$ for the positive integers (natural numbers), $\mathbb{N} = \{1, 2, 3, \ldots\}$, and $\mathbb{N}_0 = \{0, 1, 2, \ldots\}$ for the non-negative integers.

Definition 2.1. Let R be a ring and $a_0, \ldots, a_n \in R$. The polynomial $f = \sum\limits_{i=0}^{n} a_i x^i \in R[x]$ defines (or induces) a function $F\colon R \to R$ by substitution of the variable: $F(r) = \sum\limits_{i=0}^{n} a_i r^i$. A function arising from a polynomial in this way is called a *polynomial function*.

If the polynomial function $F\colon R \to R$ induced by $f \in R[x]$ is bijective, then F is called a *polynomial permutation* of R and f is called a *permutation polynomial* on R.

We will frequently consider polynomials with coefficients in $\mathbb{Z}$ inducing functions on $\mathbb{Z}_m$ for various m. We put this on a formal footing in the next definition.

Definition 2.2. Let S be a commutative ring, R an S-algebra and $f \in S[x]$.

(1) The polynomial f gives rise to a polynomial function on R, by substitution of the variable with elements of R. We denote this function by $[f]_R$, or just by $[f]$, when R is understood.

(2) In the special case where $S = \mathbb{Z}$ and $R = \mathbb{Z}_m$, we write $[f]_m$ for $[f]_{\mathbb{Z}_m}$.

(3) When $[f]_R$ is a permutation on R, we call f a *permutation polynomial* on R.

(4) If $f, g \in S[x]$ such that $[f]_R = [g]_R$, we write $f \triangleq g$ on R.

Remark 2.3.

(1) Clearly, $\triangleq$ is an equivalence relation on $S[x]$.

(2) When $R = S$, or R is a homomorphic image of S, the equivalence classes of $\triangleq$ are in bijective correspondence with the polynomial functions on R.

(3) In particular, when R is finite, the number of different polynomial functions on R equals the number of equivalence classes of $\triangleq$ on $R[x]$.

We now introduce the class of rings whose polynomial functions and polynomial permutations we will investigate.

Definition 2.4. Throughout this paper, if R is a commutative ring, then $R[\alpha]$ denotes the result of adjoining α with $\alpha^2 = 0$ to R; that is, $R[\alpha]$ is $R[x]/(x^2)$, where $\alpha = x + (x^2)$. The ring $R[\alpha]$ is called the *ring of dual numbers over R.*

Remark 2.5. Note that R is canonically embedded as a subring in $R[\alpha]$ via $a \mapsto a + 0\alpha$.

For the convenience of the reader, we summarize some easy facts about the arithmetic of rings of dual numbers.

Proposition 2.6. *Let R be a commutative ring. Then*

(1) *for $a, b, c, d \in R$, we have*
   (a) $(a + b\,\alpha)(c + d\,\alpha) = ac + (ad + bc)\,\alpha$
   (b) $(a + b\,\alpha)$ *is a unit of $R[\alpha]$ if and only if a is a unit of R. In this case* $(a + b\,\alpha)^{-1} = a^{-1} - a^{-2}b\,\alpha$.

(2) *$R[\alpha]$ is a local ring if and only if R is a local ring.*

(3) *If R is a local ring with maximal ideal $\mathfrak{m}$ of nilpotency K, then $R[\alpha]$ is a local ring with maximal ideal $\mathfrak{m} + \alpha\,R = \{a + b\alpha \mid a \in \mathfrak{m},\ b \in R\}$ of nilpotency $K + 1$.*

(4) *Let $(R, \mathfrak{m})$ be a local ring. The canonical embedding $r \mapsto r + 0\alpha$ factors through to an isomorphism of the residue fields of R and $R[\alpha]$: $R/\mathfrak{m} \cong R[\alpha]/(\mathfrak{m} + \alpha\,R)$.*

Likewise, we summarize the details of substituting dual numbers for the variable in a polynomial with coefficients in the ring of dual numbers below.

As usual, f' denotes the formal derivative of a polynomial f. That is, $f' = \sum\limits_{k=1}^{n} ka_k x^{k-1}$ for $f = \sum\limits_{k=0}^{n} a_k x^k$.

Lemma 2.7. *Let R be a commutative ring, and let $a, b \in R$.*

(1) *Let $f \in R[\alpha][x]$ and $f_1, f_2 \in R[x]$ be the unique polynomials in $R[x]$ such that $f = f_1 + \alpha\, f_2$. Then*
$$f(a + b\,\alpha) = f_1(a) + (bf_1'(a) + f_2(a))\,\alpha\,.$$

(2) *In the special case when $f \in R[x]$, we get*
$$f(a + b\,\alpha) = f(a) + bf'(a)\,\alpha\,.$$

As a consequence of the above lemma, we obtain a necessary condition for a function on $R[\alpha]$ to be a polynomial function.

Corollary 2.8. *Let $F\colon R[\alpha] \to R[\alpha]$ such that $F(a+b\,\alpha) = c_{(a,b)} + d_{(a,b)}\,\alpha$ with $c_{(a,b)}, d_{(a,b)} \in R$. If F is a polynomial function on $R[\alpha]$, then $c_{(a,b)}$ depends only on a, that is, $c_{(a,b)} = c_{(a,b_1)}$ for all $a, b, b_1 \in R$.*

The last proposition of this section goes to show that rings of dual numbers over $\mathbb{Z}_{p^n}$ $(n > 1)$ are a class of local rings for which no explicit formulas for the number of polynomial functions existed previously. By an explicit formula we mean a formula depending only on the order of the residue field and the nilpotency of the maximal ideal.

Proposition 2.9. *For a finite local ring R with maximal ideal $\mathfrak{m}$ of nilpotency K, consider the following condition:*

"For all $a, b \in R$ and all $k \in \mathbb{N}$, whenever $ab \in \mathfrak{m}^k$, it follows that $a \in \mathfrak{m}^i$ and $b \in \mathfrak{m}^j$ for $i, j \in \mathbb{N}_0$ with $i + j \geq \min(K, k)$."

Then $R = \mathbb{Z}_{p^n}[\alpha]$ satisfies the condition if and only if $n = 1$.

Proof. Since $\mathbb{Z}_{p^n}$ is a local ring with maximal ideal (p), $\mathbb{Z}_{p^n}[\alpha]$ is a local ring with maximal ideal $\mathfrak{m} = \{ap + b\,\alpha \mid a, b \in \mathbb{Z}_{p^n}\}$ and $K = n + 1$ by Proposition 2.6. If $n = 1$, then the result easily follows since $\mathfrak{m}^2 = (0)$. If $n \geq 2$, then $K = n + 1 > 2$, and $\alpha^2 = 0 \in \mathfrak{m}^{n+1}$, but $\alpha \in \mathfrak{m} \setminus \mathfrak{m}^2$. □

Local rings satisfying the condition of Proposition 2.9 have been called suitable in a previous paper by the third author [9]. Previously known explicit formulas for the number of polynomial functions and the number of polynomial permutations on a finite local ring (R, M) all concern suitable rings and are the same as Kempner's formulas (1.1) for $R = \mathbb{Z}_{p^n}$, except that p is replaced by $q = |R/M|$ and n by the nilpotency of M. The previous proposition shows that, whenever $n > 1$, $\mathbb{Z}_{p^n}[\alpha]$ is not a "suitable" ring.

3. Null polynomials on $R[\alpha]$

When one sets out to count the polynomial functions on a finite ring A, one is lead to studying the ideal of so called null-polynomials – polynomials in $A[x]$ that induce the zero-function on A–, because residue classes of $A[x]$ modulo this ideal correspond bijectively to polynomial functions on A.

In this section, we study null-polynomials for rings of dual numbers $A = R[\alpha]$ as defined in the previous section (Definition 2.4). We relate polynomial functions on $R[\alpha]$ (induced by polynomials in $R[\alpha][x]$) to polynomial functions induced on $R[\alpha]$ by polynomials in $R[x]$, and further to pairs of polynomial functions on R arising from polynomials in $R[x]$ and their formal derivatives.

Definition 3.1. Let R be a commutative ring and A an R-algebra, and notation as in Definition 2.2. A polynomial $f \in R[x]$ is called a *null polynomial* on A if $[f]_A$ is the constant zero function, which we denote by $f \triangleq 0$ on A.

We define N_R and N'_R as

(1) $N_R = \{f \in R[x] \mid f \triangleq 0 \text{ on } R\}$

(2) $N'_R = \{f \in R[x] \mid f \triangleq 0 \text{ on } R \text{ and } f' \triangleq 0 \text{ on } R\}$.

Remark 3.2. Clearly, N_R, N'_R are ideals of $R[x]$, and we have $|\mathcal{F}(R)| = [R[x] : N_R]$.

***Example* 3.3.** Let $R = \mathbb{F}_q$ be the finite field of q elements. Then

(1) $N_{\mathbb{F}_q} = (x^q - x)\mathbb{F}_q[x]$

(2) $N'_{\mathbb{F}_q} = (x^q - x)^2\mathbb{F}_q[x]$

(3) $[\mathbb{F}_q[x] : N'_{\mathbb{F}_q}] = q^{2q}$.

To see (2), let $g \in N'_{\mathbb{F}_q}$. Then clearly, $g(x) = h(x)(x^q - x)$. Hence

$$g'(x) = h(x)(qx^{q-1} - 1) + h'(x)(x^q - x) = h'(x)(x^q - x) - h(x),$$

and so $0 \triangleq g' \triangleq -h$ on $\mathbb{F}_q$. Thus h is a null polynomial on $\mathbb{F}_q$, and hence divisible by $(x^q - x)$.

By means of the ideal N'_R, we will reduce questions about polynomials with coefficients in $R[\alpha]$ to questions about polynomials with coefficients in R, as exemplified in Proposition 3.10 below.

Lemma 3.4. *Let $f \in R[x]$. Then*

(1) *f is a null polynomial on $R[\alpha]$ if and only if both f and f' are null polynomials on R*

(2) *αf is a null polynomial on $R[\alpha]$ if and only if f is a null polynomial on R.*

Proof. Ad (1). By Lemma 2.7, for every $a, b \in R$, $f(a + b\,\alpha) = f(a) + bf'(a)\,\alpha$. Thus by Definition 3.1, f being a null polynomial on $R[\alpha]$ is equivalent to $f(a) + bf'(a)\,\alpha = 0$ for all $a, b \in R$. This is equivalent to $f(a) = 0$ and $bf'(a) = 0$ for all $a, b \in R$. Setting $b = 1$, we see that $f(a) = 0$ and $f'(a) = 0$ for all $a \in R$. Hence f and f' are null polynomials on R.
Statement (2) follows from Lemma 2.7. □

Theorem 3.5. *Let $f \in R[\alpha][x]$, written as $f = f_1 + \alpha\, f_2$ with $f_1, f_2 \in R[x]$.*

f is a null polynomial on $R[\alpha]$ if and only if f_1, f_1', and f_2 are null polynomials on R.

Proof. By Lemma 2.7, for all $a, b \in R$,

$$f(a + b\,\alpha) = f_1(a) + (bf_1'(a) + f_2(a))\,\alpha\,.$$

This implies the "if" direction. To see "only if", suppose that f is a null polynomial on $R[\alpha]$. Then, for all $a, b \in R$,

$$f_1(a) + (bf_1'(a) + f_2(a))\,\alpha = 0.$$

Clearly, f_1 is a null polynomial on R. Substituting 0 for b yields that f_2 is a null polynomial on R and substituting 1 for b yields that f_1' is a null polynomial on R. □

Combining Lemma 3.4 with Theorem 3.5 gives the following criterion.

Corollary 3.6. *Let $f \in R[\alpha][x]$, written as $f = f_1 + \alpha\, f_2$ with $f_1, f_2 \in R[x]$.*

f is a null polynomial on $R[\alpha]$ if and only if f_1 and $\alpha\, f_2$ are null polynomials on $R[\alpha]$.

Also from Theorem 3.5, we obtain a criterion that we will frequently use when two polynomials induce the same polynomial function on the ring of dual numbers.

Corollary 3.7. *Let $f = f_1 + \alpha\, f_2$ and $g = g_1 + \alpha\, g_2$, with $f_1, f_2, g_1, g_2 \in R[x]$.*

$f \triangleq g$ on $R[\alpha]$ if and only if the following three conditions hold:

(1) $[f_1]_R = [g_1]_R$

(2) $[f_1']_R = [g_1']_R$

(3) $[f_2]_R = [g_2]_R$.

In other words, $f \triangleq g$ on $R[\alpha]$ if and only if the following two congruences hold:

(1) $f_1 \equiv g_1 \mod N_R'$

(2) $f_2 \equiv g_2 \mod N_R$.

We use this criterion to exhibit a polynomial with coefficients in R that induces the zero function on R, but not on $R[\alpha]$.

***Example* 3.8.** Let $R = \mathbb{Z}_{p^n}$ and $n < p$. Then the polynomial $(x^p - x)^n$ is a null polynomial on R, but not on $R[\alpha]$. Likewise, $x + (x^p - x)^n$ induces the identity function on R, but not on $R[\alpha]$.

To see that $x \not\triangleq x + (x^p - x)^n$ on $R[\alpha]$, we use Corollary 3.7. Note that

$$(x + (x^p - x)^n)' = 1 + n(x^p - x)^{n-1}(px^{p-1} - 1) \not\equiv 1 = x' \mod N_R.$$

Hence $x \not\equiv x + (x^p - x)^n \mod N_R'$, although $x \equiv x + (x^p - x)^n \mod N_R$.

In a more positive vein, Corollary 3.7 implies that $x \triangleq x + (x^p - x)^n\,\alpha$ on $R[\alpha]$.

Remark 3.9. Let R be a finite commutative ring and $f_1, f_2 \in R[x]$. Then

$$[f_1 + \alpha f_2]_{R[\alpha]} \mapsto (([f_1]_R, [f_1']_R), [f_2]_R)$$

establishes a well-defined bijection

$$\varphi\colon \mathcal{F}(R[\alpha]) \to \{(G,H) \in \mathcal{F}(R) \times \mathcal{F}(R) \mid \exists g \in R[x] \text{ with } G = [g] \text{ and } H = [g']\} \times \mathcal{F}(R)$$

between polynomial functions on $R[\alpha]$ on one hand, and triples of polynomial functions on R such that the first two entries arise from a polynomial and its derivative, on the other hand.

This mapping is well-defined and injective by Corollary 3.7, and it is clearly onto.

Proposition 3.10. *Let R be a finite commutative ring, and let N_R and N_R' be the ideals of* Definition 3.1. *Then the number of polynomial functions on $R[\alpha]$ is*

$$|\mathcal{F}(R[\alpha])| = \big[R[x] : N_R'\big]\,\big[R[x] : N_R\big].$$

Moreover, the factors on the right have the following interpretations.

1. *$[R[x] : N_R']$ is the number of pairs of functions (F, E) with $F\colon R \to R$, $E\colon R \to R$, arising as $([f], [f'])$ for some $f \in R[x]$.*
2. *$[R[x] : N_R']$ is also the number of functions induced on $R[\alpha]$ by polynomials in $R[x]$.*
3. *$[R[x] : N_R]$ is the number of polynomial functions on R.*

Proof. Everything follows from Theorem 3.5. In detail, consider the map φ defined by

$$\varphi\colon R[x] \times R[x] \to \mathcal{F}(R[\alpha]), \quad \varphi(f_1, f_2) = [f_1 + \alpha\, f_2],$$

where $[f_1 + \alpha\, f_2]$ is the function induced on $R[\alpha]$ by $f = f_1 + \alpha\, f_2$. Since every polynomial function on $R[\alpha]$ is induced by a polynomial $f = f_1 + \alpha\, f_2$ with $f_1, f_2 \in R[x]$, φ is onto. Clearly, φ is a homomorphism of the additive groups on each side. By Theorem 3.5, $\ker \varphi = N_R' \times N_R$. Hence, by the first isomorphism theorem,

$$\bar{\varphi}\colon R[x]/N_R' \times R[x]/N_R \to \mathcal{F}(R[\alpha])$$

defined by $\bar{\varphi}(f_1 + N_R', f_2 + N_R) = [f_1 + \alpha\, f_2]$ is a well defined group isomorphism.

Likewise, for (1) let

$$\mathcal{A} = \big\{(F, E) \in \mathcal{F}(R) \times \mathcal{F}(R) \mid \exists f \in R[x] \text{ with } [f] = F \text{ and } [f'] = E\big\},$$

and define $\psi\colon R[x] \to \mathcal{A}$ by $\psi(f) = ([f]_R, [f']_R)$. Then ψ is a group epimorphism with $\ker \psi = N_R'$ and hence $[R[x] : N_R'] = |\mathcal{A}|$.

Finally, (2) follows from Corollary 3.7, and (3) is obvious. □

Proposition 3.10 reduces the question of counting polynomial functions on $R[\alpha]$ to determining $[R[x] : N_R]$ and $[R[x] : N_R']$, that is, to counting polynomial functions on R and pairs of polynomial functions on R induced by a polynomial and its derivative. This will allow us to give explicit formulas for $|\mathcal{F}(R[\alpha])|$ in the case where $R = \mathbb{Z}_{p^n}$ with $n \le p$ in Section 8.

The simple case where R is a finite field we can settle right away by recalling from Example 3.3 that $N_{\mathbb{F}_q} = (x^q - x)\mathbb{F}_q[x]$ and $N_{\mathbb{F}_q}' = (x^q - x)^2\mathbb{F}_q[x]$ and hence $[\mathbb{F}_q[x] : N_{\mathbb{F}_q}'] = q^{2q}$ and $[\mathbb{F}_q[x] : N_{\mathbb{F}_q}] = q$.

Corollary 3.11. *Let $\mathbb{F}_q$ be a field with q elements. Then $|\mathcal{F}(\mathbb{F}_q[\alpha])| = q^{3q}$.*

The remainder of this section is devoted to null polynomials of minimal degree and canonical representations of polynomial functions on $R[\alpha]$ that can be derived from them.

Proposition 3.12. *Let $h_1 \in R[\alpha][x]$ and $h_2 \in R[x]$ be monic null polynomials on $R[\alpha]$ and R, respectively, with $\deg h_1 = d_1$ and $\deg h_2 = d_2$.*

Then every polynomial function $F \colon R[\alpha] \to R[\alpha]$ is induced by a polynomial $f = f_1 + f_2\,\alpha$ with $f_1, f_2 \in R[x]$ such that $\deg f_1 < d_1$ and $\deg f_2 < \min(d_1, d_2)$.

In the special case where F is induced by a polynomial $f \in R[x]$ and, also, h_1 is in $R[x]$, there exists a polynomial $g \in R[x]$ with $\deg g < d_1$, such that $[g]_R = [f]_R$ and $[g']_R = [f']_R$.

Proof. Let $g \in R[\alpha][x]$ be a polynomial that induces F. By division with remainder by h_1, we get $g(x) = q(x)h_1(x) + r(x)$ for some $r, q \in R[\alpha][x]$, where $\deg r < d_1$ and $r(x)$ induces F.

We represent r as $r = r_1 + \alpha\, r_2$ with $r_1, r_2 \in R[x]$. Clearly, $\deg r_1, \deg r_2 < d_1$. If $d_2 < d_1$, then, we divide r_2 by h_2 with remainder in $R[x]$ and get $f_2 \in R[x]$ with $\deg f_2 < d_2$ and such that $f_2 \triangleq r_2$ on R.

By Corollary 3.7, $\alpha\, r_2 \triangleq \alpha\, f_2$ on $R[\alpha]$ and hence, $f = r_1 + \alpha\, f_2$ has the desired properties.

In the special case, the existence of $g \in R[x]$ with $\deg g < d_1$ such that $f \triangleq g$ on $R[\alpha]$ follows by a similar argument. By Corollary 3.7, $[g]_R = [f]_R$ and $[g']_R = [f']_R$. □

In what follows, let m, n be positive integers such that $m > 1$ and p a prime.

Definition 3.13. For $m \in \mathbb{N}$ let $\mu(m)$ denote the smallest positive integer k such that m divides $k!$. The function $\mu \colon \mathbb{N} \to \mathbb{N}$ was introduced by Kempner [16].

When $n \le p$, clearly $\mu(p^n) = np$. We use this fact frequently, explicitly and sometimes implicitly.

Remark 3.14. It is easy to see that m divides the product of any $\mu(m)$ consecutive integers.

As Kempner [17] remarked, it follows that for any $c \in \mathbb{Z}$,

$$(x-c)_{\mu(m)} = \prod_{j=0}^{\mu(m)-1} (x-c-j)$$

is a null polynomial on $\mathbb{Z}_m$.

Theorem 3.15. *Let $m > 1$. Then*

(1) $(x)_{2\mu(m)}$ *is a null polynomial on* $\mathbb{Z}_m[\alpha]$

(2) $((x)_{\mu(m)})^2$ *is a null polynomial on* $\mathbb{Z}_m[\alpha]$.

Proof. Set $f(x) = (x)_{2\mu(m)}$. In view of Lemma 3.4, we must show that f and f' are null polynomials on $\mathbb{Z}_m$. Clearly, f is a null polynomial on $\mathbb{Z}_m$. Now consider $f'(x) = \sum\limits_{i=0}^{2\mu(m)-1} \frac{(x)_{2\mu(m)}}{x-i}$. Each term $\frac{(x)_{2\mu(m)}}{x-i}$ is divisible by a polynomial of the form $\prod\limits_{j=0}^{\mu(m)-1}(x-c-j)$. Thus $\frac{(x)_{2\mu(m)}}{x-i}$ is a null polynomial on $\mathbb{Z}_m$ by Remark 3.14. Hence f' is a null polynomial on $\mathbb{Z}_m$. The proof of the second statement is similar. □

In the case when $m = p^n$, $(x)_{2\mu(p^n)}$ is a null polynomial on $\mathbb{Z}_{p^n}[\alpha]$. When $n \le p$, this says $(x)_{2np}$ is a null polynomial on $\mathbb{Z}_{p^n}[\alpha]$, but in this case more is true, namely, $(x)_{\mu(p^n)+p} = (x)_{(n+1)p}$ is a null polynomial on $\mathbb{Z}_{p^n}[\alpha]$.

Proposition 3.16. *Let $n \le p$. Then $(x)_{(n+1)p}$ is a null polynomial on $\mathbb{Z}_{p^n}[\alpha]$.*

Proof. Since $n \leq p$, we have $\mu(p^n) = np$. Set $f(x) = (x)_{\mu(p^n)+p}$. Then clearly, f is a null polynomial on $\mathbb{Z}_{p^n}$. We represent $f(x)$ as a product of $n+1$ polynomials, each of which has p consecutive integers as roots and is, therefore, a null-polynomial modulo p:

$$(x)_{(n+1)p} = \prod_{l=0}^{n} \prod_{k=lp}^{(l+1)p-1} (x-k).$$

Now regarding $f'(x) = \sum\limits_{i=0}^{(n+1)p-1} \frac{(x)_{(n+1)p}}{x-i}$, it becomes apparent that each term $\frac{(x)_{(n+1)p}}{x-i}$ is divisible by a product of n different polynomials of the form $\prod\limits_{j=0}^{p-1}(x-c-j)$. Hence the claim follows. □

Combining Theorem 3.15 with Proposition 3.12 and Remark 3.14, we obtain the following corollary, which will be needed to establish a canonical form for a polynomial representation of a polynomial function on $\mathbb{Z}_{p^n}[\alpha]$ for $n \leq p$ (see Theorems 9.2 and 9.4).

Corollary 3.17. *Let $F\colon \mathbb{Z}_m[\alpha] \to \mathbb{Z}_m[\alpha]$ be a polynomial function. Then F can be represented as a polynomial $f \in \mathbb{Z}_m[\alpha][x]$ with $\deg f \leq 2\mu(m) - 1$. Moreover, f can be chosen such that $f = f_1 + f_2\,\alpha$, with $f_1, f_2 \in \mathbb{Z}_m[x]$, $\deg f_1 \leq 2\mu(m) - 1$ and $\deg f_2 \leq \mu(m) - 1$.*

When $R = \mathbb{F}_q$ is a finite field, we have already remarked in Corollary 3.11 that the number of polynomial functions on $\mathbb{F}_q[\alpha]$ is q^{3q}. We can make this more explicit by giving a canonical representation for the different polynomial functions on $\mathbb{F}_q[\alpha]$.

Corollary 3.18. *Let $\mathbb{F}_q$ be a finite field with q elements. Every polynomial function $F\colon \mathbb{F}_q[\alpha] \to \mathbb{F}_q[\alpha]$ can be represented uniquely as a polynomial*

$$f(x) = \sum_{i=0}^{2q-1} a_i x^i + \sum_{j=0}^{q-1} b_j x^j\,\alpha \qquad \text{for } a_i, b_j \in \mathbb{F}_q. \tag{3.1}$$

Proof. We note that the polynomials $(x^q - x)^2$ and $(x^q - x)$ satisfy the conditions of Proposition 3.12. Thus every polynomial function on $\mathbb{F}_q[\alpha]$ is represented by a polynomial as in Equation (3.1).

Since there are exactly q^{3q} different polynomials of the form (3.1) and also, by Corollary 3.11, q^{3q} different polynomial functions on $\mathbb{F}_q[\alpha]$, every polynomial function is represented uniquely.

We can also show uniqueness directly, without using Corollary 3.11, by demonstrating that every expression of type (3.1) representing the zero function is the zero polynomial. Let $f \in \mathbb{F}_q[\alpha][x]$ be a null polynomial on $\mathbb{F}_q[\alpha]$ with $f(x) = \sum\limits_{i=0}^{2q-1} a_i x^i + \sum\limits_{j=0}^{q-1} b_j x^j\,\alpha$.

Then $\sum\limits_{i=0}^{2q-1} a_i x^i \in N'_{\mathbb{F}_q}$ and $\sum\limits_{j=0}^{q-1} b_j x^j \in N_{\mathbb{F}_q}$ by Theorem 3.5. Recalling from Example 3.3 that $N'_{\mathbb{F}_q} = (x^q - x)^2\mathbb{F}_q[x]$ and $N_{\mathbb{F}_q} = (x^q - x)\mathbb{F}_q[x]$, we see that $a_i = 0$ for $i = 0, \ldots, 2q-1$; and $b_j = 0$ for $j = 0, \ldots, q-1$. □

4. Permutation polynomials on $R[\alpha]$

We know direct our attention to permutation polynomials on $R[\alpha]$, where $R[\alpha]$ is the ring of dual numbers over a finite commutative ring R (defined in Definition 2.4). As in the previous section, we first relate properties of polynomials in $R[\alpha][x]$ to properties of polynomials in $R[x]$, about which more may be known.

Theorem 4.1. *Let R be a commutative ring. Let $f = f_1 + \alpha\, f_2$, where $f_1, f_2 \in R[x]$. Then f is a permutation polynomial on $R[\alpha]$ if and only if the following conditions hold:*

(1) *f_1 is a permutation polynomial on R*

(2) *for all $a \in R$, $f_1'(a)$ is a unit of R.*

Proof. ($\Rightarrow$) To see (1), let $c \in R$. Since f is a permutation polynomial on $R[\alpha]$, there exist $a, b \in R$ such that $c = f(a + b\,\alpha)$, that is, $c = f_1(a) + (bf_1'(a) + f_2(a))\,\alpha$ (by Lemma 2.7). In particular, $f_1(a) = c$, and, therefore, $[f_1]_R$ is onto and hence a permutation of R.

To see (2), let $a \in R$ and suppose that $f_1'(a)$ is not a unit of R. R being finite, it follows that $f_1'(a)$ is a zerodivisor of R. Let $b \in R$, $b \neq 0$, such that $bf_1'(a) = 0$. Then

$$f(a + b\,\alpha) = f_1(a) + (bf_1'(a) + f_2(a))\,\alpha = f_1(a) + f_2(a)\,\alpha = f(a).$$

So f is not one-to-one; a contradiction.

($\Leftarrow$) Assume (1) and (2) hold. It suffices to show that $[f]_{R[\alpha]}$ is one-to-one. Let $a, b, c, d \in R$ such that $f(a + b\,\alpha) = f(c + d\,\alpha)$, that is,

$$f_1(a) + (bf_1'(a) + f_2(a))\,\alpha = f_1(c) + (df_1'(c) + f_2(c))\,\alpha\,.$$

Then $f_1(a) = f_1(c)$ and hence $a = c$, by (1). Furthermore, $bf_1'(a) = df_1'(a)$, and, since $f_1'(a)$ is not a zerodivisor, $b = d$ follows. □

The special case of polynomials with coefficients in R is so important that we state it separately.

We call a function on R that maps every element of R to a unit of R a *unit-valued* function on R.

Corollary 4.2. *Let R be a commutative ring and $f \in R[x]$. Then f is a permutation polynomial on $R[\alpha]$ if and only if the following two conditions hold:*

(1) *$[f]_R$ is a permutation of R*

(2) *$[f']_R$ is unit-valued.*

Theorem 4.1 shows that whether $f = f_1 + \alpha\, f_2 \in R[\alpha][x]$ is a permutation polynomial on $R[\alpha]$ depends only on f_1. In particular, $f_1 + \alpha\, f_2$ is a permutation polynomial on $R[\alpha]$ if and only if $f_1 + \alpha \cdot 0$ is a permutation polynomial on $R[\alpha]$. We rephrase the last remark as a corollary.

Corollary 4.3. *Let R be a finite ring. Let $f = f_1 + \alpha\, f_2$, where $f_1, f_2 \in R[x]$. Then f is a permutation polynomial on $R[\alpha]$ if and only if f_1 is a permutation polynomial on $R[\alpha]$.*

Corollary 4.4. *Let R be a finite ring and R^* the group of units on R. Let B denote the number of pairs of functions (H, G) with*

$$H\colon R \to R \text{ bijective} \qquad \text{and} \qquad G\colon R \to R^*$$

that occur as $([g], [g'])$ for some $g \in R[x]$. Then the number $|\mathcal{P}(R[\alpha])|$ of polynomial permutations on $R[\alpha]$ is equal to

$$|\mathcal{P}(R[\alpha])| = B \cdot |\mathcal{F}(R)|.$$

Proof. By Corollary 3.7 and Remark 3.9,

$$[f_1 + \alpha f_2]_{R[\alpha]} \mapsto ([f_1]_R, [f_1']_R, [f_2]_R)$$

is a bijection between $\mathcal{F}(R[\alpha])$ and triples of polynomial functions on R such that the first two entries of the triple arise from one polynomial and its derivative.

By Theorem 4.1, the restriction of this bijection to $\mathcal{P}(R[\alpha])$ is surjective onto the set of those triples $([f_1]_R, [f_1']_R, [f_2]_R)$ such that $[f_1]_R$ is bijective and $[f_1']_R$ takes values in R^*. □

We now introduce a subgroup of the group of polynomial permutations of a ring of dual numbers that will play an important role in determining the order of the group.

Definition 4.5. Let

$$St_\alpha(R) = \{F \in \mathcal{P}(R[\alpha]) \mid F(a) = a \text{ for every } a \in R\}.$$

$St_\alpha(R)$, which is clearly a subgroup of $\mathcal{P}(R[\alpha])$, is called the pointwise stabilizer (or shortly the stabilizer) of R in the group $\mathcal{P}(R[\alpha])$.

Proposition 4.6. *Let R be a finite commutative ring. Then*

$$St_\alpha(R) = \{F \in \mathcal{P}(R[\alpha]) \mid F \text{ is induced by } x + h(x),\ \text{for some } h \in N_R\}.$$

In particular, every element of the stabilizer of R can be realized by a polynomial in $R[x]$.

Proof. It is clear that

$$St_\alpha(R) \supseteq \{F \in \mathcal{P}(R[\alpha]) \mid F \text{ is induced by } x + h(x),\ \text{for some } h \in N_R\}.$$

Now, let $F \in \mathcal{P}(R[\alpha])$ such that $F(a) = a$ for every $a \in R$. Then F is represented by $f_1 + f_2\,\alpha$, where $f_1, f_2 \in R[x]$, and $a = F(a) = f_1(a) + f_2(a)\,\alpha$ for every $a \in R$. It follows that $f_2(a) = 0$ for every $a \in R$, i.e., f_2 is a null polynomial on R. Thus, $f_1 + f_2\,\alpha \triangleq f_1$ on $R[\alpha]$ by Lemma 2.7, that is, F is represented by f_1. Therefore, $[f_1]_R = \mathrm{id}_R$ (since F is the identity on R) and, so, $f_1(x) = x + h(x)$ for some $h \in R[x]$ that is a null polynomial on R. □

Remark 4.7. To prevent confusion about the expression for the stabilizer group in Proposition 4.6, we emphasize that, in general, not every polynomial of the form $x + h$ with $h \in N_R$ induces a polynomial permutation of $R[\alpha]$, as the following example shows.

***Example* 4.8.** Let $R = \mathbb{F}_q$. Consider the polynomial $(x^q - x) \in N_{\mathbb{F}_q}$. Then the polynomial $f(x) = x + (x^q - x) = x^q$ induces the identity on $\mathbb{F}_q$, but f is not a permutation polynomial on $\mathbb{F}_q[\alpha]$, since $f(\alpha) = f(0) = 0$. Thus f does not induce an element of $St_\alpha(\mathbb{F}_q)$.

The remainder of this section is concerned with polynomial permutations of the ring of dual numbers in the simple case where the base ring is a finite field. We already determined the number of polynomial functions on the dual ring over a finite field (see Corollary 3.11). The number of polynomial permutations now follows readily from Corollary 4.4, since every pair of functions on a finite field arises as the pair of functions induced by a polynomial and its derivative.

Lemma 4.9. *Let $\mathbb{F}_q$ be a finite field with q elements. Then for all functions $F, G\colon \mathbb{F}_q \to \mathbb{F}_q$ there exists a polynomial $f \in \mathbb{F}_q[x]$ such that*

$$(F, G) = ([f], [f']) \quad \textit{and} \quad \deg f < 2q.$$

Proof. Let $f_0, f_1 \in \mathbb{F}_q[x]$ such that $[f_0] = F$ and $[f_1] = G$ and set

$$f(x) = f_0(x) + (f_0'(x) - f_1(x))(x^q - x).$$

Then $[f] = [f_0] = F$ and $[f'] = [f_1] = G$. Moreover, by division with remainder by $(x^q - x)$, we can find f_0, f_1 such that $\deg f_0, \deg f_1 < q$. □

Proposition 4.10. *Let $\mathbb{F}_q$ be a finite field with q elements. The number $|\mathcal{P}(\mathbb{F}_q[\alpha])|$ of polynomial permutations on $\mathbb{F}_q[\alpha]$ is given by*

$$|\mathcal{P}(\mathbb{F}_q[\alpha])| = q!(q-1)^q q^q.$$

Proof. Let $\mathcal{B}$ be the set of pairs of functions (H, G) such that

$$H\colon \mathbb{F}_q \to \mathbb{F}_q \text{ bijective} \qquad \text{and} \qquad G\colon \mathbb{F}_q \to \mathbb{F}_q \setminus \{0\}.$$

Clearly, $|\mathcal{B}| = q!(q-1)^q$. By Lemma 4.9, each $(H, G) \in \mathcal{B}$ arises as $([f], [f'])$ for some $f \in \mathbb{F}_q[x]$. Thus by Corollary 4.4, $|\mathcal{P}(\mathbb{F}_q[\alpha])| = |\mathcal{B}| \cdot |\mathcal{F}(\mathbb{F}_q)| = q!(q-1)^q q^q$. □

When R is a finite field, then, as we have seen, we do not need the stabilizer group to determine the number of polynomial permutations on the ring of dual numbers. We will nevertheless investigate this group, starting with its order, for comparison purposes, and because it yields some information on the structure of $\mathcal{P}(\mathbb{F}_q[\alpha])$.

Theorem 4.11. *Let $\mathbb{F}_q$ be a finite a field with q elements. Then*

(1) $|St_\alpha(\mathbb{F}_q)| = |\{[f']_{\mathbb{F}_q} \mid f \in \mathbb{F}_q[x],\ [f]_{\mathbb{F}_q} = \mathrm{id}_{\mathbb{F}_q}$ *and* $[f']_{\mathbb{F}_q}$ *is unit-valued*$\}|$

(2) $|St_\alpha(\mathbb{F}_q)| = |\{[f']_{\mathbb{F}_q} \mid f \in \mathbb{F}_q[x],\ [f]_{\mathbb{F}_q} = \mathrm{id}_{\mathbb{F}_q},\ \deg f < 2q$ *and* $[f']_{\mathbb{F}_q}$ *is unit-valued*$\}|$

(3) $|St_\alpha(\mathbb{F}_q)| = (q-1)^q$.

Proof. To see (1), set $A = \{[f']_{\mathbb{F}_q} \mid f \in \mathbb{F}_q[x],\ [f]_{\mathbb{F}_q} = \mathrm{id}_{\mathbb{F}_q}$ and $[f']_{\mathbb{F}_q}$ is unit-valued$\}$. We define a bijection φ from $St_\alpha(\mathbb{F}_q)$ to A. Given $F \in St_\alpha(\mathbb{F}_q)$, there exists a polynomial $f \in \mathbb{F}_q[x]$ inducing F on $\mathbb{F}_q[\alpha]$ such that $[f]_{\mathbb{F}_q} = \mathrm{id}_{\mathbb{F}_q}$ by Definition 4.5. By Theorem 4.1, $[f']_{\mathbb{F}_q}$ is unit-valued. We set $\varphi(F) = [f']_{\mathbb{F}_q}$. Corollary 3.7 shows that φ is well-defined and injective, and Theorem 4.1 shows that it is surjective.

(2) follows from (1) and Lemma 4.9. Ad (3). By (1), $|St_\alpha(\mathbb{F}_q)| \le |\{G\colon \mathbb{F}_q \to \mathbb{F}_q^*\}| = (q-1)^q$. Now consider a function $G\colon \mathbb{F}_q \to \mathbb{F}_q^*$. By Lemma 4.9, there exists a polynomial $h \in \mathbb{F}_q[x]$ such that $[h]_{\mathbb{F}_q} = \mathrm{id}_{\mathbb{F}_q}$ and $[h']_{\mathbb{F}_q} = G$. Thus h represents an element of $St_\alpha(\mathbb{F}_q)$, and G maps to this element under the bijection φ in the proof of (1). Hence $|St_\alpha(\mathbb{F}_q)| \ge (q-1)^q$. □

The equalities of Theorem 4.11 actually come from a group isomorphism, as the second author has shown [1]. By Proposition 4.10 and Theorem 4.11, we immediately see the special case for finite fields of a more general result that we will show in the next section (see Theorem 5.7).

Corollary 4.12. *The number $|\mathcal{P}(\mathbb{F}_q[\alpha])|$ of polynomial permutations on $\mathbb{F}_q[\alpha]$ is given by*

$$|\mathcal{P}(\mathbb{F}_q[\alpha])| = |\mathcal{P}(\mathbb{F}_q)||\mathcal{F}(\mathbb{F}_q)||St_\alpha(\mathbb{F}_q)|.$$

5. The stabilizer of R in the group of polynomial permutations of $R[\alpha]$

In this section we express the numbers of polynomial functions and polynomial permutations on $R[\alpha]$ in terms of the order of $St_\alpha(R)$, the stabilizer of R, that is, the group of those polynomial permutations of $R[\alpha]$ that fix R pointwise. The group of those polynomial permutations of $R[\alpha]$ that can be realized by polynomials with coefficients in R will play a role, as it contains the stabilizer.

Notation 5.1. Let $\mathcal{P}_R(R[\alpha]) = \{F \in \mathcal{P}(R[\alpha]) \mid F = [f]$ for some $f \in R[x]\}$.

Remark 5.2. Proposition 4.6 shows that the elements of $St_\alpha(R)$, a priori induced by polynomials in $R[\alpha][x]$, can be realized by polynomials in $R[x]$, that is,

$$St_\alpha(R) \subseteq \mathcal{P}_R(R[\alpha]).$$

The following well-known, useful characterization of permutation polynomials on finite local rings has been shown by Nöbauer [23: section III, statement 6, p. 335] (also for several variables [23: Theorem 2.3]). It is implicitly shown in the proof of a different result in McDonalds's monograph on finite rings [19: pp. 269–272], and explicitly in a paper of Nechaev [20: Theorem 3].

Lemma 5.3 ([23: Theorem. 2.3])**.** *Let R be a finite local ring, not a field, M its maximal ideal, and $f \in R[x]$.*

Then f is a permutation polynomial on R if and only if the following conditions hold:

(1) *f is a permutation polynomial on R/M*

(2) *for all $a \in R$, $f'(a) \neq 0 \mod M$.*

Lemma 5.4. *Let R be a finite commutative ring and $F \in \mathcal{P}(R)$. Then there exists a polynomial $f \in R[x]$ such that $[f]_R = F$ and $f'(r)$ is a unit of R for every $r \in R$.*

Proof. Since every finite commutative ring is a direct sum of local rings, we may assume R local. When R is a finite field, the statement follows from Lemma 4.9, while, when R is a finite local ring but not a field, it follows from Lemma 5.3. □

Lemma 5.5. *$\mathcal{P}_R(R[\alpha])$ is a subgroup of $\mathcal{P}(R[\alpha])$; and the map*

$$\varphi\colon \mathcal{P}_R(R[\alpha]) \to \mathcal{P}(R) \quad \textit{defined by} \quad F \mapsto F\big|_R \quad \textit{(the restriction of } F \textit{ to } R\textit{)}$$

is a group epimorphism with $\ker\varphi = St_\alpha(R)$. In particular,

(1) *every element of $\mathcal{P}(R)$ occurs as the restriction to R of some $F \in \mathcal{P}_R(R[\alpha])$*

(2) *$\mathcal{P}_R(R[\alpha])$ contains $St_\alpha(R)$ as a normal subgroup and*

$$\mathcal{P}_R(R[\alpha])\big/ St_\alpha(R) \;\cong\; \mathcal{P}(R).$$

Proof. $\mathcal{P}_R(R[\alpha])$ is a finite subset of $\mathcal{P}(R)$ that is closed under composition, and hence a subgroup of $\mathcal{P}(R)$. Polynomial permutations of $R[\alpha]$ induced by polynomials in $R[x]$ map R to itself bijectively. The map φ is therefore well defined, and clearly a homomorphism with respect to composition of functions.

Ad (1) This is evident from Theorem 4.1 and Lemma 5.4.

Ad (2) $St_\alpha(R)$ is contained in $\mathcal{P}_R(R[\alpha])$, by Proposition 4.6. $St_\alpha(R)$, the pointwise stabilizer of R in $\mathcal{P}(R[\alpha])$ is, therefore, equal to the pointwise stabilizer of R in $\mathcal{P}_R(R[\alpha])$, which is the kernel of φ. □

Recall that a function on R is unit-valued if it maps R into, R^*, the group of units on R.

Corollary 5.6. *For any fixed $F \in \mathcal{P}(R)$,*

$$|St_\alpha(R)| = |\{([f]_R, [f']_R) \mid f \in R[x], \qquad [f]_R = F, \ \textit{and } [f']_R \textit{ is unit-valued}\}|\,.$$

Proof. Let $f \in R[x]$ such that $[f]_R = F$ and $[f']_R$ is unit-valued. Such a polynomial f exists by Lemma 5.4. By Corollary 4.2, f induces a permutation of $R[\alpha]$, which we denote by $[f]$.

Let C be the coset of $[f]$ with respect to $St_\alpha(R)$. Then $|C| = |St_\alpha(R)|$. By Lemma 5.5 (2), C consists precisely of those polynomial permutations $G \in \mathcal{P}_R(R[\alpha])$ with $G\big|_R = F$.

A bijection ψ between C on one hand and the set of pairs $([g]_R, [g']_R)$, where $g \in R[x]$ such that $[g]_R = F$ and $[g']_R$ is unit-valued on the other hand is given by $\psi(G) = ([g]_R, [g']_R)$, where g is any polynomial in $R[x]$ which induces G on $R[\alpha]$. The map ψ is well-defined and injective by Corollary 3.7 and onto by Corollary 4.2. □

Theorem 5.7. *Let R be a finite local ring. Then*

$$|\mathcal{P}(R[\alpha])| = |\mathcal{F}(R)| \cdot |\mathcal{P}(R)| \cdot |St_\alpha(R)|.$$

Proof. Set

$$B = \{([f]_R, [f']_R) \mid f \in R[x],\ [f]_R \in P(R) \text{ and } [f']_R \text{ is unit-valued}\}.$$

By Corollary 5.6, $|B| = |\mathcal{P}(R)| \cdot |St_\alpha(R)|$.

We define a function $\psi\colon \mathcal{P}(R[\alpha]) \to B \times \mathcal{F}(R)$ as follows: if $G \in \mathcal{P}(R[\alpha])$ is induced by $g = g_1 + \alpha\, g_2$, where $g_1, g_2 \in R[x]$, we let $\psi(G) = (([g_1]_R, [g_1']_R), [g_2]_R)$. By Theorem 4.1 and Corollary 3.7, ψ is well-defined and one-to-one. The surjectivity of ψ follows by Theorem 4.1. Therefore,

$$|\mathcal{P}(R[\alpha])| = |B \times \mathcal{F}(R)| = |\mathcal{P}(R)| \cdot |St_\alpha(R)| \cdot |\mathcal{F}(R)|. \qquad \square$$

Remark 5.8. Let R be a finite local ring which is not a field, M the maximal ideal of R, and $q = |R/M|$. Jiang [13] has shown the following relation between the number of polynomial functions and the number of polynomial permutations on R:

$$|\mathcal{P}(R)| = \frac{q!(q-1)^q}{q^{2q}} |\mathcal{F}(R)|.$$

Corollary 5.9. *Let R be a finite local ring which is not a field. Then*

$$|\mathcal{F}(R[\alpha])| = |\mathcal{F}(R)|^2 \cdot |St_\alpha(R)|.$$

Proof. The residue fields of R and $R[\alpha]$ are isomorphic by Proposition 2.6 (4). Let q denote the order of this residue field. By Theorem 5.7, $|\mathcal{P}(R[\alpha])| = |\mathcal{F}(R)| \cdot |\mathcal{P}(R)| \cdot |St_\alpha(R)|$. Now apply Remark 5.8 to $\mathcal{P}(R[\alpha])$ and $\mathcal{P}(R)$ simultaneously and cancel. □

6. Permutation polynomials on $\mathbb{Z}_m[\alpha]$

In this section we characterize permutation polynomials on $\mathbb{Z}_{p^n}[\alpha]$ in relation to permutation polynomials on $\mathbb{Z}_{p^n}$.

Lemma 6.1 ([25: Hilfssatz 8]). *Let $n > 1$, and $f \in \mathbb{Z}[x]$. Then f is a permutation polynomial on $\mathbb{Z}_{p^n}$ if and only if the following conditions hold:*

(1) *f is a permutation polynomial on $\mathbb{Z}_p$*

(2) *for all $a \in \mathbb{Z}$, $f'(a) \not\equiv 0 \pmod p$.*

We now apply the principle of Lemma 6.1 to Theorem 4.1 and Corollary 4.3 in the special case where $R = \mathbb{Z}_{p^n}$.

Theorem 6.2. *Let $f \in \mathbb{Z}[\alpha][x]$, $f = f_1 + \alpha f_2$ with $f_1, f_2 \in \mathbb{Z}[x]$. Then the following statements are equivalent:*

(1) *f is a permutation polynomial on $\mathbb{Z}_{p^n}[\alpha]$ for all $n \geq 1$*

(2) *f is a permutation polynomial on $\mathbb{Z}_{p^n}[\alpha]$ for some $n \geq 1$*

(3) *f_1 is a permutation polynomial on $\mathbb{Z}_{p^n}[\alpha]$ for all $n \geq 1$*

(4) *f_1 is a permutation polynomial on $\mathbb{Z}_{p^n}[\alpha]$ for some $n \geq 1$*

(5) *f_1 is a permutation polynomial on $\mathbb{Z}_p$ and for all $a \in \mathbb{Z}$, $f_1'(a) \not\equiv 0 \pmod p$*

(6) *f_1 is a permutation polynomial on $\mathbb{Z}_{p^n}$ for all $n \geq 1$*

(7) *f_1 is a permutation polynomial on $\mathbb{Z}_{p^n}$ for some $n > 1$.*

Proof. By Corollary 4.3, (1) is equivalent to (3), and (2) is equivalent to (4). By Lemma 6.1, the statements (5), (6) and (7) are equivalent.

By Theorem 4.1, (1) is equivalent to (6) together with the fact that $f_1'(a) \not\equiv 0 \pmod{p}$ for any $a \in \mathbb{Z}$. But Lemma 6.1 shows that the condition on the derivative of f_1 is redundant. Therefore, (1) is equivalent to (6).

(1) implies (2) a fortiori. Finally, taking into account the fact that a permutation polynomial on $\mathbb{Z}_{p^n}$ is also a permutation polynomial on $\mathbb{Z}_p$, Theorem 4.1 shows that (2) implies (5). □

The special case $f = f_1$ yields the following corollary.

Corollary 6.3. *Let $f \in \mathbb{Z}[x]$. Then the following statements are equivalent:*

(1) *f is a permutation polynomial on $\mathbb{Z}_{p^n}[\alpha]$ for all $n \geq 1$*

(2) *f is a permutation polynomial on $\mathbb{Z}_{p^n}[\alpha]$ for some $n \geq 1$*

(3) *f is a permutation polynomial on $\mathbb{Z}_p$ and for all $a \in \mathbb{Z}$, $f'(a) \not\equiv 0 \pmod{p}$*

(4) *f is a permutation polynomial on $\mathbb{Z}_{p^n}$ for all $n \geq 1$*

(5) *f is a permutation polynomial on $\mathbb{Z}_{p^n}$ for some $n > 1$.*

We exploit the equivalence of being a permutation polynomial on $\mathbb{Z}_{p^n}[\alpha]$ and being a permutation polynomial on $\mathbb{Z}_{p^n}$ (only valid for $n > 1$) in the following corollary, always keeping in mind that being a null-polynomial on $\mathbb{Z}_{p^n}$ is not equivalent to being a null-polynomial on $\mathbb{Z}_{p^n}[\alpha]$.

Corollary 6.4. *Let $n > 1$, and $f, g \in \mathbb{Z}[x]$.*

(1) *If f is a permutation polynomial on $\mathbb{Z}_{p^n}$ and g a null polynomial on $\mathbb{Z}_{p^n}$ then $f + g$ is a permutation polynomial on $\mathbb{Z}_{p^n}[\alpha]$.*

(2) *In particular, if g is a null-polynomial on $\mathbb{Z}_{p^n}$, $x + g$ induces an element of $St_\alpha(\mathbb{Z}_{p^n})$.*

Proof. Ad (1). Set $h = f + g$. Then $[h]_{p^n} = [f]_{p^n}$ and h is, therefore, a permutation polynomial on $\mathbb{Z}_{p^n}$. Since $n > 1$, Corollary 6.3 applies and $h(x)$ is a permutation polynomial on $\mathbb{Z}_{p^n}[\alpha]$. Now (2) follows from (1) and Definition 4.5. □

The following example illustrates the necessity of the condition $n > 1$ in Theorem 6.2 (7) and Corollary 6.4.

***Example* 6.5.** Consider the polynomials $f(x) = (p-1)x$ and $g(x) = (p-1)(x^p - x)$. Clearly, f is a permutation polynomial on both $\mathbb{Z}_p$ and $\mathbb{Z}_p[\alpha]$, while $g(x)$ is a null polynomial on $\mathbb{Z}_p$. Now, $h(x) = f(x) + g(x) = (p-1)x^p$ permutes the elements of $\mathbb{Z}_p$, but h is not a permutation polynomial on $\mathbb{Z}_p[\alpha]$, as $h(\alpha) = h(0) = 0$.

We can apply the Chinese Remainder Theorem to Theorem 6.2 and Corollary 6.4 to obtain statements about permutation polynomials on $\mathbb{Z}_m[\alpha]$.

Theorem 6.6. *Let $f = f_1 + \alpha f_2$ with $f_1, f_2 \in \mathbb{Z}[x]$. Then f is a permutation polynomial on $\mathbb{Z}_m[\alpha]$ if and only if for every prime p dividing m, f_1 is a permutation polynomial on $\mathbb{Z}_p$ and f_1' has no zero modulo p.*

Corollary 6.7. *Let $m = p_1^{n_1} \cdots p_k^{n_k}$, where $p_1, \ldots, p_k$ are distinct primes and $n_j > 1$ for $j = 1, \ldots, k$. Let $f, g \in \mathbb{Z}[x]$. If f is a permutation polynomial on $\mathbb{Z}_m$ and g a null polynomial on $\mathbb{Z}_m$ then $f + g$ is a permutation polynomial on $\mathbb{Z}_m[\alpha]$. In particular, for every null polynomial g on $\mathbb{Z}_m$, $x + g$ induces an element of $St_\alpha(\mathbb{Z}_m)$.*

7. The stabilizer of $\mathbb{Z}_{p^n}$ in the group of polynomial permutations of $\mathbb{Z}_{p^n}[\alpha]$

Recall from Definition 4.5 that $St_\alpha(\mathbb{Z}_m)$ denotes the pointwise stabilizer of $\mathbb{Z}_m$ in the group of polynomial permutations on $\mathbb{Z}_m[\alpha]$. We have seen in Theorem 5.7 the importance of this subgroup for counting polynomial functions and polynomial permutations on $\mathbb{Z}_m[\alpha]$. The somewhat technical results on $St_\alpha(\mathbb{Z}_m)$ that we develop in this section will allow us to determine its order and, from that, to derive explicit formulas for the number of polynomial functions polynomial and permutations on $\mathbb{Z}_{p^n}[\alpha]$ for $n \leq p$ in Section 8.

We have already defined the ideal of null-polynomials and the ideal of polynomials that are null together with their first derivative in Section 3 (Definition 3.1). For counting purposes, we now pay special attention to the degrees of the polynomials inducing the null function. We are interested in the case of $R = \mathbb{Z}_{p^n}$ for $n > 1$ (finite fields having been covered already).

Definition 7.1. Let

$$N_{\mathbb{Z}_m}(< k) = \{f \in \mathbb{Z}_m[x] \mid f \in N_{\mathbb{Z}_m} \text{ and } \deg f < k\},$$
$$N'_{\mathbb{Z}_m}(< k) = \{f \in \mathbb{Z}_m[x] \mid f \in N'_{\mathbb{Z}_m} \text{ and } \deg f < k\}.$$

Recall from Definition 2.2 that $[f]_m$, short for $[f]_{\mathbb{Z}_m}$, denotes the polynomial function induced by f on $\mathbb{Z}_m$.

Proposition 7.2. *Let $m = p_1^{n_1} \cdots p_l^{n_l}$, where $p_1, \dots, p_l$ are distinct primes and suppose that $n_j > 1$ for $j = 1, \dots, l$. Then*

(1) $|St_\alpha(\mathbb{Z}_m)| = |\{[f']_m \mid f \in N_{\mathbb{Z}_m}\}|$

(2) *if there exists a monic polynomial in $\mathbb{Z}[x]$ of degree k that is a null polynomial on $\mathbb{Z}_m[\alpha]$, then*

   (a) $|St_\alpha(\mathbb{Z}_m)| = |\{[f']_m \mid f \in N_{\mathbb{Z}_m} \text{ with } \deg f < k\}|$

   (b) $|St_\alpha(\mathbb{Z}_m)| = [N_{\mathbb{Z}_m} : N'_{\mathbb{Z}_m}] = \frac{|N_{\mathbb{Z}_m}(<k)|}{|N'_{\mathbb{Z}_m}(<k)|}$.

Proof. Ad (1). We define a bijection φ from $St_\alpha(\mathbb{Z}_m)$ to the set of functions induced on $\mathbb{Z}_m$ by the derivatives of null polynomials on $\mathbb{Z}_m$. Given $F \in St_\alpha(\mathbb{Z}_m)$, let $h \in \mathbb{Z}[x]$ be (such as we know to exist by Proposition 4.6) a null polynomial on $\mathbb{Z}_m$ such that $x + h(x)$ induces F. We set $\varphi(F) = [h']_m$. Now Corollary 3.7 shows φ to be well-defined and injective, and Corollary 6.7 shows it to be surjective.

Ad (2a). If $g \in N_{\mathbb{Z}_m}$, then by Proposition 3.12, there exists $f \in \mathbb{Z}_m[x]$ with $\deg f < k$ such that $[f]_m = [g]_m$ (that is, $f \in N_{\mathbb{Z}_m}$) and $[f']_m = [g']_m$.

Ad (2b). Define $\varphi \colon N_{\mathbb{Z}_m} \to \mathcal{F}(\mathbb{Z}_m)$ by $\varphi(f) = [f']_m$. Clearly, φ is a homomorphism of additive groups. Furthermore, $\ker \varphi = N'_{\mathbb{Z}_m}$ and $\operatorname{Im} \varphi = \{[f']_m \mid f \in N_{\mathbb{Z}_m}\}$. By (1),

$$|St_\alpha(\mathbb{Z}_m)| = [N_{\mathbb{Z}_m} : N'_{\mathbb{Z}_m}].$$

For evaluating the ratio, we restrict φ to the additive subgroup of $\mathbb{Z}_m[x]$ consisting of polynomials of degree less than k and get a homomorphism of additive groups defined on $N_{\mathbb{Z}_m}(< k)$, whose image is still $\{[f']_m \mid f \in N_{\mathbb{Z}_m}\}$, by Corollary 3.7, and whose kernel is $N'_{\mathbb{Z}_m}(< k)$. Hence

$$|St_\alpha(\mathbb{Z}_m)| = [N_{\mathbb{Z}_m}(< k) : N'_{\mathbb{Z}_m}(< k)].$$

□

We now substitute concrete numbers from Theorem 3.15 and Proposition 3.16 for the k that stands for the degree of a monic null polynomial on $\mathbb{Z}_m[\alpha]$ in Proposition 7.2 (2). Here, as in Definition 3.13, $\mu(m)$ denotes the smallest positive integer whose factorial is divisible by m.

Corollary 7.3. *Let $m = p_1^{n_1} \cdots p_k^{n_k}$, where $p_1, \dots, p_k$ are distinct primes and suppose that $n_j > 1$ for $j = 1, \dots, k$. Then*

(1) $|St_\alpha(\mathbb{Z}_m)| = |\{[f']_m \mid f \in N_{\mathbb{Z}_m} \text{ with } \deg f < 2\mu(m)\}|$

(2) $|St_\alpha(\mathbb{Z}_m)| = \dfrac{|N_{\mathbb{Z}_m}(< 2\mu(m))|}{|N'_{\mathbb{Z}_m}(< 2\mu(m))|}$.

Corollary 7.4. *For a prime number p and a natural number n, where $1 < n \le p$, we have*

(1) $|St_\alpha(\mathbb{Z}_{p^n})| = |\{[f']_{p^n} \mid f \in N_{\mathbb{Z}_{p^n}} \text{ with } \deg f < (n+1)p\}|$

(2) $|St_\alpha(\mathbb{Z}_{p^n})| = \dfrac{|N_{\mathbb{Z}_{p^n}}(< (n+1)p)|}{|N'_{\mathbb{Z}_{p^n}}(< (n+1)p)|}$.

Remark 7.5. When $m = p$ is a prime, Proposition 7.2 and its Corollaries do not apply. This case has been treated in Theorem 4.11.

We now employ Proposition 7.2 to show that Corollary 5.6 takes a simpler form for polynomial functions on $\mathbb{Z}_{p^n}$, when $n > 1$. (Again, the case $n = 1$ is exceptional, see Theorem 4.11.)

Corollary 7.6. *Let $n > 1$. Then for any fixed $F \in \mathcal{F}(\mathbb{Z}_{p^n})$,*

$$|St_\alpha(\mathbb{Z}_{p^n})| = |\{([f]_{p^n}, [f']_{p^n}) \mid f \in \mathbb{Z}[x] \text{ with } [f]_{p^n} = F\}|.$$

Proof. Set

$$A = \{([f]_{p^n}, [f']_{p^n}) \mid f \in \mathbb{Z}[x] \text{ with } [f]_{p^n} = F\},$$

and fix $f_0 \in \mathbb{Z}[x]$ with $[f_0]_{p^n} = F$. Then, $f - f_0$ is a null polynomial on $\mathbb{Z}_{p^n}$ for any $f \in \mathbb{Z}[x]$ with $([f]_{p^n}, [f']_{p^n}) \in A$.

We define a bijection

$$\phi\colon A \to \{[h']_{p^n} \mid h \in N_{\mathbb{Z}_{p^n}}\}, \qquad \phi(([f]_{p^n}, [f']_{p^n})) = [(f - f_0)']_{p^n}.$$

Since $[(f - f_0)']_{p^n} = [f']_{p^n} - [f_0']_{p^n}$, ϕ is well defined. Also, ϕ is injective, because, for two different elements of A, $([f_1]_{p^n}, [f_1']_{p^n}) \ne ([f]_{p^n}, [f']_{p^n})$ implies $[f_1']_{p^n} \ne [f']_{p^n}$ and hence $[(f_1 - f_0)']_{p^n} \ne [(f - f_0)']_{p^n}$.

To see that ϕ is surjective, consider $[h']_{p^n}$, where $h \in N_{\mathbb{Z}_{p^n}}$. Then $[f_0 + h]_{p^n} = F$ and, therefore, $([f_0 + h]_{p^n}, [f_0' + h']_{p^n})$ is in A and maps to $[h']_{p^n}$ under ϕ.

By Proposition 7.2 (1),

$$|St_\alpha(\mathbb{Z}_{p^n})| = |\{[f']_{p^n} \mid f \in N_{\mathbb{Z}_{p^n}}\}| = |A|.$$

□

Remark 7.7. Let $n = 1$ and $A = \{([f]_{p^n}, [f']_{p^n}) \mid f \in \mathbb{Z}[x] \text{ with } [f]_{p^n} = F\}$. Then $|A| = p^p$ by Lemma 4.9, but $|St_\alpha(\mathbb{Z}_{p^n})| = (p-1)^p$ by Theorem 4.11. This shows that the condition on n in Corollary 7.6 is necessary.

We now we give a self-contained proof of Corollary 5.9 (not using Jiang's ratio [13], but emulating the argument in the proof of Theorem 5.7), for $R = \mathbb{Z}_{p^n}[\alpha]$.

Corollary 7.8. *For any integer $n > 1$,*

$$|\mathcal{F}(\mathbb{Z}_{p^n}[\alpha])| = |\mathcal{F}(\mathbb{Z}_{p^n})|^2 \cdot |St_\alpha(\mathbb{Z}_{p^n})|.$$

Proof. Set

$$B = \bigcup_{F\in\mathcal{F}(\mathbb{Z}_{p^n})} \{([f]_{p^n}, [f']_{p^n}) \mid [f]_{p^n} = F \text{ and } f \in \mathbb{Z}[x]\}.$$

By Corollary 7.6,

$$|B| = |\mathcal{F}(\mathbb{Z}_{p^n})| \cdot |St_\alpha(\mathbb{Z}_{p^n})|.$$

We now define a function $\psi\colon \mathcal{F}(R[\alpha]) \to B \times \mathcal{F}(R)$ as follows: if $G \in \mathcal{F}(R[\alpha])$ is induced by $g = g_1 + \alpha\, g_2$, where $g_1, g_2 \in \mathbb{Z}_{p^n}[x]$, we let $\psi(G) = (([g_1]_{p^n}, [g_1']_{p^n}), [g_2]_{p^n})$.

By Corollary 3.7, ψ is well-defined and bijective, and, hence, $|\mathcal{F}(\mathbb{Z}_{p^n}[\alpha])| = |B| \cdot |\mathcal{F}(\mathbb{Z}_{p^n})|$. □

As $|\mathcal{F}(\mathbb{Z}_{p^n})|$ is a well-known quantity (quoted in the introduction in Equation (1.1)), all we now need for an explicit formula for $\mathcal{F}(\mathbb{Z}_{p^n}[\alpha])$ is an expression for $|St_\alpha(\mathbb{Z}_{p^n})|$. We will derive one for $n \le p$ in the next section.

8. On the number of polynomial functions on $\mathbb{Z}_{p^n}[\alpha]$

In this section we find explicit counting formulas for the number of polynomial functions and the number of polynomial permutations on $\mathbb{Z}_{p^n}[\alpha]$ for $n \le p$. The reason for the assumption $n \le p$ is that in this case (unlike the case $n > p$) the ideal of null polynomials on $\mathbb{Z}_{p^n}$ is equal to $((x^p - x), p)^n$. The equality can be seen by a counting argument [10: Corollary 2.5] – the ideal $((x^p - x), p)^n$ is clearly contained in $N_{\mathbb{Z}_{p^n}}$, and, for $n \le p$, their respective indices in $\mathbb{Z}_{p^n}[x]$ are the same — but it can also be derived from other results [30: Theorem 3.3 (2)].

This fact allows us to see at a glance if a polynomial is a null polynomial modulo p^k (for any $k \le n$) once we have expanded the polynomial as a $\mathbb{Z}[x]$-linear combination of the powers $(x^p - x)^m$, with coefficients of degree less than p. Our Lemma to this effect, Lemma 8.2, is taken from an earlier paper [10].

Remark 8.1. Let R be a commutative ring and $h \in R[x]$ monic with $\deg h = q > 0$.

(1) Every polynomial $f \in R[x]$ can be represented uniquely as

$$f(x) = f_0(x) + f_1(x)h(x) + f_2(x)h(x)^2 + \dots$$

with $f_k \in R[x]$ and $\deg f_k < q$ for all $k \ge 0$.

(2) Let I an ideal of R. Let $f, g \in R[x]$, $f = \sum\limits_i a_i x^i$ and $g = \sum\limits_i b_i x^i$ be expanded as in (1) with $f_k = \sum\limits_{j=0}^{q-1} a_{jk} x^j$ and $g_k = \sum\limits_{j=0}^{q-1} b_{jk} x^j$. Then

$$a_i \equiv b_i \bmod I \quad \text{for all } i \quad \Longleftrightarrow \quad a_{jk} \equiv b_{jk} \bmod I \quad \text{for all } j, k.$$

(1) follows easily from repeated division with remainder by $h(x)$ and the fact that quotient and remainder are unique in polynomial division. (2) follows from the uniqueness of the expansion applied to polynomials in $(R/I)[x]$.

Lemma 8.2 ([10: Lemma 2.5]). *Let p be a prime and $f \in \mathbb{Z}[x]$ represented as in* Remark 8.1 *with respect to $h(x) = x^p - x$.*

$$f(x) = f_0(x) + f_1(x)(x^p - x) + f_2(x)(x^p - x)^2 + \dots$$

with $f_k \in \mathbb{Z}[x]$ and $\deg f_k < p$ for all $k \ge 0$.

Let $n \le p$. Then f is a null polynomial on $\mathbb{Z}_{p^n}$ if and only if $f_k \in p^{n-k}\mathbb{Z}[x]$ for $0 \le k \le n$.

Corollary 8.3. *Let $n \le p$. Then $|N_{\mathbb{Z}_{p^n}}(< (n+1)p)| = p^{\frac{n(n+1)p}{2}}$.*

Proof. We express $f \in \mathbb{Z}[x]$ with $\deg f < (n+1)p$ as in Remark 8.1, Lemma 8.2, $f(x) = \sum\limits_{k=0}^{n} f_k(x)(x^p - x)^k$, where $f_k(x) = \sum\limits_{j=0}^{p-1} a_{jk}x^j$.

By Lemma 8.2 and Remark 8.1 (2), $|N_{\mathbb{Z}_{p^n}}(< (n+1)p)|$ is equal to the number of ways to choose the a_{jk} from a fixed system of representatives modulo p^n, such that $a_{jk} \equiv 0 \mod p^{(n-k)}$ for $k \leq n$. This number is $\prod\limits_{k=0}^{n} p^{kp} = p^{p\sum\limits_{k=0}^{n} k} = p^{\frac{n(n+1)p}{2}}$. □

Lemma 8.4. *Let* $f \in \mathbb{Z}[x]$*, where* $f(x) = \sum\limits_{k \geq 0} f_k(x)(x^p - x)^k$ *such that* $f_k(x) = \sum\limits_{j=0}^{p-1} a_{jk}x^j$*. If we expand* f' *in a similar way,* $f'(x) = \sum\limits_{k \geq 0} \hat{f}_k(x)(x^p - x)^k$*, where* $\hat{f}_k(x) = \sum\limits_{j=0}^{p-1} \hat{a}_{jk}x^j$*, then the following relations hold for all* $k \geq 0$

$$\begin{aligned} \hat{a}_{0k} &= (kp+1)a_{1k} - (k+1)a_{0\,k+1} \\ \hat{a}_{jk} &= (kp+j+1)a_{j+1\,k} + (k+1)(p-1)a_{j\,k+1} \qquad \text{for } 1 \leq j \leq p-2 \\ \hat{a}_{p-1\,k} &= (k+1)(p-1)a_{p-1\,k+1} + (k+1)pa_{0\,k+1}. \end{aligned} \tag{8.1}$$

Proof. Consider

$$\big(f_k(x)(x^p - x)^k\big)' = f_k'(x)(x^p - x)^k - kf_k(x)(x^p - x)^{k-1} + kpx^{p-1}f_k(x)(x^p - x)^{k-1}. \tag{8.2}$$

We rewrite the last term of Equation (8.2) by expanding $x^{p-1}f_k(x)$ as $\sum\limits_{j=0}^{p-1} a_{jk}x^{p+j-1}$ and substituting $x^{j+1} + x^j(x^p - x)$ for x^{p+j}, to get integer linear-combinations of terms $x^j(x^p - x)^k$.

$$\begin{aligned} kpx^{p-1}f_k(x)(x^p - x)^{k-1} &= \sum_{j=0}^{p-1} kpa_{jk}x^{p+j-1}(x^p - x)^{k-1} \\ &= \Big(\sum_{j=1}^{p-1} kpa_{jk}x^{p+j-1} + kpa_{0k}x^{p-1}\Big)(x^p - x)^{k-1} \\ &= \Big(\sum_{j=1}^{p-1} kpa_{jk}(x^j + x^{j-1}(x^p - x)) + kpa_{0k}x^{p-1}\Big)(x^p - x)^{k-1} \\ &= \Big(\sum_{j=1}^{p-2} kpa_{jk}x^j + (kpa_{p-1\,k} + kpa_{0k})x^{p-1}\Big)(x^p - x)^{k-1} \\ &\qquad + \Big(\sum_{j=0}^{p-2} kpa_{j+1\,k}x^j\Big)(x^p - x)^k \end{aligned}$$

and, therefore,

$$\begin{aligned} \big(f_k(x)(x^p - x)^k\big)' = \Big(&-ka_{0k} + \sum_{j=1}^{p-2} k(p-1)a_{jk}x^j + (k(p-1)a_{p-1\,k} + kpa_{0k})x^{p-1}\Big)(x^p - x)^{k-1} \\ &+ \Big(\sum_{j=0}^{p-2}(kp + j + 1)a_{j+1\,k}x^j\Big)(x^p - x)^k. \end{aligned} \tag{8.3}$$

Thus $f'(x) = \sum\limits_{k\geq 0} (f_k(x)(x^p - x)^k)' = \sum\limits_{k=0} \hat{f}_k(x)(x^p - x)^k$, where

$$\begin{aligned}\hat{f}_k(x) = (kp+1)a_{1k} - (k+1)a_{0\,k+1} &+ \sum_{j=1}^{p-2} \big((kp+j+1)a_{j+1\,k} + (k+1)(p-1)a_{j\,k+1}\big)x^j \\ &+ ((k+1)(p-1)a_{p-1\,k+1} + (k+1)pa_{0\,k+1})x^{p-1}.\end{aligned}$$

Finally, expressing the $\hat{a}_{jk}$ in terms of the a_{jk}, we get

$$\begin{aligned}\hat{a}_{0k} &= (kp+1)a_{1k} - (k+1)a_{0\,k+1}, \\ \hat{a}_{jk} &= (kp+j+1)a_{j+1\,k} + (k+1)(p-1)a_{j\,k+1} && \text{for } 1 \leq j \leq p-2, \\ \hat{a}_{p-1\,k} &= (k+1)(p-1)a_{p-1\,k+1} + (k+1)pa_{0\,k+1} && \text{for } k \geq 0.\end{aligned}$$

□

Let $f \in \mathbb{Z}[x]$, p a prime and $n \leq p$. We are now in a position to tell from the coefficients of the expansion of f with respect to powers of $(x^p - x)$ (as in Remark 8.1) whether both f and f' are null polynomials on $\mathbb{Z}_{p^n}$.

Theorem 8.5. *Let $n \leq p$ and $f(x) = \sum\limits_{k=0}^{m} f_k(x)(x^p - x)^k \in \mathbb{Z}[x]$, where $f_k(x) = \sum\limits_{j=0}^{p-1} a_{jk}x^j$.*

Then f and f' are both null polynomials on $\mathbb{Z}_{p^n}$ if and only if, for $1 \leq k < \min(p, n+1)$,

$$\begin{aligned} a_{j0} &\equiv 0 \pmod{p^n} \\ a_{jk} &\equiv 0 \pmod{p^{n-k+1}}. \end{aligned} \tag{8.4}$$

Proof. ($\Rightarrow$) Suppose f and f' are null polynomials on $\mathbb{Z}_{p^n}$. Then $f'(x) = \sum\limits_{k=0}^{m} \hat{f}_k(x)(x^p - x)^k$, with $\hat{f}_k(x) = \sum\limits_{j=0}^{p-1} \hat{a}_{jk}x^j$, such that, by Lemma 8.4, the coefficients a_{jk} and $\hat{a}_{jk}$ satisfy Equation (8.1). Since f' is a null polynomial on $\mathbb{Z}_{p^n}$, Lemma 8.2 implies, for $j = 0, \ldots, p-1$,

$$\hat{a}_{jk} \equiv 0 \pmod{p^{n-k}} \qquad \text{for } k \leq n. \tag{8.5}$$

Again by Lemma 8.2, it is clear that

$$a_{j0} \equiv 0 \pmod{p^n} \qquad \text{for } j = 0, 1, \ldots, p-1. \tag{8.6}$$

For $1 \leq k < \min(p, n+1)$, we use induction. To see $a_{j1} \equiv 0 \pmod{p^n}$, we set $k = 0$ in Equation (8.1), and get

$$\begin{aligned}\hat{a}_{00} &= a_{10} - a_{0\,1}, \\ \hat{a}_{j0} &= (j+1)a_{j+1\,0} + (p-1)a_{j\,1} \qquad \text{for } 1 \leq j \leq p-2, \\ \hat{a}_{p-1\,0} &= (p-1)a_{p-1\,1} + pa_{0\,1}.\end{aligned} \tag{8.7}$$

From Equations (8.5), (8.6), and (8.7), we conclude that $a_{j1} \equiv 0 \pmod{p^n}$, $j = 0, 1, \ldots, p-1$.

Now, for $2 \leq k+1 < \min(p, n+1)$, we prove the statement for $k+1$ under the hypothesis

$$a_{jk} \equiv 0 \pmod{p^{n+1-k}} \qquad \text{for } j = 0, 1, \ldots, p-1. \tag{8.8}$$

We rewrite Equation (8.1) as

$$\begin{aligned}(k+1)a_{0\,k+1} &= (kp+1)a_{1k} - \hat{a}_{0k} \\ (k+1)(p-1)a_{j\,k+1} &= \hat{a}_{jk} - (kp+j+1)a_{j+1\,k} && \text{for } 1 \leq j \leq p-2 \\ (k+1)(p-1)a_{p-1\,k+1} &= \hat{a}_{p-1\,k} - (k+1)pa_{0\,k+1} && \text{for } k = 0, 1, \ldots, n-1.\end{aligned} \tag{8.9}$$

Since $k+1 < p$ and $n+1-k > n-k$, Equations (8.9), (8.5) and the induction hypothesis (Equation (8.8)) give

$$a_{j\,k+1} \equiv 0 \pmod{p^{n-k}} \qquad \text{for } j = 0, 1, \ldots, p-1.$$

For $k \geq \min(p, n+1)$, we note that $(x^p - x)^k \in N'_{\mathbb{Z}_{p^n}}$. Hence $f_k(x)(x^p - x)^k \in N'_{\mathbb{Z}_{p^n}}$. So, there are no restrictions on a_{jk} for $j = 0, \ldots, p-1$.

($\Leftarrow$) Assume that (8.4) is true. Then, for $k \leq p$, $a_{jk} \equiv 0 \pmod{p^{(n-k)}}$ since $n+1-k > n-k$. We use Lemma 8.4 and Equation (8.4) to show that $\hat{a}_{jk} \equiv 0 \pmod{p^{(n-k)}}$ for $0 \leq k \leq p$. The result now follows by Lemma 8.2. □

Corollary 8.6. *Let $n \leq p$ and $r = \min(n+1, p)$, that is, $r = \begin{cases} n+1 & \text{if } n < p \\ p & \text{if } n = p \end{cases}$.*

Then $(x^p - x)^r$ is a monic null polynomial on $\mathbb{Z}_{p^n}[\alpha]$ of minimal degree.

Proof. By Lemma 3.4, $(x^p - x)^r$ is a null polynomial on $\mathbb{Z}_{p^n}[\alpha]$. Let $h \in \mathbb{Z}[\alpha][x]$ be a null polynomial on $\mathbb{Z}_{p^n}[\alpha]$ with $\deg h < rp$. By Corollary 3.6, it suffices to consider $h \in \mathbb{Z}[x]$. We show that h is not monic. If $h = 0$ this is evident. If $h \neq 0$, we expand h as in Lemma 8.2:

$$h(x) = h_0(x) + h_1(x)(x^p - x) + \cdots + h_{r-1}(x)(x^p - x)^r$$

with $h_k(x) = \sum\limits_{j=0}^{p-1} a_{jk} x^j \in \mathbb{Z}[x]$. By Theorem 8.5, it follows that for $0 \leq j \leq p-1$

$$\begin{aligned} a_{j0} &\equiv 0 \pmod{p^n}, \\ a_{jk} &\equiv 0 \pmod{p^{(n-k+1)}} \quad \text{for } 1 \leq k < r. \end{aligned}$$

If l is the largest number such that $h_l(x) \neq 0$, then $a_{p-1\,l} \neq 1$, since $a_{p-1\,l} \equiv 0 \mod p^{(n-l+1)}$. Thus h cannot be monic. □

Recall from Definitions 3.1 and 7.1 that $f \in N'_{\mathbb{Z}_{p^n}}(< (n+1)p)$ means f and f' are null polynomials on $\mathbb{Z}_{p^n}$ and $\deg f < (n+1)p$.

Corollary 8.7. *Let $n \leq p$. Then $|N'_{\mathbb{Z}_{p^n}}(< (n+1)p)| = \begin{cases} p^{\frac{n(n-1)p}{2}} & \text{if } n < p \\ p^{\frac{(n^2-n+2)p}{2}} & \text{if } n = p \end{cases}$.*

Proof. We represent every polynomial $f \in \mathbb{Z}_{p^n}[x]$ with $\deg f < (n+1)p$ uniquely, by Remark 8.1, as

$$f(x) = \sum_{k=0}^{n} f_k(x)(x^p - x)^k \qquad \text{with } f_k(x) = \sum_{j=0}^{p-1} a_{jk} x^j \in \mathbb{Z}_{p^n}[x].$$

By Theorem 8.5, counting the polynomials in $N'_{\mathbb{Z}_{p^n}}(< (n+1)p)$ amounts to counting the number of choices for the a_{jk} such that $a_{j0} \equiv 0 \mod p^n$ and $a_{jk} \equiv 0 \mod p^{n-k+1}$ for $1 \leq k < \min(p, n+1)$ and $0 \leq j \leq p-1$.

When $n < p$, there are p^{k-1} choices for a_{jk} for each pair (j,k) with $1 \leq k \leq n$ and $0 \leq j \leq p-1$. Hence the total number of ways of choosing all coefficients, when $n < p$, is equal to

$$\prod_{k=1}^{n} p^{p(k-1)} = \prod_{k=0}^{n-1} p^{pk} = p^{p\sum\limits_{k=0}^{n-1} k} = p^{\frac{pn(n-1)}{2}}.$$

When $n = p$, a_{jn} can be chosen in p^n ways, and the resulting total is

$$p^{np}\prod_{k=1}^{n-1} p^{p(k-1)} = p^{np}\prod_{k=0}^{n-2} p^{pk} = p^{np+p\sum\limits_{k=0}^{n-2} k} = p^{\frac{p(n^2-n+2)}{2}}. \qquad \square$$

At last, we obtain an explicit formula for the order of $St_\alpha(\mathbb{Z}_{p^n})$ for $n \le p$.

Theorem 8.8. *Let $1 \le n \le p$. Then*

$$|St_\alpha(\mathbb{Z}_{p^n})| = \begin{cases} (p-1)^p & \text{if } n = 1 \\ p^{np} & \text{if } 1 < n < p \\ p^{(n-1)p} & \text{if } n = p \end{cases}.$$

Proof. The case $n = 1$ is a special case of Theorem 4.11 (3). Let $1 < n \le p$. By Corollary 7.4,

$$|St_\alpha(\mathbb{Z}_{p^n})| = \frac{|N_{\mathbb{Z}_{p^n}}(< (n+1)p)|}{|N'_{\mathbb{Z}_{p^n}}(< (n+1)p)|}.$$

Now Corollaries 8.3 and 8.7, respectively, say that

$$|N_{\mathbb{Z}_{p^n}}(< (n+1)p)| = p^{\frac{n(n+1)p}{2}} \qquad \text{and} \qquad |N'_{\mathbb{Z}_{p^n}}(< (n+1)p)| = \begin{cases} p^{\frac{n(n-1)p}{2}} & \text{if } n < p \\ p^{\frac{(n^2-n+2)p}{2}} & \text{if } n = p \end{cases}. \qquad \square$$

***Example* 8.9.** Let $R = \mathbb{Z}_4$. Then $|St_\alpha(\mathbb{Z}_4)| = 4$ by Theorem 8.8. Now, by Corollary 8.6, the polynomial $(x^2 - x)^2$ is a monic null polynomial on $\mathbb{Z}_4[\alpha]$ of minimal degree. So every polynomial function on $\mathbb{Z}_4[\alpha]$ can be represented by a polynomial of degree less than 4. Consider the following null polynomials on $\mathbb{Z}_4$:

$$f_1 = 0, \quad f_2 = 2(x^2 - x), \quad f_3 = 2(x^3 - x), \quad f_4 = 2(x^3 - x^2).$$

It is evident that $[x+f_i]_4 = id_{\mathbb{Z}_4}$, and so by Corollary 6.4, $[x+f_i] \in St_\alpha(\mathbb{Z}_4)$, where $[x+f_i]$ denotes the function induced by $x + f_i$ on $\mathbb{Z}_4[\alpha]$ for $i = 1, \dots, 4$. Note that $[1 + f'_i]_4 \neq [1 + f'_j]_4$, however, and hence by Corollary 3.7, $[x + f_i] \neq [x + f_j]$ whenever $i \neq j$. Therefore $St_\alpha(\mathbb{Z}_4) = \{[x + f_i], i = 1, \dots, 4\}$. Actually, $St_\alpha(\mathbb{Z}_4)$ is the Klein 4-group.

Theorem 8.8 now allows us to state explicit formulas for the number of polynomial functions and polynomial permutations on $\mathbb{Z}_{p^n}[\alpha]$ for $n \le p$. Our formula for $|\mathcal{P}(\mathbb{Z}_{p^n}[\alpha])|$ depends on p and n. To understand it in terms of the residue field and nilpotency of the maximal ideal of $\mathbb{Z}_{p^n}[\alpha]$, recall from Proposition 2.6 that the residue field of $\mathbb{Z}_{p^n}[\alpha]$ is isomorphic to $\mathbb{Z}_p$ and the nilpotency of the maximal ideal is $n + 1$.

Theorem 8.10. *Let $1 \le n \le p$. Then the number $|\mathcal{P}(\mathbb{Z}_{p^n}[\alpha])|$ of polynomial permutations on $\mathbb{Z}_{p^n}[\alpha]$ is given by*

$$|\mathcal{P}(\mathbb{Z}_{p^n}[\alpha])| = \begin{cases} p!(p-1)^p p^{(n^2+2n-2)p} & \text{if } n < p \\ p!(p-1)^p p^{(n^2+2n-3)p} & \text{if } n = p \end{cases}.$$

Proof. The case $n = 1$ is covered by Proposition 4.10. Now, let $1 < n \le p$. Using that $\mu(p^k) = kp$ for $k \le p$, we simplify the formulas for $|\mathcal{F}(\mathbb{Z}_{p^n})|$ and $|\mathcal{P}(\mathbb{Z}_{p^n})|$ quoted in the introduction (Equation (1.1)) accordingly. For $1 < n \le p$,

$$|\mathcal{F}(\mathbb{Z}_{p^n})| = p^{\frac{n(n+1)p}{2}} \qquad \text{and} \qquad |\mathcal{P}(\mathbb{Z}_{p^n})| = p!(p-1)^p p^{-2p} p^{\frac{n(n+1)p}{2}}. \tag{8.10}$$

Substituting the formula from Theorem 8.8 for $|St_\alpha(\mathbb{Z}_{p^n})|$ and the above expressions for $|\mathcal{F}(\mathbb{Z}_{p^n})|$ and $|\mathcal{P}(\mathbb{Z}_{p^n})|$ in Theorem 5.7, we obtain the desired result. □

Theorem 8.11. *Let $n \leq p$. The number $|\mathcal{F}(\mathbb{Z}_{p^n}[\alpha])|$ of polynomial functions on $\mathbb{Z}_{p^n}[\alpha]$ is given by*

$$|\mathcal{F}(\mathbb{Z}_{p^n}[\alpha])| = \begin{cases} p^{(n^2+2n)p} & \text{if } n < p \\ p^{(n^2+2n-1)p} & \text{if } n = p \end{cases}.$$

Proof. The case $n = 1$ is covered by Corollary 3.11. For $1 < n \leq p$, we substitute the expression from Theorem 8.8 for $|St_\alpha(\mathbb{Z}_{p^n})|$ and the formula for $|\mathcal{F}(\mathbb{Z}_{p^n})|$ from Equation (1.1) (simplified as in Equation (8.10) in the proof of Theorem 8.10) in Corollary 7.8. □

9. A canonical form

In this section we find a canonical representation for the polynomial functions on $\mathbb{Z}_{p^n}[\alpha]$ whenever $n \leq p$. As before (see Definition 3.13), $\mu(m)$ stands for the smallest natural number n such that m divides $n!$.

Lemma 9.1 ([26: Theorem 10]). *Let F be a polynomial function on $\mathbb{Z}_m$. Then F is uniquely represented by a polynomial $f \in \mathbb{Z}[x]$ of the form*

$$f(x) = \sum_{i=0}^{\mu(m)-1} a_i x^i \qquad \text{with } \ 0 \leq a_i < \frac{m}{\gcd(m, i!)}.$$

Proposition 9.2. *Let $F\colon \mathbb{Z}_m[\alpha] \to \mathbb{Z}_m[\alpha]$ be a polynomial function on $\mathbb{Z}_m[\alpha]$. Then F can be represented by a polynomial $f \in \mathbb{Z}[x]$ of the form*

$$f(x) = \sum_{i=0}^{2\mu(m)-1} a_i x^i + \sum_{j=0}^{\mu(m)-1} b_j x^j \, \alpha \qquad \text{with } 0 \leq a_i, b_j < m \ \text{ and } \ 0 \leq b_j < \frac{m}{\gcd(m, j!)}$$

and the b_j in such a representation are unique.

Proof. By Corollary 3.17, F can be represented by a polynomial $g_1 + \alpha\, g_2$, where

$$g_1(x) = \sum_{i=0}^{2\mu(m)-1} c_i x^i \qquad \text{and} \qquad g_2(x) = \sum_{j=0}^{\mu(m)-1} d_j x^j$$

with $c_i, d_j \in \mathbb{Z}$. Choosing a_i, b_j to be the smallest non-negative integers such that $c_i \equiv a_i$ and $d_j \equiv b_j \mod m$, we see that F is represented by

$$g(x) = \sum_{i=0}^{2\mu(m)-1} a_i x^i + \sum_{j=0}^{\mu(m)-1} b_j x^j \, \alpha$$

with $0 \leq a_i, b_j < m$. Now, since $\mathbb{Z}_m[\alpha]$ is a $\mathbb{Z}$-algebra, substituting elements of $\mathbb{Z}_m[\alpha]$ for the variable x in g defines a function on $\mathbb{Z}_m[\alpha]$. For $k, l \in \mathbb{Z}_m$, we have

$$g(k + l\,\alpha) = \sum_{i=0}^{2\mu(m)-1} a_i (k + l\,\alpha)^i + \sum_{j=0}^{\mu(m)-1} b_j k^j \, \alpha \, .$$

By Corollary 3.7, F depends on the function induced by $\sum\limits_{j=0}^{\mu(m)-1} b_j x^j$ on $\mathbb{Z}_m$ but not on the function induced by its derivative. So we can replace $\sum\limits_{j=0}^{\mu(m)-1} b_j x^j$ by any polynomial $h \in \mathbb{Z}[x]$ such that

$[\sum_{j=0}^{\mu(m)-1} b_j x^j]_m = [h]_m$. Hence, by Corollary 3.7 and Lemma 9.1, b_j can be chosen uniquely such that $0 \leq b_j < \frac{m}{\gcd(m,j!)}$. □

By combining Proposition 9.2 with Proposition 3.16, we obtain the following corollary.

Corollary 9.3. *Let p be a prime number and $n \leq p$ a positive integer. Let $F \colon \mathbb{Z}_{p^n}[\alpha] \to \mathbb{Z}_{p^n}[\alpha]$ be a polynomial function on $\mathbb{Z}_{p^n}[\alpha]$. Then F can be represented as a polynomial $f(x) = \sum_{i=0}^{(n+1)p-1} a_i x^i + \sum_{j=0}^{np-1} b_j x^j \alpha$ with $0 \leq a_i, b_j < p^n$. Moreover, b_j can be chosen uniquely such that $0 \leq b_j < \frac{p^n}{\gcd(p^n,j!)}$.*

Finally, we give a canonical representation for polynomial functions on $\mathbb{Z}_{p^n}[\alpha]$ for $n \leq p$.

Theorem 9.4. *Let $n \leq p$. Every polynomial function F on $\mathbb{Z}_{p^n}[\alpha]$ is uniquely represented by a polynomial $f \in \mathbb{Z}[x]$ of the form*

$$f(x) = \sum_{k=0}^{m} f_k(x)(x^p - x)^k + \sum_{i=0}^{np-1} b_i x^i \alpha \quad \textit{with} \quad f_k(x) = \sum_{j=0}^{p-1} a_{jk} x^j,$$

where

1. *$m = \min(n, p-1)$*
2. *$0 \leq a_{j0} < p^n$ and $0 \leq a_{jk} < p^{n-k+1}$ (for $j = 0, \ldots, p-1$ and $k = 1, \ldots, m$)*
3. *$0 \leq b_i < \frac{p^n}{\gcd(p^n,i!)}$ (for $i = 0, \ldots, np-1$).*

Proof. Let F be a polynomial function on $\mathbb{Z}_{p^n}[\alpha]$. By Corollary 9.3, we can represent F by $f = g + \alpha\, h$ with $g, h \in \mathbb{Z}[x]$, such that $\deg g < (n+1)p - 1$ and $h(x) = \sum_{i=0}^{np-1} b_i x^i$ with $0 \leq b_i < \frac{p^n}{\gcd(p^n,i!)}$; and the coefficients b_i in such a representation are unique.

By Corollary 8.6, $(x^p - x)^{m+1}$ is null on $\mathbb{Z}_{p^n}[\alpha]$. Thus we can choose g with $\deg g < p(m+1)$ by Proposition 3.12. We expand g as in Lemma 8.2, $g(x) = \sum_{k=0}^{m} g_k(x)(x^p - x)^k$, where $g_k(x) = \sum_{j=0}^{p-1} c_{jk} x^j \in \mathbb{Z}[x]$.

By division with remainder, we get $c_{j0} = p^n q_{j0} + a_{j0}$ and $c_{jk} = p^{n-k+1} q_{jk} + a_{jk}$ with $0 \leq a_{j0} < p^n$ and $0 \leq a_{jk} < p^{n-k+1}$ for $j = 0, \ldots, p-1$, and $k = 1, \ldots, m$. By Theorem 8.5,

$$p^n(x^p - x) \triangleq p^{n-k+1}(x^p - x)^k \triangleq 0 \qquad \text{on} \quad \mathbb{Z}_{p^n}[\alpha].$$

Thus, if we set $f_k(x) = \sum_{j=0}^{p-1} a_{jk} x^j$ for $k = 0, \ldots, m$, we have, by Corollary 3.7,

$$g(x) = \sum_{k=0}^{m} g_k(x)(x^p - x)^k \triangleq \sum_{k=0}^{m} f_k(x)(x^p - x)^k \qquad \text{on} \quad \mathbb{Z}_{p^n}[\alpha],$$

and hence we can replace g by $\sum_{k=0}^{m}\sum_{j=0}^{p-1} f_k(x)(x^p - x)^k$ in the representation of the function F. Therefore F is induced by $f = g + \alpha\, h$, where $g(x) = \sum_{k=0}^{m}\sum_{j=0}^{p-1} a_{jk} x^j (x^p - x)^k$, with $0 \leq a_{j0} < p^n$, $0 \leq a_{jk} < p^{n-k+1}$ for $j = 0, \ldots, p-1$, and $k = 1, \ldots, m$; and h as above. To count the number of ways of selecting such a polynomial f, we need to count the number of ways of choosing g and h. First, we do that for g. We note that $f_0(x)$ can be determined in p^{np} ways, since $a_{j0} < p^n$ for $j = 0, \dots, p-1$. While, if $1 \le k \le m$, $f_k(x)$ can be selected in $p^{p(n-k+1)}$ ways, since $0 \le a_{jk} < p^{n-k+1}$ for $j = 0, \dots, p-1$. So, the number of ways to choose g is

$$p^{np} \prod_{k=1}^{m} p^{p(n-k+1)} = p^{np} \prod_{k=0}^{m-1} p^{p(n-k)}.$$

On the other hand, simple calculations show that $\sum\limits_{i=0}^{np-1} b_i x^i \alpha$ can be chosen in $p^{\frac{pn(n+1)}{2}}$ ways, since $0 \le b_i < \frac{p^n}{\gcd(p^n, i!)}$. Thus the number of ways that f can be chosen is

$$p^{np} \prod_{k=0}^{m-1} p^{p(n-k)} \cdot p^{\frac{pn(n+1)}{2}} = \begin{cases} p^{(n^2+2n)p} & \text{if } n < p \\ p^{(n^2+2n-1)p} & \text{if } n = p \end{cases}.$$

By Theorem 8.11, this last quantity equals $|\mathcal{F}(\mathbb{Z}_{p^n}[\alpha])|$ and, therefore, the representation is unique. □

Acknowledgement. The authors would like to thank Irena Swanson for valuable suggestions and comments on earlier versions of the manuscript.

REFERENCES

[1] AL-MAKTRY, A. A.: *On the group of unit-valued polynomial functions*, AAECC (2021); `https://doi.org/10.1007/s00200-021-00510-x`.

[2] AL-MAKTRY, A. A.: *Polynomial functions over dual numbers of several variables*, `https://arxiv.org/abs/2002.01304`.

[3] BRAWLEY, J. V.—MULLEN, G. L.: *Functions and polynomials over Galois rings*, J. Number Theory **41** (1992), 156–166.

[4] BULYOVSZKY, B.—HORVÁTH, G.: *Polynomial functions over finite commutative rings*, Theoret. Comput. Sci. **703** (2017), 76–86.

[5] CENGELLENMIS, Y.—DERTLI, A.—AYDIN, N.: *Some constacyclic codes over $\mathbb{Z}_4[u]/\langle u^2\rangle$, new Gray maps, and new quaternary codes*, Algebra Colloq. **25** (2018), 369–376.

[6] CHEN, Z.: *On polynomial functions from $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_r}$ to $\mathbb{Z}_m$*, Discrete Math. **162** (1996), 67–76.

[7] DING, J.—LI, H.: *The Gray images of $(1+u)$ constacyclic codes over $F_{2^m}[u]/\langle u^k\rangle$*, J. Appl. Math. Comput. **49** (2015), 433–445.

[8] FRISCH, S.: *When are weak permutation polynomials strong?*, Finite Fields Appl. **1** (1995), 437–439.

[9] FRISCH, S.: *Polynomial functions on finite commutative rings* In: Advances in Commutative Ring Theory (Fez, 1997), Lecture Notes in Pure and Appl. Math. 205, 1999, pp. 323–336.

[10] FRISCH, S.—KRENN, D.: *Sylow p-groups of polynomial permutation on the integers* $\bmod p^n$, J. Number Theory **133** (2013), 4188–4199.

[11] GÖRCSÖS, D.—HORVÁTH, G.—MÉSZÁROS, A.: *Permutation polynomials over finite rings*, Finite Fields Appl. **49** (2018), 198–211.

[12] GUHA, A.—DUKKIPATI, A.: *A faster algorithm for testing polynomial representability of functions over finite integer rings*, Theoret. Comput. Sci. **579** (2015), 88–99.

[13] JIANG, J.: *A note on polynomial functions over finite commutative rings*, Adv. Math. (China) **39** (2010), 555–560.

[14] KAISER, H. K.—NÖBAUER, W.: *Permutation polynomials in several variables over residue class rings*, J. Austral. Math. Soc. Ser. A **43** (1987), 171–175.

[15] KELLER, G.—OLSON, F. R.: *Counting polynomial functions* (mod p^n), Duke Math. J. **35** (1968), 835–838.

[16] KEMPNER, A. J.: *Miscellanea*, Amer. Math. Monthly **25** (1918), 201–210.

[17] KEMPNER, A. J.: *Polynomials and their residue systems*, Trans. Amer. Math. Soc. **22** (1921), 240–266, 267–288.

[18] LIU, N. P.—JIANG, J. J.: *Polynomial functions in n variables over a finite commutative ring*, Sichuan Daxue Xuebao **46** (2009), 44–46.

[19] MCDONALD, R. N.: *Finite Rings with Identity*, Marcel Dekker, Inc., New York, 1979.

[20] NECHAEV, A. A.: *Polynomial transformations of finite commutative local rings of principal ideals*, Math. Notes **27** (1980), 425–432. transl. from Mat. Zametki **27** (1980), 885–897.

[21] NÖBAUER, W.: *Polynomfunktionen auf primen Restklassen*, Arch. Math. (Basel) **39** (1982), 431–435.

[22] NÖBAUER, W.: *Die Operation des Einsetzens bei Polynomen in mehreren Unbestimmten*, J. Reine Angew. Math. (1979), 207–220.

[23] NÖBAUER, W.: *Zur Theorie der Polynomtransformationen und Permutationspolynome*, Math. Ann. **157** (1964), 332–342.

[24] NÖBAUER, W.: *Gruppen von Restpolynomidealrestklassen nach Primzahlpotenzen*, Monatsh. Math. **59** (1955), 194–202.

[25] NÖBAUER, W.: *Über Gruppen von Restklassen nach Restpolynomidealen*, Österreich. Akad. Wiss. Math.-Nat. Kl. S.-B. IIa **162** (1953), 207–233.

[26] SINGMASTER, D.: *On polynomial functions* mod m, J. Number Theory **6** (1974), 345–352.

[27] WEI, Q.—ZHANG, Q.: *On permutation polynomials in two variables over* $\mathbb{Z}/p^2\mathbb{Z}$, Acta Math. Sin. (Engl. Ser.) **25** (2009), 1191–1200.

[28] WEI, Q.—ZHANG, Q.: *On strong orthogonal systems and weak permutation polynomials over finite commutative rings*, Finite Fields Appl. **13** (2007), 113–120.

[29] WIESENBAUER, J.: *On polynomial functions over residue class rings of* $\mathbb{Z}$. Contributions to general algebra 2 (Proc. of Conf. in Klagenfurt 1982), Hölder-Pichler-Tempsky, Teubner, 1983, pp. 395–398.

[30] ZHANG, Q.: *Polynomial functions and permutation polynomials over some finite commutative rings*, J. Number Theory **105** (2004), 192–202.

Received 22. 2. 2020
Accepted 30. 12. 2020

* *Department of Mathematics*
The University of Jordan
Amman 11942
JORDAN
E-mail: alezehh@ju.edu.jo

** *Department of Analysis and Number Theory (5010)*
Technische Universität Graz
Kopernikusgasse 24/II
8010 Graz
AUSTRIA
E-mail: almaktry@math.tugraz.at
frisch@math.tugraz.at