Amr Ali Abdulkader Al-Maktry, M.Sc.

Polynomial functions of dual numbers over finite commutative rings

DOCTORAL THESIS

to achieve the university degree of

Doktor der Naturwissenschaften

submitted to

Graz University of Technology

Supervisor

Ao.Univ.-Prof. Mag.rer.nat. Dr.techn. Sophie Frisch

Institute of Analysis and Number Theory

Graz, June 2021

AFFIDAVIT

I declare that I have authored this thesis independently, that I have not used other than the declared sources/resources, and that I have explicitly indicated all material which has been quoted either literally or by content from the sources used. The text document uploaded to TUGRAZonline is identical to the present doctoral thesis.

Date, Signature

In memory of my father Ali Abdulkader Saeed

Contents

Abstract

Let R be a finite commutative ring with unity $1 \neq 0$. The ring of dual numbers over the ring R is $R[\alpha] = R[x]/(x^2)$, where α denotes $x + (x^2)$. We investigate four distinct, but related, topics concerning polynomial functions on rings of dual numbers.

Firstly, 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 $n \leq p$ (p prime).

The second topic regards the connection between the group of unit-valued polynomial functions $\mathcal{F}(R)^\times$ and the group of polynomial permutations on $R[\alpha]$. Since R is finite, $\mathcal{F}(R)^\times$ is the group of units in $\mathcal{F}(R)$, the ring of polynomial functions with pointwise addition and multiplication. We show that the group $\mathcal{P}_R(R[\alpha])$, consisting of those polynomial permutations of $R[\alpha]$ represented by polynomials in $R[x]$, is embedded in a semidirect product of $\mathcal{F}(R)^\times$ by the group $\mathcal{P}(R)$ of polynomial permutations on R. This embedding leads to a normal embedding of the pointwise stabilizer group of R (in the group of polynomial permutations on the ring $R[\alpha]$), $St_\alpha(R)$, in this semidirect product. Also, we count unit-valued polynomial functions on the ring of integers modulo p^n and obtain canonical representations for these functions.

In the third topic, we consider ideals of the polynomial ring $R[x]$ with the property of being closed under products of formal derivatives of polynomials. For a large class of local principal ideal rings, we show that the null ideal (consisting of polynomials inducing the zero function on R) has this property. As a consequence, we prove, for this class of rings, that the stabilizer group $St_\alpha(R)$ is isomorphic to a certain factor group of the additive group of the null ideal.

Finally, we investigate, for a positive integer k, the polynomial functions on the ring of dual numbers of k variables over R, $R[\alpha_1, \ldots, \alpha_k]$, where $\alpha_i \, \alpha_j = 0$ for every i, j. In most cases, such an investigation can be reduced to the case $k = 1$. We also show that some groups of polynomial permutations on $R[\alpha_1, \ldots, \alpha_k]$ are independent of the number of variables k. In particular, we prove that the pointwise stabilizer group of R in the group of polynomial permutations on $R[\alpha_1, \ldots, \alpha_k]$, $St_{\alpha_1,\ldots,\alpha_k}(R)$, is isomorphic to $St_\alpha(R)$.

Kurzfassung

Sei R ein endlicher kommutativer Ring mit Einselement $1 \neq 0$. Der Ring der Doppelzahlen über dem Ring R ist $R[\alpha] = R[x]/(x^2)$, wobei α für $x + (x^2)$ steht. Wir untersuchen vier verschiedene, aber zusammenhängende, Themen in Bezug auf Polynomfunktionen auf Ringen der Doppelzahlen.

Erstens charakterisieren wir Nullpolynome und Permutationspolynome auf $R[\alpha]$ mit Hilfe der durch ihre Koordinatenpolynome induzierten Funktionen ($f_1, f_2 \in R[x]$, wobei $f = f_1\alpha + f_2$) und ihrer formalen Ableitungen auf R. Wir leiten explizite Formeln für die Anzahl von Polynomfunktionen und die Anzahl von Polynompermutationen auf $\mathbb{Z}_{p^n}[\alpha]$ her in dem Fall, dass $n \leq p$ (p eine Primzahl).

Das zweite Thema betrifft den Zusammenhang zwischen der Gruppe $\mathcal{F}(R)^\times$ jener Polynomfunktionen, die R auf die Einheiten abbilden, und der Gruppe der Polynompermutationen auf $R[\alpha]$. Da R endlich ist, ist $\mathcal{F}(R)^\times$ die Einheitengruppe von $\mathcal{F}(R)$, des Rings der Polynomfunktionen mit punktweiser Addition und Multiplikation. Wir zeigen, dass die Gruppe $\mathcal{P}_R(R[\alpha])$ jener Polynompermutationen von $R[\alpha]$, die als Polynome in $R[x]$ dargestellt werden können, in einem semidirekten Produkt der Gruppe $\mathcal{P}(R)$ der Polynompermutationen auf R mit $\mathcal{F}(R)^\times$ eingebettet ist. Diese Einbettung führt zu einer normalen Einbettung der punktweisen Stabilisatorgruppe von R (in der Gruppe von Polynompermutationen auf dem Ring $R[\alpha]$), $St_\alpha(R)$, in dieses semidirekte Produkt. Wir zählen ebenfalls die Polynomfunktionen, die auf die Einheiten abbilden, auf dem Ring der ganzen Zahlen modulo p^n und erhalten kanonische Darstellungen für diese Funktionen.

Das dritte Thema handelt von Idealen des Polynomrings $R[x]$ mit der Eigenschaft, unter Produkten von formalen Ableitungen von Polynomen abgeschlossen zu sein. Wir zeigen für eine große Klasse lokaler Hauptidealringe, dass das Nullideal von R (bestehend aus Polynomen, die auf 0 abbilden), diese Eigenschaft hat. Folglich ist, für Ringe dieser Klasse, die punktweise Stabilisatorgruppe $St_\alpha(R)$ isomorph zu einer bestimmten Faktorgruppe der additiven Gruppe des Nullideals von R.

Schlussendlich untersuchen wir, viertens, für eine positive ganze Zahl k die Polynomfunktionen auf dem Ring der Doppelzahlen in k Variablen über R, $R[\alpha_1, \ldots, \alpha_k]$, wobei $\alpha_i\,\alpha_j = 0$ für alle i, j. Meist kann eine solche Untersuchung auf den Fall $k = 1$ reduziert werden. Wir zeigen, dass bestimmte Gruppen von Polynompermutationen auf

$R[\alpha_1, \ldots, \alpha_k]$ von der Zahl der Variablen k unabhängig sind. Insbesondere beweisen wir, dass die punktweise Stabilisatorgruppe von R in der Gruppe der Polynompermutationen von $R[\alpha_1, \ldots, \alpha_k]$, $St_{\alpha_1,\ldots,\alpha_k}(R)$, zu $St_\alpha(R)$ isomorph ist.

Acknowledgements

I would like to express my deep thanks and appreciation to my supervisor Prof. Sophie Frisch for giving me a terrific chance to continue my career in mathematics, and for her significant efforts, guidance, constructive advice that helped me to achieve this work.

Great thanks are due to Prof. Irena Swanson, Dr. Mohammed Boudjada, Dr. Chimere Anabanti, Dr. Kwok Chi Chim and Dr. Paolo Leontti for reading earlier versions of my preprints.

Many thanks are due to Prof. Günther Eigenthaler for the valuable bunch of papers that were very helpful while writing this study and would open up a way for future works.

I am also so grateful to the Austrian Science Fund FWF for the financial support during my long stay in Graz.

Also, I would like to thank all the members of the Institute of Analysis and Number Theory of TU Graz University. Particular thanks are due to Prof. Peter Grabner, Prof. Robert Tichy, Mag. Hermine Panzenböck, M.Sc. Michael Muhr, Amtsrätin Irene Pfeifer-Wilfinger Mag. Jochen Resch and our former colleague Dr. Roswitha Risnner.

Special thanks go to my friends Dr. Amran Alagbary, Dr. Aiman Awwad, Dr. Ayman Najeeb, Dr. Mahadi Ddamulira, Dr. Shaher Zyoud, Dr. Damir Ferizovic, MTech. Ziad Abdulwahed, MSc. Mohammed Sultan and Mohammed S. Kouidri for their support and encouragement.

Finally, my deep sense of love and appreciation go to my mother, brothers and sisters.

Preface

This thesis includes four articles of the author. In addition to the introduction chapter, the thesis contains another four chapters each consisting of a reprint of an article. One of the articles is published in Applicable Algebra in Engineering, Communication and Computing journal; two of them are accepted for publication whereas the last one is submitted. The order of the articles is the same as they appear in the coming list of publications.

List of Puplications

1. Hasan Al-Ezeh, Amr Al-Maktry and Sophie Frisch, *Polynomial functions on rings of dual numbers over residue class rings of the integers.* To appear in Mathematica Slovaca, `https://arxiv.org/abs/1910.00238`.

2. Amr A. Al-Maktry, *On the group of unit-valued polynomial functions.* Applicable Algebra in Engineering, Communication and Computing, (2021), `https://doi.org/10.1007/s00200-021-00510-x`.

3. Amr A. Al-Maktry, *On a property of the ideals of the polynomial ring* $R[x]$. To appear in the International Electronic Journal of Algebra.

4. Amr A. Al-Maktry, *Polynomial functions over dual numbers of several variables.* Submitted, `https://arxiv.org/abs/2002.01304`.

List of Symbols

$\mathcal{F}(A)$	the monoid of polynomial function on the ring A	(on page 1)
$\mathcal{P}(A)$	the group of polynomial permutations on the ring A	(on page 1)
$[f]_A$	the polynomial function on A induced by f	(on page 1)
$\|B\|$	the number of elements of an arbitrary set B	(on page 5)
$\mathbb{Z}_m$	the ring of integers modulo m	(on page 13)
$[f]_m$	the polynomial function on $\mathbb{Z}_m$ induced by f	(on page 16)
$R[\alpha]$	the ring of dual numbers over R	(on page 16)
N_R	the null ideal on the ring R	(on page 18)
N'_R	the ideal of null polynomials whose null formal derivatives	(on page 18)
$St_\alpha(R)$	the stabilizer group of R in the group $\mathcal{P}(R[\alpha])$	(on page 25)
$\mathcal{P}_R(R[\alpha])$	the subgroup of $\mathcal{P}(R[\alpha])$ induced by polynomials on R	(on page 27)
$\mathcal{F}(R)^\times$	the group of unit-valued polynomial functions on R	(on page 47)
θ	a homomorphism from $\mathcal{P}(R)$ into $Aut(\mathcal{F}(R)^\times)$	(on page 47)
$\mathcal{P}(R) \ltimes_\theta \mathcal{F}(R)^\times$	the semidirect product of $\mathcal{F}(R)^\times$ by $\mathcal{P}(R)$	(on page 50)
$N(\mathfrak{m})$	the ideal of polynomials vanishing on the maximal ideal $\mathfrak{m}$	(on page 64)
$R[\alpha_1, \ldots, \alpha_k]$	the ring of dual numbers of k variables	(on page 77)
$St_{\alpha_1,\ldots,\alpha_k}(R)$	the stabilizer group of R in the group $\mathcal{P}(R[\alpha_1,\ldots,\alpha_k])$	(on page 86)

1 Introduction

1.1 A general overview

Let R be a commutative ring with unity $1 \neq 0$. A function $F\colon R \longrightarrow R$ is said to be a polynomial function on R if there is a polynomial $f \in R[x]$ such that $f(a) = F(a)$ for every $a \in R$. In this case, we say that f induces (represents) F. Further, such a polynomial function is called a polynomial permutation when it is a bijection while f is called a permutation polynomial on R. We insist here to distinguish between a polynomial (permutation polynomial) $f \in R[x]$ and a polynomial function (polynomial permutation) $F \in \mathcal{F}(R)$, because a polynomial (permutation polynomial) f induces a unique polynomial function (polynomial permutation), whereas a polynomial function (polynomial permutation) F can be represented by a class of polynomials. To relate a polynomial $f \in R[x]$ to its induced polynomial function F on R, we use $[f]_R$ for F instead or just $[f]$ when the ring R is understood. The set $\mathcal{F}(R)$ of all polynomial functions is a monoid with respect to composition, its group of units $\mathcal{P}(R)$ consists of polynomial permutations.

Rédei and Szele have proved that every function on the ring R is polynomial function if and only R is a finite field [75, 80]. In fact, they do not require R to have a unity, though when R is a ring with unity $1 \neq 0$, we notice when R has nonzero zerodivisors that the function

$$F(r) = \begin{cases} 1 & if\ r \neq 0, \\ 0 & if\ r = 0 \end{cases}$$

is not a polynomial function (otherwise every nonzero zerodivisor is invertible, which is a contradiction). On the other hand, when R is infinite domain, every non-constant function that maps infinitely many elements of R into 0 is not a polynomial function; in particular, the function

$$F(r) = \begin{cases} 0 & if\ r \neq 0, \\ 1 & if\ r = 0 \end{cases}$$

is not a polynomial function (otherwise F is induced by a non-constant polynomial f with infinitely many roots, which is impossible).

Polynomial functions and polynomial permutations have been widely studied over different algebraic structures like algebras, groups and lattices (see for example [25, 44, 59, 26]). However, we try here to have only a glimpse on the development of the theory of polynomial functions and polynomial permutations on finite commutative rings.

Due to Nechaev [63], to explore polynomial functions on finite rings, there are two essential problems to tackle:

- Representing and counting the elements of $\mathcal{F}(R)$.
- Representing and counting the elements of $\mathcal{P}(R)$.

Unlikely, these tasks are not always easy. One can see this in the work of Kempner, the first mathematician who considered polynomial functions on a finite ring that is not a field [43]. He extensively examined polynomial functions on the ring of integers modulo m, $\mathbb{Z}_m$, and derived formulas for $\mathcal{F}(\mathbb{Z}_m)$ and $\mathcal{P}(\mathbb{Z}_m)$ in terms of his function $\mu(m)$. However, his results and arguments are somewhat lengthy and sophisticated.

Over decades, several authors have been influenced by Kempner's work (see for example [17, 41, 81, 62]). They obtained equivalent results and easier proofs and contributed to the subject as well. In most of these works, the authors reduced the problem to examine polynomial functions modulo a prime power. For instance, Carlitz [17] obtained necessary and sufficient conditions for a function to be a polynomial function on $\mathbb{Z}_{p^n}$; and in [41] Keller and Olson gave canonical representations for polynomial functions by means of the falling factorial. While Singmaster [81] derived a counting formula for polynomial functions on $\mathbb{Z}_m$ independent from Kempner's function $\mu(m)$ (the smallest positive integer k such that m divides $k!$) and represented them canonically only in terms of the power of the indeterminate x.

Likewise, some researchers characterized the polynomial functions on more general classes of rings like Galois rings and local principal rings [15, 63]. At the end of the last century, Frisch [29] characterized the polynomial functions on the class of suitable rings (see Section 2.1). Amazingly, all finite local rings that have been examined previously are suitable and they all satisfy the following equation when they are not fields

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

where q is the number of elements in the residue field of R. The previous equation has been proved for any finite local ring that is not a field by Jiang [40]. In an interesting paper but less well-known, Maxson and van der Merwe [56] determined an upper bond for $|\mathcal{F}(R)|$. They, also proved this upper bound to be optimal for a class of local rings satisfying some condition and they noticed that Galois rings are in this class, though they

overlooked to notice that this class coincides with the class of the so-called "suitable" discussed above.

Meanwhile, many results have been achieved concerning only the permutation polynomials and their applications especially on finite fields [50, 60]. Nevertheless, we expose here briefly some aspects of these results with some examples from the literature. The main aspect is to find new types (classes) of permutation polynomials [18, 49]. Another aspect is investigating and counting permutation polynomials on a finite field $\mathbb{F}_q$ that also permute the elements of the ring $M_n(\mathbb{F}_q)$ of $n \times n$ matrices [14, 13]. A third one is to study the structures of some polynomial permutations groups [61, 87].

1.2 A short summary of the theory of permutation polynomials and their applications

Apart from the fact that Kempner has counted polynomial permutations on $\mathbb{Z}_{p^n}$, Nöbauer was the first mathematician who investigated intensively polynomial permutations and permutation polynomials not only on $\mathbb{Z}_{p^n}$ but also on other structures from different aspects. His work had a significant effect on other researchers (see for example [84, 31, 29, 89, 36]). We cannot here provide an adequate account of his tremendous contributions on this area, though we offer the readers to consult his book with Lausch [47]; and rather we give a brief outline of his results on polynomial permutations and permutation polynomials on $\mathbb{Z}_{p^n}$ and their influence on other mathematicians. In [69], Nöbauer has explicitly spelled out and proved the following criterion: "a polynomial $f \in \mathbb{Z}$ is a permutation polynomial on $\mathbb{Z}_{p^n}$ $(n > 1)$ if and only if

1. f is a permutation polynomial on $\mathbb{Z}_p$;

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

Here, we may indicate that some authors [62, 77] referred to the previous criterion as a corollary of a more general theorem mentioned in Hardy and Wright's book [39]. Later, in less well-known paper, Nöbauer has generalized this criterion to permutation polynomials of several variables over arbitrary ring [70]. As a consequence of his general result is the following criterion on permutation polynomials on finite local ring (R, M) "a polynomial $f \in R[x]$ is a permutation polynomial on R if and only if

1. f is a permutation polynomial on R/M;

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

The power of the previous criterion can be seen in [36], when the authors obtained the following characterization of permutation polynomials on the finite local ring R with the residue field $R/M \cong \mathbb{Z}_2$, which is a generalization of the main result of [77]:

"a polynomial $f = \sum_{i\geq 0} a_i x^i \in R[x]$ is a permutation polynomial on R if and only if $a_1 = 1 \mod M$, $a_2 + a_4 + \cdots = 0 \mod M$ and $a_3 + a_5 + \cdots = 0 \mod M$".

Nöbauer [65], also considered the structure of the group of polynomial permutations on $\mathbb{Z}_{p^n}$, $\mathcal{P}(\mathbb{Z}_{p^n})$, and showed that $\mathcal{P}(\mathbb{Z}_{p^n})$ is isomorphic to the wreath product of a subgroup of $\mathcal{P}(\mathbb{Z}_{p^{n-1}})$ (defined below) by the symmetric group S_p, that is,

$$\mathcal{P}(\mathbb{Z}_{p^n}) \cong H \wr S_p,$$

where H is the subgroup of $\mathcal{P}(\mathbb{Z}_{p^{n-1}})$ consisting of elements that can be uniquely represented by polynomials of the form

$$a_0 + a_1 x + a_2 p x + \cdots + a_{n-1} p^{n-2} x^{n-1},$$

$0 \leq a_0, a_1 < p^{n-1}$ with $a_1 \not\equiv 0 \pmod{p}$; and $0 \leq a_i < p^{n-i-v_p(i!)}$ for $i > 1$, where $v_p(i!)$ is the exponent of p in the prime factorization of $i!$. The previous wreath product inspired other researchers to find a more general relation for finite local rings. Later on, Frisch [29] showed for a finite local ring, when the maximal ideal M satisfies $M^2 = \{0\}$, that

$$\mathcal{P}(R) \cong (\mathbb{F}_q^* \ltimes (M, +)) \wr S_q.$$

Recently, Görcsös, Horváth and Mészáros [36] succeeded to describe $\mathcal{P}(R)$ for an arbitrary finite local ring R as the following

$$\mathcal{P}(R) \cong \mathcal{P}(M) \wr S_q,$$

where $\mathcal{P}(M)$ is a subset of $\mathcal{F}(R)$ consisting of polynomial functions that permute the elements of M. Furthermore, they employed their structure relation to find a general counting formula for the order of $\mathcal{P}(R)$ with the maximal ideal M satisfying the condition $M^q = \{0\}$.

The notions of permutation polynomials have been appeared in different areas of algebra over several decades of years. Sometimes they appear as R automorphisms of $R[x]$ (see for example [34, 38]), and sometimes as automorphisms of combinatorial objects [10, 11]. Also, under some circumstances, they occur as level transitive automorphisms of binary trees [1]. The utilization of permutation polynomials influenced other areas of research; many applications of permutation polynomials occurred in computer science (for example [83, 85, 82]). Another influence of permutation polynomials can be seen in

the theory of the p-adic dynamical systems [6, 27].

1.3 The null ideal

To count and characterize the polynomial functions on a ring R one needs to investigate the null ideal N_R, in other words, to investigate the ideal of the polynomial ring $R[x]$ consisting of all polynomials that vanish on R. Because the map $\phi\colon R[x] \longrightarrow \mathcal{F}(R)$ defined by $\phi(f) = F$, where $F(r) = f(r)$ for every $r \in R$, is an epimorphism with $\ker\phi = N_R$ and from this one infers that $|\mathcal{F}(R)| = [R[x]\colon N_R]$. Though, finding this index is not an easy task. Simplifying such a difficulty requires finding a monic-null polynomial of minimal degree k, where a polynomial is called null whenever it is an element of the null ideal N_R. The minimal monic-null polynomial on R always exists since the set

$$\mathcal{A} = \{n\colon n = \deg f \text{ for some monic } f \in N_R\}$$

is not empty. Indeed, $\deg\prod_{r\in R}(x-r) = |R| \in \mathcal{A}$, and it has therefore a minimal element k. Then one can choose the minimal monic-null polynomial to be any monic-null polynomial corresponding to the number k in the definition of the set $\mathcal{A}$. This minimal monic-null polynomial guarantees that every element of $\mathcal{F}(R)$ can be represented (not necessarily uniquely) by a polynomial of degree smaller than k. After that, the rest is to find the number of all non-monic null polynomials of degree smaller than k say l, since then

$$|\mathcal{F}(R)| = [R[x]\colon N_R] = \frac{|R|^k}{l}.$$

For example, Kempner [43] showed that $\prod_{j=0}^{\mu(m)-1}(x-j)$ is a minimal-null polynomial on $\mathbb{Z}_m$, where $\mu(m)$ stands for the smallest positive integer k such that m divides $k!$, the Kempner's function. Then he surveyed all other null polynomials on $\mathbb{Z}_m$ of degree less than $\mu(m)$. Latterly, Singmaster [81] managed to represent canonically these null polynomials as sums of raising factorials.

The problem of finding a generating set for the null ideal N_R was of interest to many researchers. For instance, when $R = \mathbb{Z}_{p^n}$, Dickson [22] showed that $N_{\mathbb{Z}_{p^n}} = ((x^p - x), p)^n$ for $n \leq p$; and Bandiny [9] found a set of generators for $N_{\mathbb{Z}_{p^n}}$ for every $n > p$. Some others considered this problem more generally. Gilmer [35] proved that for a zero-dimensional local ring (R, M) that N_R is principal if and only if either R/M is an infinite field or R is a finite field. Also, he showed that for a finite ring A, N_A is a principal ideal if and only if A is a direct sum of finite fields. A direct consequence of this $N_{\mathbb{Z}_m}$ is principal if and only if m is square-free. Recently, Rogers and Wickham [78] managed to find a set of generators of N_R for a wide class of principal finite local rings. Further, they reduced

the problem to find only the generators of the ideal $N(M)$ consisting of all polynomials vanishing on the maximal ideal M for any Henselian local ring of finite residue field.

An exciting property of the null ideal is being a full ideal, where an ideal I of $R[x]$ is a full ideal if and only if it satisfies $g \circ f \in I$ for every $g \in I$ and $f \in R[x]$ (see for example [84]). In [71, 72], Nöbauer developed some arithmetical theory on full ideals.

Since every ring can be viewed as an algebra over it self, the null ideal N_R can be considered as a special case of a more-general one; namely, when R is an A-algebra, the ideal

$$N_R^A = \{f \in A[x] \colon f(r) = 0 \text{ for every } r \in R\},$$

of $A[x]$. Such an ideal appeared implicitly in [14, 13, 12] within investigating scalar polynomial permutations and polynomial functions of algebra of $n \times n$ matrices over finite fields; and explicitly within investigating polynomial permutations of finite algebra over a finite field $\mathbb{F}_q$ [7, 8]. It is apparent that the ideal N_R^A is always a full ideal of $A[x]$. However, when $A = \mathbb{F}_q$, Ashlock [7] showed that every full ideal $I \in \mathbb{F}_q[x]$ is the null ideal $N_R^{\mathbb{F}_q}$, where $R = \mathbb{F}_q[x]/I$. Also, this general form of the null ideal played an effective role in the last decade in the theory of integer-valued polynomials (see for example [74, 73, 79]). It should be mentioned that the terminology of null ideal has been used in a different sense in some contexts with respect to a fixed element rather than the whole ring R (see for example [28, 30, 76]).

1.4 Polynomial functions on dual numbers over finite rings

1.4.1 Dual numbers and their polynomial functions

For a commutative ring R, the ring of dual numbers over the ring R is quotient ring $R[x]/(x^2)$, or equivalently, the ring $R[\alpha] = \{a+b\alpha : a, b \in R\}$ with $\alpha^2 = 0$, where α stands for $x+(x^2)$. This ring has a nice feature, because it appears in dissimilar forms. It can be viewed as the idealization of the ring R by its self, that is, the ring $R(+)R$ is isomorphic to the ring of dual numbers over R. Also, it can be considered as the ring of all 2×2 matrices of the form $\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}$ (equivalently, of the form $\begin{pmatrix} a & 0 \\ b & a \end{pmatrix}$), where $a, b \in R$. The ring of dual numbers, $R[\alpha]$, is an R algebra with basis $\{1_R, \alpha\}$, but, then R is embedded canonically in $R[\alpha]$ and evidently $R[\alpha]$ is a ring extension of R. This ring extension is known to be minimal if and only if R is a field [24]. Such an extension has been called in the literature the trivial extension of the ring R by R (see for example [52]). But, this

term "trivial" should not give the reader a negative impression about the importance of dual numbers as this ring has been employed to construct counterexamples in the theory of rings (see for example [9]). Also, we will see that the ring $R[\alpha]$ has its own figure that differs from R. It may not have a property that is valid for R (see Propositions 2.2.9 and 5.2.9) or it has a property that may not be valid for R (see Proposition 4.3.20).

In this thesis, we investigate the polynomial functions on the ring $R[\alpha]$ by means of the polynomial functions on the ring R that are induced by polynomials over R and by their formal derivatives. Since every finite ring is a direct product of finite local rings, in most cases, we restrict our investigation to polynomial functions on the ring of dual numbers over a finite local ring R. However, the behavior of polynomial functions of dual numbers over finite fields is somewhat different from the general case. Therefore, on several occasions, we have to distinguish between R being a field and R being a local ring with non-zero maximal ideal.

To illustrate our approach for inspecting the polynomial functions on dual numbers over finite ring R, let us consider a polynomial $f \in R[\alpha][x]$. Then f can be expressed uniquely as $f = f_1 + \alpha\, f_2$ for some $f_1, f_2 \in R[x]$. If we take the value of f on $a + b\,\alpha$, where $a, b \in R$, we have by Taylor formula and the fact $\alpha^2 = 0$,

$$f(a + b\,\alpha) = f_1(a) + (bf_1'(a) + f_2(a))\,\alpha\,. \tag{1.1}$$

This shows that the polynomial function $[f]_{R[\alpha]}$ depends not only on the polynomial functions $[f_1]_R$ and $[f_2]_R$ but also on the polynomial function $[f_1']_R$. As a result of the previous discussion, we have the polynomial f is a null polynomial on $R[\alpha]$ if and only if $f, f_1', f_2 \in N_R$ (see also Theorem 2.3.5). Then, the collection of all polynomials $f \in N_R$ such that $f' \in N_R$ is an ideal of $R[x]$ which we denote by N_R'. Therefore, more explicitly,

$$N_{R[\alpha]} = N_R' + N_R\,\alpha\,.$$

In Chapter 2, we see that the examination of $\mathcal{F}(R[\alpha])$ can be accomplished by examining the composition rings $(R[x]/N_R', +, \cdot, \circ)$ and $(R[x]/N_R, +, \cdot, \circ)$ instead. To see the significant difference between $R[x]/N_R'$ and $R[x]/N_R$ with respect to the ring $R[\alpha]$, we consider, $R = \mathbb{Z}_{p^n}$, $f(x) = x$ and $g(x) = x + p^{n-1}(x^p - x)$. Simple argument shows that f and g induce the same function on $\mathbb{Z}_{p^n}$. However, they induce distinct functions on $\mathbb{Z}_{p^n}[\alpha]$, as $f(\alpha) = \alpha \neq (1 - p^{n-1})\,\alpha = g(\alpha)$ since $\alpha^2 = 0$. Indeed, $f \equiv g \mod N_R$ but $f \not\equiv g \mod N_R'$ (see Corollary 2.3.7). In fact $R[x]/N_R'$ is the set of all polynomial functions on $R[\alpha]$ that are represented by polynomials over R whereas it is a evident that $R[x]/N_R$ is the set of polynomial functions on R, $\mathcal{F}(R)$. In Proposition 2.3.10, we

connect the number of elements of $\mathcal{F}(R[\alpha])$ with those of $R[x]/N'_R$ and $R[x]/N_R$, that is,

$$|\mathcal{F}(R[\alpha])| = \big[R[x]\colon N'_R\big]\big[R[x]\colon N_R\big].$$

Also, the number $\big[R[x]\colon N'_R\big]$ is shown to be the number of all distinct pairs $([f]_R, [f']_R)$ where $f \in R[x]$.

Such investigation leads to more outstanding for the polynomial functions on R its self and answers some questions of interest that have been overlooked in the literature. Here are some natural questions arise for a given fixed polynomial function F on R and any polynomial $f \in R[x]$ inducing F on R:

1. How many pairs of functions of the form $(F, [f']_R)$ are there? Or at least can we interpret this number as the order of an algebraic structure?

2. Does this number depend on the function F?

Although these questions are simple, it seems they have not been tackled before. Answering these questions increases our knowledge not only on the polynomial functions on $R[\alpha]$ but also on those on R. In other words, examining polynomial functions on $R[\alpha]$ increases our knowledge on the polynomial functions on R. In all circumstances, this number is shown to be independent of the choice of the polynomial function F. We describe this number as the order of a group of polynomial permutations on $R[\alpha]$ (see Corollary 2.7.6 for the case $R = \mathbb{Z}_{p^n}$, and Proposition 5.4.14 for the general case). In particular, when $R = \mathbb{Z}_{p^n}$, we find this number explicitly for $n \leq p$ (Theorem 2.8.8).

The group of polynomial permutations of order that equals the number of pairs of functions discussed in the previous paragraph consists of all polynomial permutations that stabilize the elements of R pointwisely which we denote by $St_\alpha(R)$. Therefore, for the case $M \neq \{0\}$, we have

$$|St_\alpha(R)| = |\{(F, [g']_R)\colon g \in R[x] \text{ with } [g]_R = F\}|.$$

The stabilizer group $St_\alpha(R)$ will play an important role through this study, and we will find out some of its properties. For instance, we represent the elements of the stabilizer group $St_\alpha(R)$ by polynomials from the set $x + N_R$. Another interesting property of the stabilizer group $St_\alpha(R)$ is being a normal subgroup of the group $\mathcal{P}_R(R[\alpha])$ of polynomial permutations on $R[\alpha]$ that are induced by polynomials over R. Also, in the case $M \neq \{0\}$, we show that $|St_\alpha(R)| = [N_R\colon N'_R]$ (this is another description of the number of pairs of polynomial functions mentioned previously). Further, for a wide class of finite local rings which are not fields, we prove that $St_\alpha(R) \cong N_R/N'_R$ (Chapter 4).

1.4.2 Unit-valued polynomial functions

The set of polynomial functions $\mathcal{F}(R)$ is a commutative ring with identity, where addition and multiplication defined pointwisely. Its group of units $\mathcal{F}(R)^\times$ consists of all unit-valued polynomial functions (with respect to the pointwise multiplication "$\cdot$") since we consider R to be finite (Chapter 3). A polynomial $f \in R[x]$ that induces a unit-valued polynomial function is called a unit-valued polynomial, equivalently, when $f(R) \subseteq R^\times$, where $R^\times$ is the group of units of R. Unit-valued polynomials appeared in the literature within inspecting other mathematical objects. For example, they have been used to check non-D-rings (see for example [53, 54, 58]), where a commutative ring R is a non-D-ring whenever there exists a non-constant unit-valued polynomial $f \in R[x]$. Another example, that we already have seen before in the criterion for permutation polynomials on finite local rings (see section 1.2). Indeed, the condition on f' requires it to be a unit-valued polynomial on R. Also, Nöbauer studied a related monoid $\mathcal{F}(\mathbb{Z}_{p^n}^\times)$ (with respect to composition) consisting of all polynomial functions from $\mathbb{Z}_{p^n}^\times$ to $\mathbb{Z}_{p^n}^\times$ that are induced by polynomials over $\mathbb{Z}_{p^n}$, namely,

$$\mathcal{F}(\mathbb{Z}_{p^n}^\times) = \{F\colon F(\mathbb{Z}_{p^n}^\times) = G(\mathbb{Z}_{p^n}^\times) \subseteq \mathbb{Z}_{p^n}^\times \text{ for some } G \in \mathcal{F}(\mathbb{Z}_{p^n})\}.$$

Evidently, the restriction of every element of $\mathcal{F}(\mathbb{Z}_{p^n})^\times$ to $\mathbb{Z}_{p^n}^\times$ is an element of $\mathcal{F}(\mathbb{Z}_{p^n}^\times)$, though we claim that $|\mathcal{F}(\mathbb{Z}_{p^n})^\times| > |\mathcal{F}(\mathbb{Z}_{p^n}^\times)|$. In fact, each element of $\mathcal{F}(\mathbb{Z}_{p^n}^\times)$ can be viewed as the restriction of different elements of $\mathcal{F}(\mathbb{Z}_{p^n})^\times$ to $\mathbb{Z}_{p^n}^\times$. For this, we recall from [66, Satz I] that: "every polynomial function on $\mathbb{Z}_{p^n}$ can be obtained uniquely by the relation

$$i + px \mapsto a_i + pb_{i\,0} + \sum_{j=1}^{e} b_{i\,j} p^j x^j \mod p^n, \quad 0 \le i < p, \quad 0 \le x < p^{n-1}$$

with $0 \le a_i < p$, $0 \le b_{i\,0} < p^{n-1}$ and $0 \le b_{i\,j} < p^{n-j-v_p(j!)}$ for $1 \le j \le e$, where e is the largest natural number j such that $j + v_p(j!) < n$". From the previous relation, one obtain all the elements of $\mathcal{F}(\mathbb{Z}_{p^n})^\times$ by the restriction $1 \le a_i < p$; and as Nöbauer noticed [67], we obtain all the elements of $\mathcal{F}(\mathbb{Z}_{p^n}^\times)$ by the restrictions $1 \le i < p$ and $1 \le a_i < p$. But, then our claim follows easily.

In the thesis, we try to shed light on the interplay between the group of unit-valued polynomial functions $(\mathcal{F}(R)^\times, \cdot)$, the group of polynomial permutations $(\mathcal{P}(R), \circ)$ and the group $(\mathcal{P}_R(R[\alpha]), \circ)$ of polynomial permutations on $R[\alpha]$ consisting of elements that are induced by polynomial on R rather than $R[\alpha]$. More precisely, we show that $\mathcal{P}_R(R[\alpha])$ is embedded in a semidirect product of $\mathcal{F}(R)^\times$ by $\mathcal{P}(R)$, $\mathcal{P}(R) \ltimes_\theta \mathcal{F}(R)^\times$, where the homomorphism θ depends on the right action of $\mathcal{P}(R)$ (with respect to composition) on $\mathcal{F}(R)^\times$

(Proposition 3.3.8). Furthermore, we link the group of unit-valued polynomial functions $\mathcal{F}(R)^\times$ to the stabilizer group $St_\alpha(R)$ by embedding $St_\alpha(R)$ in $\mathcal{F}(R)^\times$. In particular, we prove that $St_\alpha(\mathbb{F}_q) \cong \mathcal{F}(\mathbb{F}_q)^\times$ (Theorem 3.4.5). Moreover, the embedding of $St_\alpha(R)$ in $\mathcal{F}(R)^\times$ leads to a normal embedding of $St_\alpha(R)$ in $\mathcal{P}(R) \ltimes_\theta \mathcal{F}(R)^\times$ (Theorem 3.4.12).

The motivation of the construction of this semidirect product spouts from the elementary calculations of the values of the polynomials of $R[x]$ on the elements of $R[\alpha]$ and from the criterion for permutation polynomials (mentioned on page 3). For a simple explanation, let $f, g \in R[x]$ be permutation polynomials on the local ring R. Then, for $a, b \in R$, we have by applying Equation (1.1) two times,

$$f \circ g(a + b\alpha) = f(g(a)) + bg'(a)f'(g(a))\alpha.$$

It is evident that $f \circ g$ is a permutation polynomial on R since f, g are, but then $(f \circ g)' = (f' \circ g)g'$ is a unit-valued polynomial by the criterion for permutation polynomials. Therefore, in terms of polynomial functions, we can assign the pair $([f]_R \circ [g]_R, ([f']_R \circ [g]_R) \cdot [g']_R)$ to the pairs $([f]_R, [f']_R)$ and $([g]_R, [g']_R)$, where $[f]_R, [g]_R, [f]_R \circ [g]_R \in \mathcal{P}(R)$ and $[f']_R, [g']_R, ([f']_R \circ [g]_R) \cdot [g']_R \in \mathcal{F}(R)^\times$. Inspired by the previous statement, we define an operation on $\mathcal{P}(R) \times \mathcal{F}(R)^\times$ by

$$(G_1, F_1)(G_2, F_2) = \big(G_1 \circ G_2, (F_1 \circ G_2) \cdot F_2\big),$$

for each $(G_1, F_1), (G_2, F_2) \in \mathcal{P}(R) \times \mathcal{F}(R)^\times$. We will see in Chapter 3 that this operation defines the semidirect product of $\mathcal{F}(R)^\times$ by $\mathcal{P}(R)$, $\mathcal{P}(R) \ltimes_\theta \mathcal{F}(R)^\times$, mentioned before.

1.4.3 Ideals of polynomials closed under multiplication of formal derivatives

Beyond addition, multiplication and composition of polynomials, the ring of polynomials $R[x]$ is equipped with another operation that occurs normally, namely the differentiation operation. Being strongly influenced by investigating the group $St_\alpha(R)$, we consider the following property of an ideal I of $R[x]$:

$$\text{given } f, g \in I \text{ then } f'g' \in I \text{ as well,}$$

or in terms of words, we consider ideals of polynomial rings closed under products of formal derivatives (Chapter 4). More precisely, we prove that the null ideal over a wide class of finite local rings has this property. Furthermore, such a property is proved to be hold if and only if the map $\psi\colon N_R \longrightarrow St_\alpha(R)$ defined by $\psi(f) = [x + f(x)]$ is an epimorphism with $\ker\phi = N'_R$. As a consequence of this, $St_\alpha(R) \cong N_R/N'_R$ which

interprets the equalities of Proposition 2.7.2 (2b) and Theorem 5.4.12 (2b) for this class of rings in terms of group isomorphisms. In this case, we also learn more about the elements of the group $St_\alpha(R)$ (see Proposition 4.3.8).

1.4.4 Some generalizations

Another tempting objective to achieve is to investigate the polynomial functions on the ring of dual numbers of k variables, $R[\alpha_1, \ldots, \alpha_k]$, obtained from R by joining $\alpha_1, \ldots, \alpha_k$ with $\alpha_i \, \alpha_j = 0$ for $i, j = 1, \ldots, k$. It is not hard to notice that $R[\alpha_1, \ldots, \alpha_k]$ coincides with the ring of dual numbers over R when $k = 1$, that is, $R[\alpha_1] \cong R[\alpha]$. We characterize null polynomials and permutation polynomials on $R[\alpha_1, \ldots, \alpha_k]$ in similar manner like what we do for $R[\alpha]$. For example, we show the null ideal on $R[\alpha_1, \ldots, \alpha_k]$ depends on the ideals N_R and N'_R. In general, all examinations can be reduced to the case $k = 1$ since a polynomial $f \in R[\alpha_1, \ldots, \alpha_k][x]$ can be expressed as $f = f_0 + \sum_{i=1}^{k} f_i \, \alpha_i$, where $f_0, f_1, \ldots, f_k \in R[x]$, and since the polynomials $f_1, \ldots, f_k$ admit the same conditions. Likewise the case $k = 1$, we define the group $\mathcal{P}_R(R[\alpha_1, \ldots, \alpha_k])$ to be the group of all polynomial permutations on $R[\alpha_1, \ldots, \alpha_k]$ represented by polynomials over R and the stabilizer group consisting of all polynomial permutations on $R[\alpha_1, \ldots, \alpha_k]$ that fix the elements of R pointwisely. We show these groups to be independent of the number of variables k, that is,

$$\mathcal{P}_R(R[\alpha_1, \ldots, \alpha_k]) \cong \mathcal{P}_R(R[\alpha]) \quad \text{and} \quad St_{\alpha_1,\ldots,\alpha_k}(R) \cong St_\alpha(R).$$

We already had an overview of the content of the thesis. Nevertheless, we summarize the main points of other chapters. In addition to the introduction chapter, the thesis contains another four chapters. Chapter 2 is the heart of the thesis in which the ideas that either have been employed (Chapters 3 and 4) or have been imitated (Chapter 5) in other chapters.

The main target of Chapter 2 is to investigate the polynomial functions on the ring of dual numbers over finite rings $R[\alpha]$. We give some basic properties of $R[\alpha]$ and its polynomial ring $R[\alpha][x]$, we characterize null polynomials and permutation polynomials on $R[\alpha]$, we define the stabilizer group $St_\alpha(R)$, and obtain counting formulas for the numbers of polynomial functions and polynomial permutations on $R[\alpha]$ in terms of $|\mathcal{F}(R)|$, $|\mathcal{P}(R)|$ and $|St_\alpha(R)|$. Also, we restrict our investigation to dual numbers over the ring of integers modulo p^n, $\mathbb{Z}_{p^n}[\alpha]$, to find explicitly, when $n \leq p$, the number of elements of $St_\alpha(\mathbb{Z}_{p^n})$, $\mathcal{F}(\mathbb{Z}_{p^n}[\alpha])$ and $\mathcal{P}(\mathbb{Z}_{p^n}[\alpha])$. Also, when $n \leq p$, we give canonical representations for the elements of $\mathcal{F}(\mathbb{Z}_{p^n}[\alpha])$.

We show in chapter 3 that the group $\mathcal{P}_R(R[\alpha])$ consisting of polynomial permutations

on $R[\alpha]$ that are induced by polynomial on R is embedded in a semidirect product of $\mathcal{F}(R)^\times$ by $\mathcal{P}(R)$, $\mathcal{P}(R) \ltimes_\theta \mathcal{F}(R)^\times$. Furthermore, we show that the stabilizer group $St_\alpha(R)$ is embedded normally in $\mathcal{P}(R) \ltimes_\theta \mathcal{F}(R)^\times$.

Chapter 4 is an attempt to find out some of the properties of the null ideal N_R in which we consider a class of finite local rings having null ideal satisfying the following property:

$$f'g' \in N_R \text{ whenever } f, g \in N_R.$$

In this case, we show that $St_\alpha(R) \cong N_R/N_R'$ and we infer some facts about the elements of $St_\alpha(R)$.

Beyond carrying over most of the results of Chapter 2 to the polynomial functions on $R[\alpha_1, \ldots, \alpha_k]$, Chapter 5 contains some generalizations of some results of Chapter 2 that proved only for $R = \mathbb{Z}_m$ or for $R = \mathbb{Z}_{p^n}$ (Proposition 5.4.14 and Theorem 5.4.12). Additionally, we show that the group $\mathcal{P}_R(R[\alpha_1, \ldots, \alpha_k])$ of polynomial permutations on $R[\alpha_1, \ldots, \alpha_k]$ represented by polynomials over R and the stabilizer group $St_{\alpha_1,\ldots,\alpha_k}(R)$ do not depend on the number k.

2 Polynomial functions on rings of dual numbers over residue class rings of the integers

The content of this chapter is the accepted paper [2] in Mathematica Slovaca Journal. It is a joint work with Hasan Al-Ezeh and Sophie Frisch.

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 $n \leq p$ (p prime).

Keywords. Finite rings, finite commutative rings, dual numbers, polynomials, polynomial functions, polynomial mappings, polynomial permutations, permutation polynomials, null polynomials

2010 Mathematics Subject Classification: Primary 13F20; Secondary 11T06, 13B25, 12E10, 05A05, 06B10

2.1 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 $f = \sum_{k=0}^{n} c_k x^k \in A[x]$ such that $F(a) = \sum_{k=0}^{n} c_k a^k$ 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 [16, 37].

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 [19, 23].

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.

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:

$$|\mathcal{F}(\mathbb{Z}_{p^n})| = p^{\sum_{k=1}^{n} \mu(p^k)} \quad \text{and} \quad |\mathcal{P}(\mathbb{Z}_{p^n})| = p!p^p(p-1)^p p^{\sum_{k=3}^{n} \mu(p^k)} \quad \text{for} \quad n > 1, \tag{2.1}$$

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 $\sum_{j \geq 1} \lfloor \frac{l}{p^j} \rfloor \geq k$. (Here $\lfloor z \rfloor$ means the largest integer smaller than or equal to z).

Kempner's proof has been simplified [41, 81, 90] and his formulas shown to hold for more general classes of local rings [15, 29, 63] 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 2.8.11 and 2.8.10, do not have this property, except for $n = 1$, see Proposition 2.2.9.

Statements about the number of polynomial functions and permutations that hold for any finite commutative ring A are necessarily less explicit in nature than the counting formulas in

Equation (2.1) on one hand and Theorems 2.8.10 and 2.8.11 on the other hand.

Görcsös, Horváth and Mészáros [36] provide a formula, valid for any finite local commutative ring 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 [40] has determined the ratio of $|\mathcal{P}(A)|$ to $|\mathcal{F}(A)|$, see Remark 2.5.8.

Chen [21], Wei and Zhang [89, 88], Liu and Jiang [51], among others [64, 32] 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 [5].

Beyond number formulas, some structural results about groups of permutation polynomials on $\mathbb{Z}_{p^n}$ are known, due to Nöbauer [66, 67] and others [91, 33].

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 $n \leq p$.

Here is an outline of the paper. After establishing some notation in Section 2.2, we characterize null polynomials on $R[\alpha]$ in Section 2.3 and permutation polynomials on $R[\alpha]$ in Section 2.4, for any finite local ring R. Section 2.5 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 2.6 relates permutation polynomials on $\mathbb{Z}_{p^n}[\alpha]$ to permutation polynomials on $\mathbb{Z}_{p^n}$. Section 2.7 contains counting formulas for the numbers of polynomial functions and polynomials 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 2.8 contains explicit formulas for $|\mathcal{F}(\mathbb{Z}_{p^n}[\alpha])|$ and $|\mathcal{P}(\mathbb{Z}_{p^n}[\alpha])|$ for $n \leq p$. Section 2.9 gives a canonical representation for polynomial functions on $\mathbb{Z}_{p^n}[\alpha]$ for $n \leq p$. The easy special case where R is a finite field is treated en passant in sections 2.3 and 2.4.

2.2 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 2.2.1. *Let R be a ring and $a_0, \ldots, a_n \in R$. The polynomial $f = \sum_{i=0}^{n} a_i x^i \in R[x]$ defines (or induces) a function $F\colon R \longrightarrow R$ by substitution of the variable: $F(r) = \sum_{i=0}^{n} a_i r^i$. A function arising from a polynomial in this way is called a* polynomial function.

If the polynomial function $F\colon R \longrightarrow R$ 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 2.2.2. *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 2.2.3.

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 2.2.4. *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 of R.

Remark 2.2.5. *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 2.2.6. *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* $\mathfrak{m} + \alpha\,R = \{a + b\alpha \colon a \in \mathfrak{m},\ b \in R\}$ *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, $f' = \sum_{k=1}^{n} k a_k x^{k-1}$ for $f = \sum_{k=0}^{n} a_k x^k$.

Lemma 2.2.7. *Let* R *be a commutative, and let* $a, b \in R$*.*

1. *Let* $f \in R[\alpha][x]$ *and* $f_1, f_2 \in R[x]$ *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 2.2.8. *Let* $F \colon R[\alpha] \longrightarrow R[\alpha]$ *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 $\mathbb{Z}_{p^n}$ (p a prime) 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 2.2.9. *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 $\mathfrak{m} = \{ap + b\,\alpha \colon a, b \in \mathbb{Z}_{p^n}\}$ and $K = n + 1$ by Proposition 2.2.6. 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 2.2.9 have been called suitable in a previous paper by the third author [29]. 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 (2.1) 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.

2.3 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 corresponds 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 2.2.4). 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 2.3.1. *Let R be a commutative ring and A an R-algebra, and notation as in Definition 2.2.2. 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. $N_R = \{f \in R[x] \colon f \triangleq 0 \text{ on } R\}$;
2. $N'_R = \{f \in R[x] \colon f \triangleq 0 \text{ on } R \text{ and } f' \triangleq 0 \text{ on } R\}$.

Remark 2.3.2. *Clearly, N_R, N'_R are ideals of $R[x]$, and we have $|\mathcal{F}(R)| = [R[x] \colon N_R]$.*

Example 2.3.3. *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 2.3.10 below.

Lemma 2.3.4. *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. *$\alpha\, f$ is a null polynomial on $R[\alpha]$ if and only if f is a null polynomial on R.*

Proof. Ad (1). By Lemma 2.2.7, for every $a, b \in R$, $f(a + b\,\alpha) = f(a) + bf'(a)\,\alpha$. Thus by Definition 2.3.1, 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 2.2.7. □

Theorem 2.3.5. *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 2.2.7, 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 2.3.4 with Theorem 2.3.5 gives the following criterion.

Corollary 2.3.6. *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 2.3.5, we obtain a criterion that we will frequently use for when two polynomials induce the same polynomial function on the ring of dual numbers.

Corollary 2.3.7. *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 2.3.8. *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 2.3.7. 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 2.3.7 implies that $x \triangleq x + (x^p - x)^n \alpha$ on $R[\alpha]$.

Remark 2.3.9. *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

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

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 2.3.7, and it is clearly onto.

Proposition 2.3.10. *Let R be a finite commutative ring, and let N_R and N_R' be the ideals of Definition 2.3.1. Then the number of polynomial functions on $R[\alpha]$ is*

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

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 $F\colon R \longrightarrow R$, $E\colon R \longrightarrow R$, arising as $([f], [f'])$ for some $f \in R[x]$.*

2. $[R[x]\colon N'_R]$ *is also the number of functions induced on* $R[\alpha]$ *by polynomials in* $R[x]$.

3. $[R[x]\colon N_R]$ *is the number of polynomial functions on* R.

Proof. Everything follows from Theorem 2.3.5. In detail, consider the map φ defined by

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

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 2.3.5, $\ker\varphi = N'_R \times N_R$. Hence, by the first isomorphism theorem,

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

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

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

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

Finally, (2) follows from Corollary 2.3.7, and (3) is obvious. □

Proposition 2.3.10 reduces the question of counting polynomial functions on $R[\alpha]$ to determining $[R[x]\colon N_R]$ and $[R[x]\colon N'_R]$, 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 $n \leq p$ in section 2.8.

The simple case where R is a finite field we can settle right away by recalling from Example 2.3.3 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 $[\mathbb{F}_q[x]\colon N'_{\mathbb{F}_q}] = q^{2q}$ and $[\mathbb{F}_q[x]\colon N_{\mathbb{F}_q}] = q$.

Corollary 2.3.11. *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 2.3.12. *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 $F\colon R[\alpha] \longrightarrow R[\alpha]$ *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 2.3.7, $\alpha\, r_2 \triangleq \alpha\, f_2$ 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 2.3.7, $[g]_R = [f]_R$ and $[g']_R = [f']_R$. □

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

Definition 2.3.13. *For $m \in \mathbb{N}$ let $\mu(m)$ denote the smallest positive integer k such that m divides $k!$. The function $\mu\colon \mathbb{N} \longrightarrow \mathbb{N}$ was introduced by Kempner [42].*

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

Remark 2.3.14. *It is easy to see that m divides the product of any $\mu(m)$ consecutive integers.*

As Kempner [43] 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 2.3.15. *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 2.3.4, 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 $f'(x) = \sum_{i=0}^{2\mu(m)-1} \frac{(x)_{2\mu(m)}}{x-i}$. Each term $\frac{(x)_{2\mu(m)}}{x-i}$ is divisible by a polynomial of the form $\prod_{j=0}^{\mu(m)-1}(x-c-j)$. Thus $\frac{(x)_{2\mu(m)}}{x-i}$ is a null polynomial on $\mathbb{Z}_m$ by Remark 2.3.14. 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 $n \leq p$, 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 2.3.16. *Let $n \leq p$. 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 $f'(x) = \sum_{i=0}^{(n+1)p-1} \frac{(x)_{(n+1)p}}{x-i}$, 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 $\prod_{j=0}^{p-1}(x-c-j)$. Hence the claim. □

Combining Theorem 2.3.15 with Proposition 2.3.12 and Remark 2.3.14, 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 2.9.2 and 2.9.4).

Corollary 2.3.17. *Let $F\colon \mathbb{Z}_m[\alpha] \longrightarrow \mathbb{Z}_m[\alpha]$ 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 $f = f_1 + \alpha\, f_2$, 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 2.3.11 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 2.3.18. *Let $\mathbb{F}_q$ be a finite field with q elements. Every polynomial function $F\colon \mathbb{F}_q[\alpha] \longrightarrow \mathbb{F}_q[\alpha]$ can be represented uniquely as a polynomial*

$$f(x) = \sum_{i=0}^{2q-1} a_i x^i + \sum_{j=0}^{q-1} b_j x^j\, \alpha \;\; \textit{for } a_i, b_j \in \mathbb{F}_q. \tag{2.2}$$

Proof. We note that the polynomials $(x^q - x)^2$ and $(x^q - x)$ satisfy the conditions of Proposition 2.3.12. Thus every polynomial function on $\mathbb{F}_q[\alpha]$ is represented by a polynomial as in Equation (2.2).

Since there are exactly q^{3q} different polynomials of the form (2.2) and also, by Corollary 2.3.11, q^{3q} different polynomial functions on $\mathbb{F}_q[\alpha]$, every function is represented uniquely.

We can also show uniqueness directly, without using Corollary 2.3.11, by demonstrating that every expression of type (2.2) 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 $f(x) = \sum_{i=0}^{2q-1} a_i x^i + \sum_{j=0}^{q-1} b_j x^j\, \alpha$.

Then $\sum_{i=0}^{2q-1} a_i x^i \in N'_{\mathbb{F}_q}$ and $\sum_{j=0}^{q-1} b_j x^j \in N_{\mathbb{F}_q}$ by Theorem 2.3.5. Recalling from Example 2.3.3 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 $j = 0, \ldots, q-1$. □

2.4 Permutation polynomials on $R[\alpha]$

We now 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 2.2.4). 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 2.4.1. *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 2.2.7). 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 2.4.2. *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 2.4.1 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 2.4.3. *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 2.4.4. *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*

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

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 2.3.7 and Remark 2.3.9,

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

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 2.4.1, 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 2.4.5. *Let*

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

$St_\alpha(R)$, 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 2.4.6. *Let R be a finite commutative ring. Then*

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

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

Proof. It is clear that

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

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 2.2.7,

that is, F is represented by f_1. Therefore, $[f_1]_R = id_R$ (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 2.4.7. *To prevent confusion about the expression for the stabilizer group in Proposition 2.4.6 we emphasize that, in general, not every polynomial of the form $x + h$ with $h \in N_R$ induces a permutation polynomial of $R[\alpha]$, as the following example shows.*

Example 2.4.8. *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 2.3.11). The number of polynomial permutations now follows readily from Corollary 2.4.4, since every pair of functions on a finite field arises as the pair of functions induced by a polynomial and its derivative.

Lemma 2.4.9. *Let $\mathbb{F}_q$ be a finite field with q elements. Then for all functions $F, G\colon \mathbb{F}_q \longrightarrow \mathbb{F}_q$ 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 2.4.10. *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

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

Clearly, $|\mathcal{B}| = q!(q-1)^q$. By Lemma 2.4.9, each $(H, G) \in \mathcal{B}$ arises as $([f], [f'])$ for some $f \in \mathbb{F}_q[x]$. Thus by Corollary 2.4.4, $|\mathcal{P}(\mathbb{F}_q[\alpha])| = |\mathcal{B}| \cdot |\mathcal{F}(\mathbb{F}_q)| = q!(q-1)^q q^q$. □

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

1. $|St_\alpha(\mathbb{F}_q)| = |\{[f']_{\mathbb{F}_q} \colon f \in \mathbb{F}_q[x],\ [f]_{\mathbb{F}_q} = id_{\mathbb{F}_q}$ *and* $[f']_{\mathbb{F}_q}$ *is unit-valued*$\}|$;
2. $|St_\alpha(\mathbb{F}_q)| = |\{[f']_{\mathbb{F}_q} \colon f \in \mathbb{F}_q[x],\ [f]_{\mathbb{F}_q} = id_{\mathbb{F}_q},\ \deg f < 2q$ *and* $[f']_{\mathbb{F}_q}$ *is unit-valued*$\}|$;
3. $|St_\alpha(\mathbb{F}_q)| = (q-1)^q$.

Proof. To see (1), set $A = \{[f']_{\mathbb{F}_q} \colon f \in \mathbb{F}_q[x],\ [f]_{\mathbb{F}_q} = id_{\mathbb{F}_q}$ 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 $[f]_{\mathbb{F}_q} = id_{\mathbb{F}_q}$ by Definition 2.4.5. By Theorem 2.4.1, $[f']_{\mathbb{F}_q}$ is unit-valued. We set $\varphi(F) = [f']_{\mathbb{F}_q}$. Corollary 2.3.7 shows that φ is well-defined and injective, and Theorem 2.4.1 shows that it is surjective.

(2) follows from (1) and Lemma 2.4.9. Ad (3). By (1), $|St_\alpha(\mathbb{F}_q)| \leq |\{G \colon \mathbb{F}_q \longrightarrow \mathbb{F}_q^*\}| = (q-1)^q$. Now consider a function $G \colon \mathbb{F}_q \longrightarrow \mathbb{F}_q^*$. By Lemma 2.4.9, there exists a polynomial $h \in \mathbb{F}_q[x]$ such that $[h]_{\mathbb{F}_q} = id_{\mathbb{F}_q}$ 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 $|St_\alpha(\mathbb{F}_q)| \geq (q-1)^q$. □

The equalities of Theorem 2.4.11 actually come from a group isomorphism, as the second author has shown [4]. By Proposition 2.4.10 and Theorem 2.4.11, we immediately see the special case for finite fields of a more general result that we will show in the next section (see Theorem 2.5.7).

Corollary 2.4.12. *The number $|\mathcal{P}(\mathbb{F}_q[\alpha])|$ of polynomial permutations on $\mathbb{F}_q[\alpha]$ is given by*

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

2.5 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 2.5.1. *Let $\mathcal{P}_R(R[\alpha]) = \{F \in \mathcal{P}(R[\alpha]) \colon F = [f]$ for some $f \in R[x]\}$.*

Remark 2.5.2. *Proposition 2.4.6 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 [70, section III, statement 6, pp. 335] (also for several variables [70, Theorem 2.3]). It is implicitly shown in the proof of a different result in McDonalds's monograph on finite rings [57, pp. 269-272], and explicitly in a paper of Nechaev [63, Theorem 3].

Lemma 2.5.3. *[70, 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 2.5.4. *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 2.4.9, while, when R is a finite local ring but not a field, it follows from Lemma 2.5.3. □

Lemma 2.5.5. *$\mathcal{P}_R(R[\alpha])$ is a subgroup of $\mathcal{P}(R[\alpha])$; and the map*

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

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

Ad (1) This is evident from Theorem 2.4.1 and Lemma 2.5.4.

Ad (2) $St_\alpha(R)$ is contained in $\mathcal{P}_R(R[\alpha])$, by Proposition 2.4.6. $St_\alpha(R)$, 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 a unit-valued if it maps R into, R^*, the group of units on R.

Corollary 2.5.6. *For any fixed $F \in \mathcal{P}(R)$,*

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

Proof. Let $f \in R[x]$ such that $[f]_R = F$ and $[f']_R$ is unit-valued. Such a polynomial f exists by Lemma 2.5.4. By Corollary 2.4.2, 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 2.5.5 (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 $R[\alpha]$. ψ is well-defined and injective by Corollary 2.3.7 and onto by Corollary 2.4.2. □

Theorem 2.5.7. *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

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

By Corollary 2.5.6, $|B| = |\mathcal{P}(R)| \cdot |St_\alpha(R)|$.

We define a function $\psi \colon \mathcal{P}(R[\alpha]) \longrightarrow B \times \mathcal{F}(R)$ 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 2.4.1 and Corollary 2.3.7, ψ is well-defined and one-to-one. The surjectivity of ψ follows by Theorem 2.4.1. Therefore,

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

□

Remark 2.5.8. *Let R be a finite local ring which is not a field, M the maximal ideal of R, and $q = |R/M|$. Jiang [40] 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 2.5.9. *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 2.2.6 (4). Let q denote the order of this residue field. By Theorem 2.5.7, $|\mathcal{P}(R[\alpha])| = |\mathcal{F}(R)| \cdot |\mathcal{P}(R)| \cdot |St_\alpha(R)|$. Now apply Remark 2.5.8 to $\mathcal{P}(R[\alpha])$ and $\mathcal{P}(R)$ simultaneously and cancel. □

2.6 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 2.6.1. *[69, 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 2.6.1 to Theorem 2.4.1 and Corollary 2.4.3 in the special case where $R = \mathbb{Z}_{p^n}$.

Theorem 2.6.2. *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 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 2.4.3, (1) is equivalent to (3), and (2) is equivalent to (4). By Lemma 2.6.1, the statements (5), (6) and (7) are equivalent.

By Theorem 2.4.1, (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 2.6.1 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 2.4.1 shows that (2) implies (5). □

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

Corollary 2.6.3. *Let $f \in \mathbb{Z}[x]$. Then the following 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 2.6.4. *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 2.6.3 applies and $h(x)$ is a permutation polynomial on $\mathbb{Z}_{p^n}[\alpha]$. Now (2) follows from (1) and Definition 2.4.5.

□

The following example illustrates the necessity of the condition $n > 1$ in Theorem 2.6.2 (7) and Corollary 2.6.4.

Example 2.6.5. *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 2.6.2 and Corollary 2.6.4 to obtain statements about permutation polynomials on $\mathbb{Z}_m[\alpha]$.

Theorem 2.6.6. *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 2.6.7. *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 $St_\alpha(\mathbb{Z}_m)$.*

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

Recall from Definition 2.4.5 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 2.5.7 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 and permutations on $\mathbb{Z}_{p^n}[\alpha]$ for $n \leq p$ in section 2.8.

We have already defined the ideal of null-polynomials and the ideal of polynomials that are null together with their first derivative in section 2.3 (Definition 2.3.1). 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 2.7.1. *Let*

$$N_m(< k) = \{f \in \mathbb{Z}_m[x] \colon f \in N_{\mathbb{Z}_m} \text{ and } \deg f < k\},$$

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

Recall from Definition 2.2.2 that $[f]_m$, short for $[f]_{\mathbb{Z}_m}$, denotes the polynomial function induced by f on $\mathbb{Z}_m$.

Proposition 2.7.2. *Let $m = p_1^{n_1} \cdots p_l^{n_l}$, where $p_1, \ldots, p_l$ are distinct primes and suppose that $n_j > 1$ for $j = 1, \ldots, l$. Then*

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

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

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

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 2.4.6) a null polynomial on $\mathbb{Z}_m$ such that $x + h(x)$ induces F. We set $\varphi(F) = [h']_m$. Now Corollary 2.3.7 shows φ to be well-defined and injective, and Corollary 2.6.7 shows it to be surjective.

Ad (2a). If $g \in N_{\mathbb{Z}_m}$, then by Proposition 2.3.12, 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 $\varphi\colon N_{\mathbb{Z}_m} \longrightarrow \mathcal{F}(\mathbb{Z}_m)$ by $\varphi(f) = [f']_m$. Clearly, φ is a homomorphism of additive groups. Furthermore, $\ker\varphi = N'_{\mathbb{Z}_m}$ and $\operatorname{Im}\varphi = \{[f']_m\colon f \in N_{\mathbb{Z}_m}\}$. By (1),

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

For 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 $N_m(<k)$, whose image is still $\{[f']_m\colon f \in N_{\mathbb{Z}_m}\}$, by Corollary 2.3.7, and whose kernel is $N'_m(<k)$. Hence

$$|St_\alpha(\mathbb{Z}_m)| = [N_m(<k)\colon N'_m(<k)]. \qquad \square$$

We now substitute concrete numbers from Theorem 2.3.15 and Proposition 2.3.16 for the k that stands for the degree of a monic null polynomial on $\mathbb{Z}_m[\alpha]$ in Proposition 2.7.2 (2). Here, as in Definition 2.3.13, $\mu(m)$ denotes the smallest positive integer whose factorial is divisible by m.

Corollary 2.7.3. *Let $m = p_1^{n_1}\cdots p_k^{n_k}$, where $p_1,\ldots,p_k$ are distinct primes and suppose that $n_j > 1$ for $j = 1,\ldots,k$. Then*

1. $|St_\alpha(\mathbb{Z}_m)| = |\{[f']_m\colon f \in N_{\mathbb{Z}_m} \text{ with } \deg f < 2\mu(m)\}|$;
2. $|St_\alpha(\mathbb{Z}_m)| = \dfrac{|N_m(<2\mu(m))|}{|N'_m(<2\mu(m))|}$.

Corollary 2.7.4. *For a prime number p and a natural number n, where $1 < n \leq p$, we have*

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

Remark 2.7.5. *When $m = p$ is a prime, Proposition 2.7.2 and its Corollaries do not apply. This case has been treated in Theorem 2.4.11.*

We now employ Proposition 2.7.2 to show that Corollary 2.5.6 takes a simpler form for polynomial functions on $\mathbb{Z}_{p^n}$, when $n > 1$. (Again, the case $n = 1$ is exceptional, see Theorem 2.4.11.)

Corollary 2.7.6. *Let $n > 1$. Then for any fixed $F \in \mathcal{F}(\mathbb{Z}_{p^n})$,*

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

Proof. Set

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

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

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

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, $([f_1]_{p^n}, [f_1']_{p^n}) \neq ([f]_{p^n}, [f']_{p^n})$ implies $[f_1']_{p^n} \neq [f']_{p^n}$ and hence $[(f_1 - f_0)']_{p^n} \neq [(f - f_0)']_{p^n}$.

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 2.7.2 (1),

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

Remark 2.7.7. *Let $n = 1$ and $A = \{([f]_{p^n}, [f']_{p^n})\colon f \in \mathbb{Z}[x]$ with $[f]_{p^n} = F\}$. Then $|A| = p^p$ by Lemma 2.4.9, but $|St_\alpha(\mathbb{Z}_p)| = (p-1)^p$ by Theorem 2.4.11. This shows the condition on n in Corollary 2.7.6 is necessary.*

We now give a self-contained proof of Corollary 2.5.9 (not using Jiang's ratio [40], but emulating the argument in the proof of Theorem 2.5.7), for the case where $R = \mathbb{Z}_{p^n}[\alpha]$.

Corollary 2.7.8. *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

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

By Corollary 2.7.6,

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

We now define a function $\psi\colon \mathcal{F}(R[\alpha]) \longrightarrow B \times \mathcal{F}(R)$ 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 2.3.7, ψ is well-defined and bijective, and, hence, $|\mathcal{F}(\mathbb{Z}_{p^n}[\alpha])| = |B| \cdot |\mathcal{F}(\mathbb{Z}_{p^n})|$. $\square$

As $|\mathcal{F}(\mathbb{Z}_{p^n})|$ is a well-known quantity (quoted in the introduction in Equation (2.1)), all we now need for an explicit formula for $|\mathcal{F}(\mathbb{Z}_{p^n})|$ is an expression for $|St_\alpha(\mathbb{Z}_{p^n})|$. We will derive one for $n \leq p$ in the next section.

2.8 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 $n \leq p$. The reason for the assumption

$n \leq p$ 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 [33, Corollary 2.5] — the ideal $((x^p - x), p)^n$ is clearly contained in $N_{\mathbb{Z}_{p^n}}$, and, for $n \leq p$, their respective indices in $\mathbb{Z}_{p^n}[x]$ are the same — but it can also be derived from other results [91, 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 $k \leq n$) 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 2.8.2, is taken from an earlier paper [33].

Remark 2.8.1. *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 $k \geq 0$.

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

$$\forall i \;\; a_i \equiv b_i \mod I \quad \Longleftrightarrow \quad \forall j, k \;\; a_{jk} \equiv b_{jk} \mod I.$$

(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 2.8.2. *[33, Lemma 2.5] Let p be a prime and $f \in \mathbb{Z}[x]$ represented as in Remark 2.8.1 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 $k \geq 0$.

Let $n \leq p$. 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 $0 \leq k \leq n$. □

Corollary 2.8.3. *Let $n \leq p$. Then $|N_{p^n}(< (n+1)p)| = p^{\frac{n(n+1)p}{2}}$.*

Proof. We express $f \in \mathbb{Z}[x]$ with $\deg f < (n+1)p$ as in Remark 2.8.1, Lemma 2.8.2, $f(x) = \sum_{k=0}^{n} f_k(x)(x^p - x)^k$, where $f_k(x) = \sum_{j=0}^{p-1} a_{jk} x^j$.

By Lemma 2.8.2 and Remark 2.8.1 (2), $|N_{p^n}(< (n+1)p)|$ is equal to the number of ways to chose 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 $\prod_{k=0}^{n} p^{kp} = p^{p\sum_{k=0}^{n} k} = p^{\frac{n(n+1)p}{2}}$. □

Lemma 2.8.4. *Let $f \in \mathbb{Z}[x]$, where $f(x) = \sum_{k\geq 0} f_k(x)(x^p - x)^k$ such that $f_k(x) = \sum_{j=0}^{p-1} a_{jk}x^j$. If we expand f' in a similar way, $f'(x) = \sum_{k\geq 0} \hat{f}_k(x)(x^p - x)^k$, where $\hat{f}_k(x) = \sum_{j=0}^{p-1} \hat{a}_{jk}x^j$, then the following relations hold for all $k \geq 0$*

$$\begin{aligned}
\hat{a}_{0k} &= (kp+1)a_{1k} - (k+1)a_{0\,k+1} \\
\hat{a}_{jk} &= (kp+j+1)a_{j+1\,k} + (k+1)(p-1)a_{j\,k+1} \text{ for } 1 \leq j \leq p-2 \\
\hat{a}_{p-1\,k} &= (k+1)(p-1)a_{p-1\,k+1} + (k+1)pa_{0\,k+1}.
\end{aligned} \tag{2.3}$$

Proof. Consider

$$\Big(f_k(x)(x^p - x)^k\Big)' = f_k'(x)(x^p - x)^k - kf_k(x)(x^p - x)^{k-1} + kpx^{p-1}f_k(x)(x^p - x)^{k-1}. \tag{2.4}$$

We rewrite the last term of Equation (2.4) by expanding $x^{p-1}f_k(x)$ as $\sum_{j=0}^{p-1} a_{jk}x^{p+j-1}$ and substituting $x^{j+1} + x^j(x^p - x)$ for x^{p+j}, to get integer linear-combinations of terms $x^j(x^p - x)^k$.

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

and, therefore,

$$\begin{aligned}
\Big(f_k(x)(x^p - x)^k\Big)' = &\left(-ka_{0k} + \sum_{j=1}^{p-2} k(p-1)a_{jk}x^j + (k(p-1)a_{p-1\,k} + kpa_{0k})x^{p-1}\right)(x^p - x)^{k-1} \\
&+ \left(\sum_{j=0}^{p-2}(kp+j+1)a_{j+1\,k}x^j\right)(x^p - x)^k.
\end{aligned} \tag{2.5}$$

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

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

□

Let $f \in \mathbb{Z}[x]$, p a prime and $n \le p$. We are now in a position to tell from the coefficients of the expansion of f with respect to $(x^p - x)$ (as in Remark 2.8.1) whether both f and f' are null polynomials on $\mathbb{Z}_{p^n}$.

Theorem 2.8.5. *Let $n \le p$ and $f(x) = \sum_{k=0}^{m} f_k(x)(x^p - x)^k \in \mathbb{Z}[x]$, where $f_k(x) = \sum_{j=0}^{p-1} a_{jk}x^j$. Then f and f' are both null polynomials on $\mathbb{Z}_{p^n}$ if and only if, for $1 \le k < \min(p, n+1)$,*

$$\begin{aligned}
a_{j0} &\equiv 0 \pmod{p^n} \\
a_{jk} &\equiv 0 \pmod{p^{n-k+1}}.
\end{aligned} \tag{2.6}$$

Proof. ($\Rightarrow$) Suppose f and f' are null polynomials on $\mathbb{Z}_{p^n}$. Then $f'(x) = \sum_{k=0}^{m} \hat{f}_k(x)(x^p - x)^k$, with $\hat{f}_k(x) = \sum_{j=0}^{p-1} \hat{a}_{jk}x^j$, such that, by Lemma 2.8.4, the coefficients a_{jk} and $\hat{a}_{jk}$ satisfy Equation (2.3). Since f' is a null polynomial on $\mathbb{Z}_{p^n}$, Lemma 2.8.2 implies, for $j = 0, \ldots, p-1$,

$$\hat{a}_{jk} \equiv 0 \pmod{p^{n-k}} \text{ for } k \le n. \tag{2.7}$$

Again by Lemma 2.8.2, it is clear that

$$a_{j0} \equiv 0 \pmod{p^n} \text{ for } j = 0, 1, \ldots, p-1. \tag{2.8}$$

For $1 \le k < \min(p, n+1)$, we use induction. To see $a_{j1} \equiv 0 \pmod{p^n}$, we set $k = 0$ in Equation (2.3), and get

$$\begin{aligned}
\hat{a}_{00} &= a_{10} - a_{0\,1}, \\
\hat{a}_{j0} &= (j+1)a_{j+1\,0} + (p-1)a_{j\,1} \quad \text{for} \quad 1 \le j \le p-2, \\
\hat{a}_{p-1\,0} &= (p-1)a_{p-1\,1} + pa_{0\,1}.
\end{aligned} \tag{2.9}$$

From Equations (2.7), (2.8), and (2.9), we conclude that $a_{j1} \equiv 0 \pmod{p^n}$, $j = 0, 1, \ldots, p-1$.

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

$$a_{jk} \equiv 0 \pmod{p^{n+1-k}} \text{ for } j = 0, 1, \ldots, p-1. \tag{2.10}$$

We rewrite Equation (2.3) as

$$\begin{aligned}(k+1)a_{0\,k+1} &= (kp+1)a_{1k} - \hat{a}_{0k},\\ (k+1)(p-1)a_{j\,k+1} &= \hat{a}_{jk} - (kp+j+1)a_{j+1\,k} \quad \text{for} \quad 1 \le j \le p-2,\\ (k+1)(p-1)a_{p-1\,k+1} &= \hat{a}_{p-1\,k} - (k+1)pa_{0\,k+1} \text{ for } k = 0,1,\ldots,n-1.\end{aligned} \tag{2.11}$$

Since $k+1 < p$ and $n+1-k > n-k$, Equations (2.11), (2.7) and the induction hypothesis (Equation (2.10)) give

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

For $k \ge \min(p, n+1)$, 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 (2.6) is true. Then, for $k \le p$, $a_{jk} \equiv 0 \pmod{p^{(n-k)}}$ since $n+1-k > n-k$. We use Lemma 2.8.4 and Equation (2.6) to show that $\hat{a}_{jk} \equiv 0 \pmod{p^{(n-k)}}$ for $0 \le k \le p$. The result now follows by Lemma 2.8.2. □

Corollary 2.8.6. *Let $n \le p$ 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 2.3.4, $(x^p-x)^r$ 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 2.3.6, it suffices to consider $h \in \mathbb{Z}[x]$. We show that h is not monic. If $h = 0$ this is evident. If $h \ne 0$, we expand h as in Lemma 2.8.2:

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

with $h_k(x) = \sum_{j=0}^{p-1} a_{jk}x^j \in \mathbb{Z}[x]$. By Theorem 2.8.5, it follows that for $0 \le j \le p-1$

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

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

Recall from Definitions 2.3.1 and 2.7.1 that $f \in N'_{p^n}(< (n+1)p)$ means f and f' are null polynomials on $\mathbb{Z}_{p^n}$ and $\deg f < (n+1)p$.

Corollary 2.8.7. *Let $n \le p$. Then $|N'_{p^n}(< (n+1)p)| = \begin{cases} p^{\frac{n(n-1)p}{2}} & \text{if } n < p \\ p^{\frac{(n^2-n+2)p}{2}} & \text{if } n = p \end{cases}$.*

Proof. We represent every polynomial $f \in \mathbb{Z}_{p^n}[x]$ with $\deg f < (n+1)p$ uniquely, by Remark 2.8.1, as

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

By Theorem 2.8.5, counting the polynomials in $N'_{p^n}(< (n+1)p)$ 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

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

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

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

□

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

Theorem 2.8.8. *Let $1 \leq n \leq p$. 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 2.4.11 (3). Let $1 < n \leq p$. By Corollary 2.7.4,

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

Now Corollaries 2.8.3 and 2.8.7, respectively, say that

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

□

Example 2.8.9. *Let $R = \mathbb{Z}_4$. Then $|St_\alpha(\mathbb{Z}_4)| = 4$ by Theorem 2.8.8. Now, by Corollary 2.8.6, 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 2.6.4, $[x + f_i] \in St_\alpha(\mathbb{Z}_4)$, where $[x + f_i]$ denotes the function induced by $x + f_i$ on $\mathbb{Z}_4[\alpha]$ for $i = 1, \ldots, 4$. Note that $[1 + f_i']_4 \neq [1 + f_j']_4$, however, and hence by Corollary 2.3.7, $[x + f_i] \neq [x + f_j]$ whenever $i \neq j$. Therefore $St_\alpha(\mathbb{Z}_4) = \{[x + f_i], i = 1, \ldots, 4\}$. Actually, $St_\alpha(\mathbb{Z}_4)$ is the Klein 4-group.

Theorem 2.8.8 now allows us to state explicit formulas for the number of polynomial functions and polynomial permutations on $\mathbb{Z}_{p^n}[\alpha]$ for $n \leq p$. 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 2.2.6 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 2.8.10. *Let $1 \leq n \leq p$. 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 2.4.10. Now, let $1 < n \leq p$. Using that $\mu(p^k) = kp$ for $k \leq p$, we simplify the formulas for $|\mathcal{F}(\mathbb{Z}_{p^n})|$ and $|\mathcal{P}(\mathbb{Z}_{p^n})|$ quoted in the introduction (Equation (2.1)) accordingly. For $1 < n \leq p$,

$$|\mathcal{F}(\mathbb{Z}_{p^n})| = p^{\frac{n(n+1)p}{2}} \quad \text{and} \quad |\mathcal{P}(\mathbb{Z}_{p^n})| = p!(p-1)^p p^{-2p} p^{\frac{n(n+1)p}{2}}. \tag{2.12}$$

Substituting the formula from Theorem 2.8.8 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 2.5.7, we obtain the desired result. □

Theorem 2.8.11. *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 2.3.18. For $1 < n \leq p$, we substitute the expression from Theorem 2.8.8 for $|St_\alpha(\mathbb{Z}_{p^n})|$ and the formula for $|\mathcal{F}(\mathbb{Z}_{p^n})|$ from Equation (2.1) (simplified as in Equation (2.12) in the proof of Theorem 2.8.10) in Corollary 2.7.8. □

2.9 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 2.3.13), $\mu(m)$ stands for the smallest natural number n such that m divides $n!$.

Lemma 2.9.1. *[81, 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*

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

Proposition 2.9.2. *Let $F\colon \mathbb{Z}_m[\alpha] \longrightarrow \mathbb{Z}_m[\alpha]$ 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*

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

and the b_j in such a representation are unique.

Proof. By Corollary 2.3.17, F can be represented by a polynomial $g_1 + \alpha\, g_2$, where

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

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 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 2.3.7, F depends on the function induced by $\sum_{j=0}^{\mu(m)-1} b_j x^j$ on $\mathbb{Z}_m$ but not on the function induced by its derivative. So we can replace $\sum_{j=0}^{\mu(m)-1} b_j x^j$ 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 2.3.7 and Lemma 2.9.1, b_j can be chosen uniquely such that $0 \leq b_j < \frac{m}{\gcd(m,j!)}$. □

By combining Proposition 2.9.2 with Proposition 2.3.16, we get the following corollary.

Corollary 2.9.3. *Let p be a prime number and let n be a positive integer such that $n \leq p$. Let $F\colon \mathbb{Z}_{p^n}[\alpha] \longrightarrow \mathbb{Z}_{p^n}[\alpha]$ 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 $\leq a_i, b_j < p^n$. 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 2.9.4. *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*

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

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 2.9.3, 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 2.8.6, $(x^p - x)^{m+1}$ is null on $\mathbb{Z}_{p^n}[\alpha]$. Thus we can choose g with $\deg g < p(m+1)$ by Proposition 2.3.12. We expand g as in Lemma 2.8.2, $g(x) = \sum_{k=0}^{m} g_k(x)(x^p - x)^k$, 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 2.8.5,

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

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 2.3.7,

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

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 $j = 0, \ldots, p-1$. While, if $1 \leq k \leq m$, $f_k(x)$ can be selected in $p^{p(n-k+1)}$ ways, since $0 \leq a_{jk} < p^{n-k+1}$ for $j = 0, \ldots, p-1$. 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 $\sum_{i=0}^{np-1} b_i x^i\, \alpha$ can be chosen in $p^{\frac{pn(n+1)}{2}}$ ways, since $0 \leq b_i < \frac{p^n}{\gcd(p^n, i!)}$. 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 2.8.11, this last quantity equals $|\mathcal{F}(\mathbb{Z}_{p^n}[\alpha])|$ and, therefore, the representation is unique. □

3 On the group of unit-valued polynomial functions

The content of this chapter is the accepted paper [4] in Applicable Algebra in Engineering, Communication and Computing Journal.

Abstract

Let R be a finite commutative ring. The set $\mathcal{F}(R)$ of polynomial functions on R is a finite commutative ring with pointwise operations. Its group of units $\mathcal{F}(R)^\times$ is just the set of all unit-valued polynomial functions. We investigate polynomial permutations on $R[x]/(x^2) = R[\alpha]$, the ring of dual numbers over R, and show that the group $\mathcal{P}_R(R[\alpha])$, consisting of those polynomial permutations of $R[\alpha]$ represented by polynomials in $R[x]$, is embedded in a semidirect product of $\mathcal{F}(R)^\times$ by the group $\mathcal{P}(R)$ of polynomial permutations on R. In particular, when $R = \mathbb{F}_q$, we prove that $\mathcal{P}_{\mathbb{F}_q}(\mathbb{F}_q[\alpha]) \cong \mathcal{P}(\mathbb{F}_q) \ltimes_\theta \mathcal{F}(\mathbb{F}_q)^\times$. Furthermore, we count unit-valued polynomial functions on the ring of integers modulo p^n and obtain canonical representations for these functions.

Keywords. Finite commutative rings, polynomial functions, polynomial mappings, unit-valued polynomial functions, permutation polynomials, polynomial permutations, dual numbers, semidirect product

3.1 Introduction

Throughout this paper R is a finite commutative ring with unity $1 \neq 0$. We denote by $R^\times$ the group of units of R. A function $F\colon R \longrightarrow R$ is called a polynomial function on R if there exists a polynomial $f \in R[x]$ such that $F(r) = f(r)$ for each $r \in R$. In this case, we say that f induces (represents) F or F is induced (represented) by f. If F is a bijection, we say that F is a *polynomial permutation* on R and f is a *permutation polynomial* on R (or f permutes R). When F is the constant zero, f is called a null polynomial on R or shortly, null on R. The set of all null polynomials is an ideal of $R[x]$, which we denote by N_R.

It is evident that the set $\mathcal{F}(R)$ of all polynomial functions on R is a monoid with respect to composition of functions. Its group of invertible elements $\mathcal{P}(R)$ consists of polynomial permu-

tations on R, and is called the group of polynomial permutations on R. Also, $\mathcal{F}(R)$ is a ring with addition and multiplication defined pointwise.

We are interested in the group of units of the pointwise ring structure on $\mathcal{F}(R)$, which we denote by $\mathcal{F}(R)^\times$. We show a relation between the group $\mathcal{F}(R)^\times$ and the group of those polynomial permutations on $R[x]/(x^2)$ that are represented by polynomials with coefficients in R. Moreover, when $R = \mathbb{Z}_{p^n}$ the ring of integers modulo p^n we find the order of $\mathcal{F}(\mathbb{Z}_{p^n})^\times$ and give canonical representations for its elements.

3.2 Preliminaries

In this section, we introduce the concepts and notations used frequently in the paper.

Definition 3.2.1. *Let A be a ring and $f \in A[x]$. Then:*

1. *$[f]_A$ denotes the polynomial function induced by f on A;*
2. *if $[f]_A$ maps A into $A^\times$, then f is called a* unit-valued polynomial *on A, and $[f]_A$ is called a* unit-valued polynomial function *on A;*
3. *when $[f]_A$ is a bijection on A, we call $[f]_A$ a* polynomial permutation *and f a* permutation polynomial *on A.*

Throughout this paper for every $f \in R[x]$, let f' denote its formal derivative.

Unit-valued polynomials and unit-valued polynomial functions have been employed in the literature to examine other mathematical objects. Loper [55] uses unit-valued polynomials for distinguishing two classes of commutative rings: D-rings and non-D-rings, where D-rings are characterized by the fact that every unit-valued polynomial is a constant. For instance, all semi-local rings (and, in particular, all finite rings) are non-D rings. Unit-valued polynomials also figure in the characterization of permutation polynomials on finite local rings. We illustrate this by a well-known fact:

Fact 3.2.2. *[63, Theorem 3] Let R be a local ring with maximal ideal M, and let $f \in R[x]$. Then f is a permutation polynomial on R if and only if the following conditions hold:*

1. *$\bar{f}$ is a permutation polynomial on the residue field R/M, where $\bar{f}$ denotes the reduction of f modulo M;*
2. *$f'(a) \neq 0 \mod M$ for every $a \in M$.*

Indeed, the second condition of the previous fact requires f' to be a unit-valued polynomial on R or, equivalently, $[f']_R$ to be a unit-valued polynomial function.

Remark 3.2.3. *Recall that, in a finite commutative ring R with unity, every element is either a unit or a zerodivisor, according to whether multiplication by the element is a bijection of R or not (see for example [48]).*

From now on, let " $\cdot$ " denote the pointwise multiplication of functions.

Fact 3.2.4. *Let R be a finite commutative ring, and $\mathcal{F}(R)$ the set of polynomial functions on R. Then $\mathcal{F}(R)$ is a finite commutative ring with nonzero unity, where addition and multiplication are defined pointwise. In particular, $\mathcal{F}(R)$ is a subring of R^R. Moreover, $\mathcal{F}(R)^\times$ is an Abelian group and;*

$$\mathcal{F}(R)^\times = \{F \in \mathcal{F}(R) \colon F \text{ is a unit-valued polynomial function}\}.$$

Proof. It is clear that $\mathcal{F}(R)$ forms a finite commutative ring under pointwise operations with the constant function 1 as its unity $1_{\mathcal{F}(R)}$.

Moreover, since $\mathcal{F}(R)$ is a commutative ring, $\mathcal{F}(R)^\times$ is an Abelian group. Now, it is easy to see that every unit-valued polynomial function is regular, and hence invertible by Remark 3.2.3. Thus $\mathcal{F}(R)^\times$ contains every unit-valued polynomial function.

For the other inclusion, let $F \in \mathcal{F}(R)^\times$. Then there exists $F^{-1} \in \mathcal{F}(R)^\times$ such that $F \cdot F^{-1} = 1_{\mathcal{F}(R)}$, that is $F(r)F^{-1}(r) = 1$ for each $r \in R$. Hence $F(r) \in R^\times$ for each $r \in R$. Therefore F is a unit-valued polynomial function by Definition 3.2.1. □

Remark 3.2.5. *When R is an infinite commutative ring, it is still true that $\mathcal{F}(R)$ is a commutative ring (infinite) and every element of $\mathcal{F}(R)^\times$ is a unit-valued polynomial function, but $\mathcal{F}(R)^\times$ may be properly contained in the set of all unit-valued polynomial functions.*

The following example illustrates the previous remark.

Example 3.2.6. *Let $R = \{\frac{a}{b} \colon a, b \in \mathbb{Z} \text{ and } 2 \nmid b\}$, that is, R is the localization of $\mathbb{Z}$ at $2\mathbb{Z}$. Then the polynomial $f = 1+2x$ is a unit-valued polynomial on R, and $F = [f]_R$ is a unit-valued polynomial function. We claim that F has no inverse in $\mathcal{F}(R)$. Assume, on the contrary, that F is invertible. So there exists $F_1 \in \mathcal{F}(R)$ such that $F \cdot F_1 = 1_{\mathcal{F}(R)}$, i.e., $F(r)F_1(r) = 1$ for every $r \in R$. Now, since $F_1 \in \mathcal{F}(R)$, there exists $f_1 \in R[x]$ such that $F_1 = [f_1]_R$. Then the polynomial $h(x) = (1+2x)f_1(x) - 1$ is of positive degree. Further, h has infinitely many roots in R since $h(r) = F(r)F_1(r) - 1 = 0$ for every $r \in R$, which contradicts the fundamental theorem of algebra.*

Definition 3.2.7. *For a commutative R, the ring $R[x]/(x^2)$ is called the ring of dual numbers over R. This ring can be viewed as the ring $R[\alpha] = \{a + b\alpha \colon a, b \in R, \alpha^2 = 0\}$, where α denotes the element $x + (x^2)$.*

Remark 3.2.8. *In the previous definition, R is a subring of $R[\alpha]$. Therefore every polynomial $g \in R[x]$ induces two functions: one on $R[\alpha]$ and one on R, namely $[g]_{R[\alpha]}$ and its restriction (to R) $[g]_R$.*

The following fact about the polynomials of $R[\alpha]$ can be proved easily.

Fact 3.2.9. *Let R be a commutative ring, and $a, b \in R$.*

1. *Let $g \in R[x]$. Then $g(a + b\,\alpha) = g(a) + bg'(a)\,\alpha$.*

2. *Let $g \in R[\alpha][x]$, and $g_1, g_2 \in R[x]$ the unique polynomials in $R[x]$ such that $g = g_1 + g_2\,\alpha$. Then*
$$g(a + b\,\alpha) = g_1(a) + (bg_1'(a) + g_2(a))\,\alpha\,.$$

Fact 3.2.10. *Let $g \in R[x]$. Then g is a null polynomial on R if and only if $g\alpha$ is a null polynomial on $R[\alpha]$.*

Proof. ($\Leftarrow$) Immediate since R is a subring of $R[\alpha]$ and, for $r \in R$, $r\,\alpha = 0$ if and only if $r = 0$.
($\Rightarrow$) Let $a, b \in R$. Then, by Fact 3.2.9 (1),

$$g(a + b\alpha)\alpha = (g(a) + g'(a)b\alpha)\alpha = g(a)\alpha + 0 = 0\alpha = 0.$$

□

Recall from the introduction that $\mathcal{P}(R[\alpha])$ denotes the group of polynomial permutations on $R[\alpha]$. It is apparent that $\mathcal{P}(R[\alpha])$, as a subset of $\mathcal{F}(R[\alpha])$, is finite.

We now consider those polynomial permutations on $R[\alpha]$ that are induced by polynomials with coefficients in R (as opposed to $R[\alpha]$).

Definition 3.2.11. *Let $\mathcal{P}_R(R[\alpha]) = \{F \in \mathcal{P}(R[\alpha]) \colon F = [f]_{R[\alpha]}$ for some $f \in R[x]\}$.*

From now on, let " $\circ$ " denote the composition of functions (or polynomials) and id_R the identity function on R.

Remark 3.2.12. *Let $f, g \in R[x]$. Then their composition $g \circ f$ induces a function on R, which is the composition of the functions induced by f and g on R. Similarly, $f + g$ and fg induce two functions on R, namely the pointwise addition and multiplication, respectively, of the functions induced by f and g. In terms of our notation this is equivalent to the following:*

1. $[f \circ g]_R = [f]_R \circ [g]_R$;

2. $[f + g]_R = [f]_R + [g]_R$;

3. $[fg]_R = [f]_R \cdot [g]_R$.

We will use the above equalities frequently in our arguments in the next sections.

Fact 3.2.13. *The set $\mathcal{P}_R(R[\alpha])$ is a subgroup of $\mathcal{P}(R[\alpha])$.*

Proof. Evidently, $id_{R[\alpha]} = [x]_{R[\alpha]} \in \mathcal{P}_R(R[\alpha])$. Since $\mathcal{P}_R(R[\alpha])$ is finite, it suffices to show that $\mathcal{P}_R(R[\alpha])$ is closed under composition. So if $F_1, F_2 \in \mathcal{P}_R(R[\alpha])$, then F_1, F_2 are induced by $f_1, f_2 \in R[x]$, respectively. Further, $F_1, F_2 \in \mathcal{P}(R[\alpha])$, and hence $[f_1 \circ f_2]_{R[\alpha]} = F_1 \circ F_2 \in \mathcal{P}(R[\alpha])$. Therefore, by Definition 3.2.11, $F_1 \circ F_2 \in \mathcal{P}_R(R[\alpha])$. □

3.3 The embedding of the group $\mathcal{P}_R(R[\alpha])$ in the group $\mathcal{P}(R) \ltimes_\theta \mathcal{F}(R)^\times$

We will show that the group $(\mathcal{P}_R(R[\alpha]), \circ)$, which consists of permutations represented by polynomials from $R[x]$, is embedded in a semidirect product of the group $(\mathcal{F}(R)^\times, \cdot)$ of unit-valued polynomial functions on R with respect to pointwise multiplication by the group $(\mathcal{P}(R), \circ)$ of polynomial permutations on R with respect to composition via a homomorphism θ defined in Lemma 3.3.2 below.

From now on, for a polynomial function L, the notation L^{-1} sometimes means the inverse with respect to pointwise multiplication (namely, when $L \in \mathcal{F}(R)^\times$) and sometimes the inverse with respect to composition (namely, when $L \in \mathcal{P}(R)$). No confusion should follow from this convention since $\mathcal{F}(R)^\times \cap \mathcal{P}(R)$ is empty.

The following lemma is easy and straightforward.

Lemma 3.3.1. *Let $F, F_1 \in \mathcal{F}(R)^\times$, and $G \in \mathcal{F}(R)$. Then the following hold:*

1. *$F \circ G \in \mathcal{F}(R)^\times$;*
2. *$(F \cdot F_1) \circ G = (F \circ G) \cdot (F_1 \circ G)$;*
3. *if F^{-1} is the inverse of F, then $F^{-1} \circ G$ is the inverse of $F \circ G$.*

An expert reader will notice that Lemma 3.3.1 defines a group action of $\mathcal{P}(R)$ on $\mathcal{F}(R)^\times$ in which every element of $\mathcal{P}(R)$ induces a homomorphism on $\mathcal{F}(R)^\times$, and what is coming now is a consequence of that. However, we do not refer to this action explicitly to avoid recalling additional materials. In fact, our arguments are elementary and depend on direct calculations.

Lemma 3.3.2. *Let R be a finite commutative ring, and $G \in \mathcal{P}(R)$. Then*

1. *the map $\theta_G \colon \mathcal{F}(R)^\times \longrightarrow \mathcal{F}(R)^\times$ defined by $(F)\theta_G = F \circ G$, for all $F \in \mathcal{F}(R)^\times$, is an automorphism of $(\mathcal{F}(R)^\times, \cdot)$;*
2. *the map $\theta \colon \mathcal{P}(R) \longrightarrow Aut(\mathcal{F}(R)^\times)$ defined by $(G)\theta = \theta_G$ is a homomorphism with respect to composition.*

Proof. Ad(1) in view of Lemma 3.3.1 (2) we need only show that θ_G is a bijection. Let $F \in \mathcal{F}(R)^\times$. Then $F \circ G^{-1} \in \mathcal{F}(R)^\times$ by Lemma 3.3.1 (1), and we have that

$$(F \circ G^{-1})\theta_G = (F \circ G^{-1}) \circ G = F \circ (G^{-1} \circ G) = F \circ id_R = F.$$

This shows that θ is a surjection, and hence a bijection, since $\mathcal{F}(R)^\times$ is finite.

Ad(2) if $\theta \colon \mathcal{P}(R) \longrightarrow Aut(\mathcal{F}(R)^\times)$ is given by $(G)\theta = \theta_G$, then for every $G_1, G_2 \in \mathcal{P}(R)$ and any $F \in \mathcal{F}(R)^\times$, we have

$$(F)\theta_{G_1 \circ G_2} = F \circ (G_1 \circ G_2) = (F \circ G_1) \circ G_2 = (F \circ G_1)\theta_{G_2} = ((F)\theta_{G_1})\theta_{G_2} = (F)\theta_{G_1} \circ \theta_{G_2}.$$

Hence $\theta_{G_1 \circ G_2} = \theta_{G_1} \circ \theta_{G_2}$ and θ is a homomorphism. $\square$

Notation and Remark 3.3.3. *Recall that, for two groups H, K and a homomorphism φ from K into $Aut(H)$, the semidirect product of H by K with respect to φ is the group of all pairs (k, h) such that $k \in K$ and $h \in H$, with the following operation*

$$(k_1, h_1)(k_2, h_2) = (k_1 k_2, (h_1)\varphi_{k_2} h_2),$$

where φ_{k_2} is the image of k_2 in $Aut(H)$ via the homomorphism φ. This group is denoted by $K \ltimes_\varphi H$.

Proposition 3.3.4. *Let R be a finite commutative ring, $\mathcal{P}(R)$ the group of polynomial permutations and $\mathcal{F}(R)^\times$ the group of unit-valued polynomial functions. Let $\theta \colon \mathcal{P}(R) \longrightarrow Aut(\mathcal{F}(R)^\times)$ be the homomorphism of Lemma 3.3.2. Then the operation on the group $\mathcal{P}(R) \ltimes_\theta \mathcal{F}(R)^\times$ is defined by*

$$(G_1, F_1)(G_2, F_2) = \big(G_1 \circ G_2, (F_1)\theta_{G_2} \cdot F_2\big) = \big(G_1 \circ G_2, (F_1 \circ G_2) \cdot F_2\big),$$

where $G_1, G_2, \in \mathcal{P}(R)$ and $F_1, F_2 \in \mathcal{F}(R)^\times$. In particular,

$$(G, F)^{-1} = (G^{-1}, F^{-1} \circ G^{-1})$$

for every $G \in \mathcal{P}(R)$ and $F \in \mathcal{F}(R)^\times$. (Here G^{-1} is the inverse with respect to composition and F^{-1} is the inverse with respect to pointwise multiplication.)

The proof of Proposition 3.3.4 depends essentially on Lemma 3.3.2, and is just the justifications of the semidirect product properties (see for example [46]).

Remark 3.3.5. *Consider the following subsets of $\mathcal{P}(R) \ltimes_\theta \mathcal{F}(R)^\times$:*

$$\overline{\mathcal{P}(R)} = \{(G, 1_{\mathcal{F}(R)}) \colon G \in \mathcal{P}(R)\}, \text{ and } \overline{\mathcal{F}(R)^\times} = \{(id_R, F) \colon F \in \mathcal{F}(R)^\times\}.$$

It is a routine verification to show that $\overline{\mathcal{P}(R)}$ and $\overline{\mathcal{F}(R)^\times}$ are subgroups of $\mathcal{P}(R) \ltimes_\theta \mathcal{F}(R)^\times$ that are isomorphic to $\mathcal{P}(R)$ and $\mathcal{F}(R)^\times$, respectively, satisfying the following conditions:

1. $\mathcal{P}(R) \ltimes_\theta \mathcal{F}(R)^\times = \overline{\mathcal{P}(R)}\ \overline{\mathcal{F}(R)^\times}$;
2. $\overline{\mathcal{F}(R)^\times} \lhd \mathcal{P}(R) \ltimes_\theta \mathcal{F}(R)^\times$;
3. $\overline{\mathcal{P}(R)} \cap \overline{\mathcal{F}(R)^\times} = \{(id_R, 1_{\mathcal{F}(R)})\}$.

This justifies calling $\mathcal{P}(R) \ltimes_\theta \mathcal{F}(R)^\times$ the (internal) semidirect product of $\overline{\mathcal{F}(R)^\times}$ by $\overline{\mathcal{P}(R)}$.

Our next aim is to show that $\mathcal{P}(R) \ltimes_\theta \mathcal{F}(R)^\times$ contains an isomorphic copy of the group $\mathcal{P}_R(R[\alpha])$ defined in Definition 3.2.11. For completeness' sake, we prove the following lemma, which is a special case of [2, Theorem 4.1].

Lemma 3.3.6. *Let $g \in R[x]$. Then g permutes $R[\alpha]$ if and only if g permutes R and g' is a unit-valued polynomial.*

Proof. ($\Rightarrow$) Let $c \in R$. Then $c \in R[\alpha]$. Since g permutes $R[\alpha]$, there exist $a, b \in R$ such that $g(a + b\alpha) = c$. Thus $g(a) + bg'(a)\alpha = c$ by Fact 3.2.9 (1). So $g(a) = c$, and therefore g is onto on the ring R, and hence a permutation polynomial on R.

Suppose that g' is not a unit-valued polynomial. Then there exists $a \in R$ such that $g'(a)$ is a zerodivisor of R. Now, if $0 \neq b \in R$ such that $bg'(a) = 0$, then by Fact 3.2.9 (1),

$$g(a + b\alpha) = g(a) + bg'(a)\alpha = g(a).$$

So g does not permute $R[\alpha]$, which is a contradiction.
($\Leftarrow$) It is enough to show that g is injective. Now, if $a, b, c, d \in R$ such that $g(a+b\alpha) = g(c+d\alpha)$, then by Fact 3.2.9 (1),

$$g(a) + bg'(a)\alpha = g(c) + dg'(c)\alpha.$$

Then we have $g(a) = g(c)$ and $bg'(a) = dg'(c)$. Hence $a = c$ since g permutes R. Then, since $g'(a)$ is a unit of R, $b = d$ follows. □

Recall from Definition 3.2.1 that, for a ring A and a polynomial $f \in A[x]$, $[f]_A$ stands for the polynomial function induced by f on A.

Remark 3.3.7. *Let $F \in \mathcal{P}_R(R[\alpha])$. Then there exists $f \in R[x]$ such that $F = [f]_{R[\alpha]}$ by Definition 3.2.11. Further, by Lemma 3.3.6, $([f]_R, [f']_R) \in \mathcal{P}(R) \ltimes_\theta \mathcal{F}(R)^\times$. Now define a map*

$$\phi\colon \mathcal{P}_R(R[\alpha]) \longrightarrow \mathcal{P}(R) \ltimes_\theta \mathcal{F}(R)^\times \text{ by } \phi(F) = ([f]_R, [f']_R).$$

To show that ϕ is well-defined, we consider another polynomial $g \in R[x]$ such that $F = [g]_{R[\alpha]}$. Then for every $a, b \in R$ we have, by Fact 3.2.9 (1),

$$[g]_R(a) + b[g']_R(a)\,\alpha = g(a) + bg'(a)\alpha = F(a + b\alpha) = f(a) + bf'(a)\alpha = [f]_R(a) + b[f']_R(a)\,\alpha\,.$$

So substituting $b = 1$ yields

$$[g]_R(a) + [g']_R(a)\,\alpha = [f]_R(a) + [f']_R(a)\,\alpha \text{ for every } a \in R.$$

Therefore $([f]_R, [f']_R) = ([g]_R, [g']_R)$, and hence ϕ is well-defined. Also, this shows that the pair $([f]_R, [f']_R)$ determines $F = [f]_{R[\alpha]}$ completely, and, therefore, ϕ is injective.

Recall from Definition 3.2.11 and Fact 3.2.4 the definitions of the groups $(\mathcal{P}_R(R[\alpha]), \circ)$ and $(\mathcal{F}(R)^\times, \cdot)$, namely

$$\mathcal{P}_R(R[\alpha]) = \{F \in \mathcal{P}(R[\alpha])\colon F = [f]_{R[\alpha]} \text{ for some } f \in R[x]\}$$

and

$$\mathcal{F}(R)^\times = \{F \in \mathcal{F}(R) \colon F \text{ is a unit-valued polynomial function}\}.$$

Proposition 3.3.8. *Let R be a finite commutative ring, and θ the homomorphism defined in Lemma 3.3.2. Then the map*

$$\phi \colon \mathcal{P}_R(R[\alpha]) \longrightarrow \mathcal{P}(R) \ltimes_\theta \mathcal{F}(R)^\times \text{ defined by } \phi(F) = ([f]_R, [f']_R),$$

where $f \in R[x]$ such that $F = [f]_{R[\alpha]}$, is an embedding of $\mathcal{P}_R(R[\alpha])$ in $\mathcal{P}(R) \ltimes_\theta \mathcal{F}(R)^\times$.

Proof. By Remark 3.3.7, ϕ is well-defined and injective. So we need only show that ϕ is a homomorphism. Let $F_1 \in \mathcal{P}_R(R[\alpha])$ be induced by $f_1 \in R[x]$. Then $F \circ F_1$ is induced by $f \circ f_1$. Since $(f \circ f_1)' = (f' \circ f_1).f_1'$, ϕ maps $F \circ F_1$ to $([f \circ f_1]_R, [(f' \circ f_1) \cdot f_1']_R)$. Therefore, using Remark 3.2.12 and Proposition 3.3.4,

$$\begin{aligned}\phi[F \circ F_1] &= ([f \circ f_1]_R, [f' \circ f_1]_R \cdot [f_1']_R) = \big([f]_R \circ [f_1]_R, ([f']_R \circ [f_1]_R) \cdot [f_1']_R\big) \\ &= ([f]_R, [f']_R)([f_1]_R, [f_1']_R) = \phi(F)\phi(F_1).\end{aligned}$$

□

3.4 The pointwise stabilizer group of R and the group $\mathcal{P}(R) \ltimes_\theta \mathcal{F}(R)^\times$

In this section, we show that the group $\mathcal{P}(R) \ltimes_\theta \mathcal{F}(R)^\times$ contains a normal subgroup that is isomorphic to the pointwise stabilizer group of R (see Definition 3.4.1). Moreover, this stabilizer group can be viewed as a subgroup of the group of unit-valued polynomial functions $\mathcal{F}(R)^\times$. In particular, when $R = \mathbb{F}_q$ is the finite field of q elements, we prove that $\mathcal{F}(\mathbb{F}_q)^\times$ is isomorphic to this subgroup. We employ this result in the end of this section to prove that $\mathcal{P}_{\mathbb{F}_q}(\mathbb{F}_q[\alpha]) \cong \mathcal{P}(\mathbb{F}_q) \ltimes_\theta \mathcal{F}(\mathbb{F}_q)^\times$.

Now we recall the definition of the pointwise stabilizer group of R from [2].

Definition 3.4.1. *Let $St_\alpha(R) = \{F \in \mathcal{P}(R[\alpha]) \colon F(r) = r \text{ for every } r \in R\}$.*

It is evident that $St_\alpha(R)$ is closed under composition, and hence a subgroup of $\mathcal{P}(R[\alpha])$, since it is a non-empty finite set. We call this group the pointwise stabilizer of R.

Recall from the introduction that the ideal N_R consists of all null polynomials on R. Thus, for any $g, h \in R[x]$, $[g]_R = [h]_R$ if and only if $g - h \in N_R$.

We need the following proposition from [2]. We include a proof for the readers' convenience.

Proposition 3.4.2. *[2, Proposition 4.6] Let R be a finite commutative ring. Then*

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

In particular, $St_\alpha(R)$ is subgroup of $\mathcal{P}_R(R[\alpha])$.

Proof. Obviously,

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

Now if $F \in St_\alpha(R)$, then by Definition 3.4.1, $F \in \mathcal{P}(R[\alpha])$ such that $F(r) = r$ for each $r \in R$. Further, F is induced by a polynomial $h_0 + h_1\,\alpha$, where $h_0, h_1 \in R[x]$; and so by Fact 3.2.9 (2), $r = F(r) = h_0(r) + h_1(r)\,\alpha$ for every $r \in R$. But then $h_1(r) = 0$ for every $r \in R$, i.e., h_1 is null on R. Hence $h_1\alpha$ is null on $R[\alpha]$ by Fact 3.2.10. Thus $[h_0]_{R[\alpha]} = [h_0 + h_1\alpha]_{R[\alpha]} = F$, that is, F is induced by h_0. Also, $h_0 \equiv x \mod N_R$, that is, $[h_0]_R = id_R$, and therefore $h_0(x) = x + f(x)$ for some $f \in N_R$. This shows the other inclusion.

The last statement follows from $x + N_R \subseteq R[x]$ and the fact that $St_\alpha(R)$ and $\mathcal{P}_R(R[\alpha])$ are subgroups of $\mathcal{P}(R[\alpha])$.

□

Remark 3.4.3. *Let $\mathbb{F}_q = \{a_0, \ldots, a_{q-1}\}$ be the finite field of q elements. If $F\colon \mathbb{F}_q \longrightarrow \mathbb{F}_q$, then the polynomial $f(x) = \sum_{i=0}^{q-1} F(a_i) \prod_{\substack{j=0 \\ j\neq i}}^{q-1} \frac{x-a_j}{a_i-a_j} \in \mathbb{F}_q[x]$ represents F. Such a polynomial is called Lagrange polynomial and this method of construction is called Lagrange interpolation. Therefore every function on a finite field is a polynomial function, and hence $|\mathcal{F}(\mathbb{F}_q)| = q^q$. In particular, every permutation (bijection) on $\mathbb{F}_q$ is a polynomial permutation, and so $|\mathcal{P}(\mathbb{F}_q)| = q!$. Further, every unit-valued function is a unit-valued polynomial function, and thus $|\mathcal{F}(\mathbb{F}_q)^\times| = (q-1)^q$ since $\mathbb{F}_q^\times = \mathbb{F}_q \backslash \{0\}$. Moreover, it is obvious that Lagrange interpolation assigns to every function on $\mathbb{F}_q$ a unique polynomial of degree at most $q-1$. Hence every polynomial of degree at most $q-1$ is Lagrange polynomial of a function on $\mathbb{F}_q$ since the number of these polynomials is q^q, which is the number of functions on $\mathbb{F}_q$.*

Next, we show that $St_\alpha(R)$ is embedded in $\mathcal{F}(R)^\times$. For this we need the following well-known fact.

Lemma 3.4.4. *For each pair of functions (G, F) with*

$$G\colon \mathbb{F}_q \longrightarrow \mathbb{F}_q \text{ bijective and } F\colon \mathbb{F}_q \longrightarrow \mathbb{F}_q \setminus \{0\}$$

there exists a polynomial $g \in \mathbb{F}_q[x]$ such that $([g]_{\mathbb{F}_q}, [g']_{\mathbb{F}_q}) = (G, F)$.

Proof. Let $f_0, f_1 \in \mathbb{F}_q[x]$ such that $[f_0]_{\mathbb{F}_q} = G$ and $[f_1]_{\mathbb{F}_q} = F$, which we know to exist by Remark 3.4.3. Then set

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

Thus

$$g'(x) = (f_0''(x) - f_1'(x))(x^q - x) + f_1(x),$$

whence $[g]_{\mathbb{F}_q} = [f_0]_{\mathbb{F}_q} = G$ and $[g']_{\mathbb{F}_q} = [f_1]_{\mathbb{F}_q} = F$ since $(x^q - x)$ is a null polynomial on $\mathbb{F}_q$. □

Theorem 3.4.5. *Let R be a finite commutative ring. Then the map*

$$\psi\colon St_\alpha(R) \longrightarrow \mathcal{F}(R)^\times \text{ defined by } \psi(F) = [f']_R,$$

where $f \in R[x]$ such that $F = [f]_{R[\alpha]}$, is an embedding of the pointwise stabilizer of R, $St_\alpha(R)$, in the group of unit-valued polynomial functions $\mathcal{F}(R)^\times$.

If $R = \mathbb{F}_q$, then $St_\alpha(\mathbb{F}_q) \cong \mathcal{F}(\mathbb{F}_q)^\times$.

Proof. Let $F \in St_\alpha(R)$. Then there exists $f \in R[x]$ such that $F = [f]_{R[\alpha]}$ by Proposition 3.4.2. Further, $[f]_R = id_R = [x]_R$ by Definition 3.4.1. To show that ψ is well-defined, let $f_1 \in R[x]$ such that $F = [f_1]_{R[\alpha]}$. Then $[f']_R = [f_1']_R$ by Remark 3.3.7. By Lemma 3.3.6, $[f']_R \in \mathcal{F}(R)^\times$. Thus ψ is well-defined. Now, let $F_1 \in St_\alpha(R)$. Then there exists $g \in R[x]$ such that $F_1 = [g]_{R[\alpha]}$ by Proposition 3.4.2. Hence

$$\begin{aligned}\psi(F \circ F_1) &= [(f \circ g)']_R = [(f' \circ g) \cdot g']_R = [f' \circ g]_R \cdot [g']_R \\ &= ([f']_R \circ [g]_R) \cdot [g']_R.\end{aligned}$$

By Definition 3.4.1, $[g]_R = id_R$, and therefore $[f']_R \circ [g]_R = [f']_R$. This implies that

$$\psi(F \circ F_1) = [f']_R \cdot [g']_R = \psi(F) \cdot \psi(F_1),$$

whence ψ is a homomorphism. Now, if $F_1 \neq F$, then $[g']_R \neq [f']_R$ by Remark 3.3.7 and hence $\psi(F_1) \neq \psi(F)$. ψ is, therefore, injective and $St_\alpha(R)$ is embedded in $\mathcal{F}(R)^\times$.

For the case $R = \mathbb{F}_q$, we need only prove that ψ is surjective. Let $F \in \mathcal{F}(\mathbb{F}_q)^\times$. Then, by Lemma 3.4.4, there exists $f \in \mathbb{F}_q[x]$ such that $[f]_{\mathbb{F}_q} = id_{\mathbb{F}_q}$ and $[f']_{\mathbb{F}_q} = F$. Hence Lemma 3.3.6 yields $[f]_{\mathbb{F}_q[\alpha]} \in \mathcal{P}_{\mathbb{F}_q}(\mathbb{F}_q[\alpha])$. Thus $[f]_{\mathbb{F}_q[\alpha]} \in St_\alpha(\mathbb{F}_q)$ by Definition 3.4.1, and hence $\psi([f]_{\mathbb{F}_q[\alpha]}) = [f']_{\mathbb{F}_q} = F$. Therefore ψ is surjective. □

Notation 3.4.6. *Let $S_\alpha(R)$ denote the subgroup $\psi(St_\alpha(R))$ of $\mathcal{F}(R)^\times$, where ψ is the embedding of Theorem 3.4.5. Note that the group operation of $St_\alpha(R)$ is composition of functions, while the group operation on $S_\alpha(R)$ is pointwise multiplication of functions.*

Remark 3.4.7. *From Remark 3.3.5, we know that*

$$\mathcal{F}(R)^\times \cong \overline{\mathcal{F}(R)^\times} = \{(id_R, F)\colon F \in \mathcal{F}(R)^\times\} \lhd \mathcal{P}(R) \ltimes_\theta \mathcal{F}(R)^\times,$$

and, so, by the embedding ψ of Theorem 3.4.5, we have, with respect to Notation 3.4.6, the isomorphisms

$$St_\alpha(R) \cong S_\alpha(R) \cong \{(id_R, F)\colon F \in S_\alpha(R)\}.$$

This shows that $St_\alpha(R)$ is embedded in $\mathcal{P}(R) \ltimes_\theta \mathcal{F}(R)^\times$.

On the other hand, if we restrict the homomorphism ϕ of Proposition 3.3.8 to $St_\alpha(R)$, we have, by the definitions of ϕ and $S_\alpha(R)$,

$$\begin{aligned}\phi(St_\alpha(R)) &= \{\phi([f]_{R[\alpha]})\colon [f]_{R[\alpha]} \in St_\alpha(R) \text{ for some } f \in R[x]\}\\ &= \{(id_R, [f']_R)\colon [f]_{R[\alpha]} \in St_\alpha(R) \text{ for some } f \in R[x]\}\\ &= \{(id_R, F)\colon F \in S_\alpha(R)\}.\end{aligned}$$

This shows that the embedding of $St_\alpha(R)$ in $\mathcal{P}(R) \ltimes_\theta \mathcal{F}(R)^\times$ via Proposition 3.3.8 is identical to the embedding using Theorem 3.4.5 and Remark 3.3.5. In other words the following diagram commutes:

$$\begin{array}{ccc} \mathcal{P}_R(R[\alpha]) & \xrightarrow{\phi(F)=([f]_R,[f']_R)} & \mathcal{P}(R) \ltimes_\theta \mathcal{F}(R)^\times \\ \Big\uparrow \text{inclusion (Proposition 3.4.2)} & & \Big\uparrow \text{embedding (Remark 3.3.5)} \\ St_\alpha(R) & \xrightarrow{\psi(F)=[f']_R} & \mathcal{F}(R)^\times \end{array}$$

where in each case $f \in R[x]$ such that $F = [f]_{R[\alpha]}$.

Notation 3.4.8. *We write $\overline{S_\alpha(R)}$ for the image of $St_\alpha(R)$ in $\mathcal{P}(R) \ltimes_\theta \mathcal{F}(R)^\times$ under the homomorphism of the commuting diagram of Remark 3.4.7. That is,*

$$\overline{S_\alpha(R)} = \{(id_R, F)\colon F \in S_\alpha(R)\}.$$

Lemma 3.4.9. *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-valued polynomial functions on R.*

Proof. Without loss of generality, we may assume that R is local. When R is a finite field, the statement follows from Lemma 3.4.4. On the other hand, when R is a finite local ring that is not a field, the result follows from Fact 3.2.2. □

Remark 3.4.10.

1. *Define a map*

$$\Lambda\colon \mathcal{P}_R(R[\alpha]) \longrightarrow \mathcal{P}(R) \quad \text{by} \quad \Lambda(F) = [f]_R, \quad \text{where } f \in R[x] \text{ such that } F = [f]_{R[\alpha]}.$$

   Then, by Remark 3.3.7 and Lemma 3.4.9, Λ is a well-defined group epimorphism with $\ker\Lambda = St_\alpha(R)$, and therefore $St_\alpha(R) \lhd \mathcal{P}_R(R[\alpha])$ (see also [2]).

2. *Let $\phi(\mathcal{P}_R(R[\alpha]))$ be the isomorphic copy of $\mathcal{P}_R(R[\alpha])$ contained in $\mathcal{P}(R) \ltimes_\theta \mathcal{F}(R)^\times$ via*

the homomorphism ϕ of Proposition 3.3.8. Then, by (1) and Remark 3.4.7, $\overline{S_\alpha(R)} \lhd \phi(\mathcal{P}_R(R[\alpha]))$.

Lemma 3.4.11. *Let $S_\alpha(R)$ be as in Notation 3.4.6, and let $F \in S_\alpha(R)$. Then $F \circ G \in S_\alpha(R)$ for every $G \in \mathcal{P}(R)$.*

Proof. Let $G \in \mathcal{P}(R)$. Using Lemma 3.4.9, choose a polynomial $f \in R[x]$ such that $[f]_R = G$ and $[f']_R = F_1 \in \mathcal{F}(R)^\times$. Then $[f]_{R[\alpha]} \in \mathcal{P}_R(R[\alpha])$ by Lemma 3.3.6. Thus, by Proposition 3.3.8, $([f]_R, [f']_R) = (G, F_1) \in \phi(\mathcal{P}_R(R[\alpha]))$, where ϕ is the homomorphism of Proposition 3.3.8 (see also, Remark 3.4.10 (2)). We now use the fact that $\overline{S_\alpha(R)} = \{(id_R, F) \colon F \in S_\alpha(R)\}$ is a normal subgroup of $\phi(\mathcal{P}_R(R[\alpha]))$, by Proposition 3.3.4 and the fact that $\mathcal{F}(R)^\times$ is Abelian, we have

$$\begin{aligned}(G, F_1)^{-1}(id_R, F)(G, F_1) &= (G^{-1}, F_1^{-1} \circ G^{-1})\big(G, (F \circ G) \cdot F_1\big) \\ &= (id_R, F_1^{-1} \cdot (F \circ G) \cdot F_1) = (id_R, F \circ G).\end{aligned}$$

Thus $(id_R, F \circ G) \in \overline{S_\alpha(R)}$, and hence $F \circ G \in S_\alpha(R)$. □

Theorem 3.4.12. *Let R be a finite commutative ring, $\mathcal{P}(R) \ltimes_\theta \mathcal{F}(R)^\times$ the semidirect product constructed in Proposition 3.3.4 and $St_\alpha(R)$ the stabilizer group defined in Definition 3.4.1. Then the map*

$$\tilde{\phi} \colon St_\alpha(R) \longrightarrow \mathcal{P}(R) \ltimes_\theta \mathcal{F}(R)^\times \text{ defined by } \tilde{\phi}(F) = (id_R, [f']_R),$$

where $f \in R[x]$ such that $F = [f]_{R[\alpha]}$, is a normal embedding of $St_\alpha(R)$ in $\mathcal{P}(R) \ltimes_\theta \mathcal{F}(R)^\times$.

Proof. It is evident that $\tilde{\phi}$ is the restriction of the embedding ϕ of Proposition 3.3.8 to $St_\alpha(R)$, and hence $\tilde{\phi}$ is an embedding of $St_\alpha(R)$ in $\mathcal{P}(R) \ltimes_\theta \mathcal{F}(R)^\times$. Then, by Remark 3.4.7 and Notation 3.4.8,

$$\tilde{\phi}(St_\alpha(R)) = \phi(St_\alpha(R)) = \overline{S_\alpha(R)}.$$

So we need only show that $\overline{S_\alpha(R)} \lhd \mathcal{P}(R) \ltimes_\theta \mathcal{F}(R)^\times$. Let $(id_R, F) \in \overline{S_\alpha(R)}$ and $(G, F_1) \in \mathcal{P}(R) \ltimes_\theta \mathcal{F}(R)^\times$. Then by Proposition 3.3.4, we have, just as in the proof of Lemma 3.4.11, that

$$(G, F_1)^{-1}(id_R, F)(G, F_1) = (id_R, F \circ G).$$

Thus $(G, F_1)^{-1}(id_R, F)(G, F_1) \in \overline{S_\alpha(R)}$ by Lemma 3.4.11.

□

Recall from Notation 3.4.6 that $S_\alpha(R)$ denotes a subgroup of $\mathcal{F}(R)^\times$, which is isomorphic to $St_\alpha(R)$.

Remark 3.4.13. *Let $G \in \mathcal{P}(R)$, and let θ_G be the automorphism of $\mathcal{F}(R)^\times$ defined by $(F)\theta_G = F \circ G$ as in Lemma 3.3.2. We prove that the restriction of θ_G to $S_\alpha(R)$ is an automorphism of $S_\alpha(R)$ by showing that $S_\alpha(R)$ is invariant under θ_G.*

Now, by Lemma 3.4.11, $F \circ G \in S_\alpha(R)$ for every $F \in S_\alpha(R)$. Thus the restriction of θ_G to $S_\alpha(R)$ is an automorphism, that is, the map $\tilde{\theta}_G \colon S_\alpha(R) \longrightarrow S_\alpha(R)$ defined by $(F)\tilde{\theta}_G = F \circ G$, for all $F \in S_\alpha(R)$, is an automorphism of $S_\alpha(R)$.

Then, similar to the homomorphism $\theta \colon \mathcal{P}(R) \longrightarrow Aut(\mathcal{F}(R)^\times)$ of Lemma 3.3.2, we have the map $\tilde{\theta} \colon \mathcal{P}(R) \longrightarrow Aut(S_\alpha(R))$ defined by $(G)\tilde{\theta} = \tilde{\theta}_G$ is a homomorphism. This allows us to define the semidirect product $\mathcal{P}(R) \ltimes_{\tilde{\theta}} S_\alpha(R)$. Further, a routine verification shows that the operation on $\mathcal{P}(R) \ltimes_{\tilde{\theta}} S_\alpha(R)$ is just the operation on $\mathcal{P}(R) \ltimes_\theta \mathcal{F}(R)^\times$ restricted to $\mathcal{P}(R) \ltimes_{\tilde{\theta}} S_\alpha(R)$. Therefore $\mathcal{P}(R) \ltimes_{\tilde{\theta}} S_\alpha(R)$ is a subgroup of $\mathcal{P}(R) \ltimes_\theta \mathcal{F}(R)^\times$.

From now on, for any set A let $|A|$ denote the number of elements in A.

Proposition 3.4.14. *Let R be a finite commutative ring. Let θ and $\tilde{\theta}$ be the homomorphisms of Remark 3.4.13. Then $St_\alpha(R) \cong \mathcal{F}(R)^\times$ if and only if $\mathcal{P}(R) \ltimes_{\tilde{\theta}} S_\alpha(R) \cong \mathcal{P}(R) \ltimes_\theta \mathcal{F}(R)^\times$.*

Proof. ($\Rightarrow$) Obvious.

($\Leftarrow$) Assume that $\mathcal{P}(R) \ltimes_{\tilde{\theta}} S_\alpha(R) \cong \mathcal{P}(R) \ltimes_\theta \mathcal{F}(R)^\times$. Then $|S_\alpha(R)| = |\mathcal{F}(R)^\times|$, and thus $S_\alpha(R) = \mathcal{F}(R)^\times$ since $S_\alpha(R)$ is a subgroup of $\mathcal{F}(R)^\times$ by Theorem 3.4.5. Again, by Theorem 3.4.5, $St_\alpha(R) \cong S_\alpha(R) = \mathcal{F}(R)^\times$. □

In Proposition 3.3.8 we have proved for any finite ring R that the group $\mathcal{P}_R(R[\alpha])$ is embedded in $\mathcal{P}(R) \ltimes_\theta \mathcal{F}(R)^\times$. In the following theorem we show that, for a finite field $\mathbb{F}_q$,

$$\mathcal{P}_{\mathbb{F}_q}(\mathbb{F}_q[\alpha]) \cong \mathcal{P}(\mathbb{F}_q) \ltimes_\theta \mathcal{F}(\mathbb{F}_q)^\times.$$

Theorem 3.4.15. *Let $\mathbb{F}_q$ be the finite field of q elements. Let θ and $\tilde{\theta}$ be the homomorphisms of Remark 3.4.13, respectively. Then*

$$\mathcal{P}_{\mathbb{F}_q}(\mathbb{F}_q[\alpha]) \cong \mathcal{P}(\mathbb{F}_q) \ltimes_\theta \mathcal{F}(\mathbb{F}_q)^\times \cong \mathcal{P}(\mathbb{F}_q) \ltimes_{\tilde{\theta}} S_\alpha(\mathbb{F}_q).$$

Proof. In view of Proposition 3.3.8, Proposition 3.4.14 and Theorem 3.4.5 we need only show that

$$|\mathcal{P}_{\mathbb{F}_q}(\mathbb{F}_q[\alpha])| \geq |\mathcal{F}(\mathbb{F}_q)^\times||\mathcal{P}(\mathbb{F}_q)|.$$

Hence, by Remark 3.4.3, it is sufficient to show that $|\mathcal{P}_{\mathbb{F}_q}(\mathbb{F}_q[\alpha])| \geq q!(q-1)^q$.

Now consider the pair of functions (G, F) with

$$G \colon \mathbb{F}_q \longrightarrow \mathbb{F}_q \text{ bijective and } F \colon \mathbb{F}_q \longrightarrow \mathbb{F}_q \setminus \{0\}.$$

It is obvious that the total number of different pairs of this form is $q!(q-1)^q$. Moreover, by Lemma 3.4.4, there exists $g \in \mathbb{F}_q[x]$ such that $(G, F) = ([g]_{\mathbb{F}_q}, [g']_{\mathbb{F}_q})$, and so $[g]_{\mathbb{F}_q[\alpha]} \in \mathcal{P}_{\mathbb{F}_q}(\mathbb{F}_q[\alpha])$ by Lemma 3.3.6. Then, by Remark 3.3.7, every two different pairs of functions satisfying the conditions of Lemma 3.4.4 determine two different elements of $\mathcal{P}_{\mathbb{F}_q}(\mathbb{F}_q[\alpha])$. Therefore $|\mathcal{P}_{\mathbb{F}_q}(\mathbb{F}_q[\alpha])| \geq q!(q-1)^q$. □

Remark 3.4.16. *When $q = p$ (where p is a prime number), Frisch and Krenn [33] showed that $\mathcal{P}(\mathbb{F}_p) \ltimes_\theta \mathcal{F}(\mathbb{F}_p)^\times$ is a homomorphic image of $\mathcal{P}(\mathbb{Z}_{p^2})$ with non-trivial kernel, and determined the number of Sylow p-subgroups of $\mathcal{P}(\mathbb{Z}_{p^n})$ by means of those of $\mathcal{P}(\mathbb{F}_p) \ltimes_\theta \mathcal{F}(\mathbb{F}_p)^\times$ for every $n \geq 2$.*

3.5 The number of unit-valued polynomial functions on the ring $\mathbb{Z}_{p^n}$

Throughout this section let p be a prime number and n be a positive integer. Several authors considered the number of polynomial functions and polynomial permutations on the ring of integers modulo p^n. However, they neglected to count unit-valued polynomial functions modulo p^n (see for example, [41, 81]). In this section we apply the results of [41] to derive an explicit formula for the order of the group $\mathcal{F}(\mathbb{Z}_{p^n})^\times$, i.e., the number of unit-valued polynomial functions modulo p^n. In addition to that, we find canonical representations of these functions.

Since $\mathbb{Z}_{p^n}$ is a homomorphic image of $\mathbb{Z}$, we can represent the polynomial functions on $\mathbb{Z}_{p^n}$ by polynomials from $\mathbb{Z}[x]$. To simplify our notation we use the symbol $[f]_{p^n}$ instead of $[f]_{\mathbb{Z}_{p^n}}$ to indicate the function induced by $f \in \mathbb{Z}[x]$ on $\mathbb{Z}_{p^n}$.

Remark 3.5.1.

1. *Evidently, an integer represents a unit modulo p if and only if it represents a unit modulo p^n for all $n \geq 1$. More generally, for a polynomial $f \in R[x]$, $[f]_p$ is a unit-valued polynomial function on $\mathbb{Z}_p$ if and only if $[f]_{p^n}$ is a unit-valued polynomial function on $\mathbb{Z}_{p^n}$ for every $n \geq 1$.*

2. *Let $n > 1$. Define a map*

$$\phi_n \colon \mathcal{F}(\mathbb{Z}_{p^n}) \longrightarrow \mathcal{F}(\mathbb{Z}_{p^{n-1}}) \text{ by } \phi_n(F) = [f]_{p^{n-1}}, \text{ where } f \in \mathbb{Z}[x] \text{ such that } F = [f]_{p^n}.$$

Evidently, ϕ_n is a well-defined epimorphism of additive groups with

$$|\mathcal{F}(\mathbb{Z}_{p^n})| = |\mathcal{F}(\mathbb{Z}_{p^{n-1}})||\ker \phi_n|.$$

Notation 3.5.2. *In the remainder of the paper let $\beta(n)$ denote the smallest positive integer k such that $p^n \mid k!$, while $v_p(n)$ denotes the largest integer s such that $p^s \mid n$.*

Let $(x)_0 = 1$, and let $(x)_j = x(x-1)(x-2)\cdots(x-j+1)$ for any positive integer j.

The following lemma from [41] gives the cardinality of $\ker \phi_n$ of the epimorphism ϕ_n mentioned in Remark 3.5.1.

Lemma 3.5.3. *[41, Theorem 2] Let $n > 1$ and let ϕ_n be the epimorphism of Remark 3.5.1. Then $|\ker \phi_n| = p^{\beta(n)}$.*

Lemma 3.5.4. *Let $n > 1$. Then $|\mathcal{F}(\mathbb{Z}_{p^n})^\times| = p^{\beta(n)}|\mathcal{F}(\mathbb{Z}_{p^{n-1}})^\times|$.*

Proof. Let ϕ_n be the epimorphism defined in Remark 3.5.1 (2). Then $\phi_n^{-1}(\mathcal{F}(\mathbb{Z}_{p^{n-1}})^\times) = \mathcal{F}(\mathbb{Z}_{p^n})^\times$ by Remark 3.5.1 (1). Hence $|\mathcal{F}(\mathbb{Z}_{p^n})^\times| = |\phi_n^{-1}(\mathcal{F}(\mathbb{Z}_{p^{n-1}})^\times)|$. Now if $F \in \mathcal{F}(\mathbb{Z}_{p^{n-1}})^\times$, then by Remark 3.5.1, $|\phi_n^{-1}(F)| = |\ker \phi_n|$. Therefore

$$|\mathcal{F}(\mathbb{Z}_{p^n})^\times| = |\phi_n^{-1}(\mathcal{F}(\mathbb{Z}_{p^{n-1}})^\times)| = |\ker \phi_n||\mathcal{F}(\mathbb{Z}_{p^{n-1}})^\times|.$$

The result now follows from Lemma 3.5.3. □

Keep the notations of Notation 3.5.2. We now state our counting formula for the order of $\mathcal{F}(\mathbb{Z}_{p^{n-1}})^\times$.

Theorem 3.5.5. *Let $n > 1$ and let $\mathcal{F}(\mathbb{Z}_{p^n})^\times$ be the group of unit-valued polynomial functions modulo p^n. Then*

$$|\mathcal{F}(\mathbb{Z}_{p^n})^\times| = (p-1)^p p^{\sum_{k=2}^n \beta(k)}.$$

Proof. By applying Lemma 3.5.4 exactly $n-1$ times, we see that $|\mathcal{F}(\mathbb{Z}_{p^n})^\times| = |\mathcal{F}(\mathbb{Z}_p)^\times| p^{\sum_{k=2}^n \beta(k)}$.
But $|\mathcal{F}(\mathbb{Z}_p)^\times| = (p-1)^p$ by Remark 3.4.3. □

We need the following fact from [41].

Lemma 3.5.6. *[41, Theorem 1 and Corollary 2.2] If $F \in \mathcal{F}(\mathbb{Z}_{p^n})$, there exists one and only one polynomial $f \in \mathbb{Z}[x]$ of the form $f = \sum_{i=0}^{\beta(n)-1} a_i(x)_i$ with $[f]_{p^n} = F$, where $0 \le a_i < p^{n-v_p(i!)}$ for $i = 0, \ldots, \beta(n)-1$.*
It follows that, $|\mathcal{F}(\mathbb{Z}_{p^n})| = p^{\sum_{i=1}^n \beta(i)}$.

Keep the notations of Notation 3.5.2. The following theorem gives canonical representations for the elements of $\mathcal{F}(\mathbb{Z}_{p^n})^\times$ as linear combinations of the falling factorials $(x)_j$ and those of the unique representations of the elements of $\mathcal{F}(\mathbb{Z}_p)^\times$ obtained by Lagrange interpolation (see Remark 3.4.3).

Theorem 3.5.7. *Let $l_1, \ldots, l_{(p-1)^p}$ denote the unique representations of the elements of $\mathcal{F}(\mathbb{Z}_p)^\times$ by polynomials of degree less than p obtained by Lagrange interpolation. Let $n \ge 2$. Then every element in $\mathcal{F}(\mathbb{Z}_{p^n})^\times$ can be represented uniquely by a polynomial of the form*

$$l_s(x) + \sum_{i=0}^{\beta(n)-1} a_i(x)_i, \tag{3.1}$$

where $0 \le a_i < p^{n-v_p(i!)}$ for $0 \le i < \beta(n)$ with $p \mid a_i$ for $i < p$; and $s = 1, \ldots, (p-1)^p$.

Proof. Let A denote the set of all polynomials in $\mathbb{Z}[x]$ that satisfy the conditions of equation (3.1). By Remark 3.5.1 (1), every element of A induces a unit-valued polynomial function on $\mathbb{Z}_{p^n}$. Now, let B denote the set of all polynomials of the form

$$\sum_{i=0}^{\beta(n)-1} a_i(x)_i, \text{ where } 0 \leq a_i < p^{n-v_p(i!)} \text{ for } 0 \leq i < \beta(n) \text{ with } p \mid a_i \text{ for } i < p. \tag{3.2}$$

Clearly,

$$|A| = (p-1)^p |B|.$$

In the light of Equation (3.2) and Lemma 3.5.6,

$$|B| = \frac{|\mathcal{F}(\mathbb{Z}_{p^n})|}{p^p} = \frac{p^{\sum_{i=1}^{n} \beta(i)}}{p^p} = p^{\sum_{i=2}^{n} \beta(i)}.$$

Therefore, by Theorem 3.5.5,

$$|A| = (p-1)^p p^{\sum_{i=2}^{n} \beta(i)} = |\mathcal{F}(\mathbb{Z}_{p^n})^\times|.$$

To complete the proof, we need only show that $[f]_{p^n} \neq [g]_{p^n}$ whenever f, g are distinct elements of A. For simplicity, write $f = l_{s_1} + f_1$ and $g = l_{s_2} + g_1$, where $f_1, g_1 \in B$ and $s_1, s_2 \in \{1, \ldots, (p-1)^p\}$. First, we notice that if $s_1 \neq s_2$, then $[f]_p = [l_{s_1}]_p \neq [l_{s_2}]_p = [g]_p$. Thus $[f]_{p^n} \neq [g]_{p^n}$ if $s_1 \neq s_2$. Now assume that $s_1 = s_2$, and $f_1 \neq g_1$. Then $[f_1]_{p^n} \neq [g_1]_{p^n}$ by Lemma 3.5.6, and hence

$$[f]_{p^n} = [l_{s_1} + f_1]_{p^n} = [l_{s_1}]_{p^n} + [f_1]_{p^n} \neq [l_{s_1}]_{p^n} + [g_1]_{p^n} = [l_{s_1} + g_1]_{p^n} = [g]_{p^n}.$$

□

Counterexample 3.5.8. *Let $R = \mathbb{Z}_4 = \{0, 1, 2, 3\}$. In this case, $\mathbb{Z}_4[\alpha] = \{a + b\alpha \colon a, b \in \mathbb{Z}_4\}$. Consider now the polynomial $f(x) = (x^2 - x)^2$. By Fermat's little theorem, f is a null polynomial on $\mathbb{Z}_4$; hence every unit-valued polynomial function is induced by a polynomial of degree less than 4. Next we show that f is null on $\mathbb{Z}_4[\alpha]$. So, if $a, b \in \mathbb{Z}_4$, then*

$$\begin{aligned} f(a + b\alpha) &= \big((a + b\alpha)^2 - (a + b\alpha)\big)^2 = \big((a^2 + 2ab\alpha) - (a + b\alpha)\big)^2 \\ &= \big((a^2 - a) + (2ab - b)\alpha\big)^2 = (a^2 - a)^2 + 2(a^2 - a)(2ab - b)\alpha = 0. \end{aligned}$$

Thus f is null on $\mathbb{Z}_4[\alpha]$; whence every polynomial function on $\mathbb{Z}_4[\alpha]$ is represented by a polynomial of degree less than 4. The null polynomials on $\mathbb{Z}_4$ of degree less than 4 are

$$f_1 = 0, \ f_2 = 2(x^2 - x), \ f_3 = 2(x^3 - x) \text{ and } f_4 = 2(x^3 - x^2).$$

Then simple calculations shows that $1 + f_1', \ldots, 1 + f_4'$ induce four different unit-valued functions on $\mathbb{Z}_4$. Thus $|St_\alpha(\mathbb{Z}_4)| = 4$, but $|\mathcal{F}(\mathbb{Z}_4)^\times| = 2^{\beta(2)} = 16$ by Theorem 3.5.5. Furthermore, by

Remark 3.4.10 (1), there is an epimorphism from $\mathcal{P}_{\mathbb{Z}_4}(\mathbb{Z}_4[\alpha])$ onto $\mathcal{P}(\mathbb{Z}_4)$ which admits $St_\alpha(\mathbb{Z}_4)$ as a kernel. Thus $|\mathcal{P}_{\mathbb{Z}_4}(\mathbb{Z}_4[\alpha])| = |\mathcal{P}(\mathbb{Z}_4)||St_\alpha(\mathbb{Z}_4)|$, and hence

$$|\mathcal{P}(\mathbb{Z}_4) \ltimes_\theta \mathcal{F}(\mathbb{Z}_4)^\times| = |\mathcal{P}(\mathbb{Z}_4)||\mathcal{F}(\mathbb{Z}_4)^\times| > |\mathcal{P}(\mathbb{Z}_4)||St_\alpha(\mathbb{Z}_4)| = |\mathcal{P}_{\mathbb{Z}_4}(\mathbb{Z}_4[\alpha])|.$$

This shows that in general the homomorphisms of Proposition 3.3.8 and Theorem 3.4.5 need not be isomorphisms.

4 Ideals of the polynomial ring closed under products of formal derivative

The content of this chapter is the accepted paper [3]. It will appear in the International Electronic Journal of Algebra with the title " On a property of the ideals of the polynomial ring $R[x]$".

Abstract

Let R be a commutative ring with unity $1 \neq 0$. In this paper we introduce the definition of the first derivative property on the ideals of the polynomial ring $R[x]$. In particular, when R is a finite local ring with principal maximal ideal $\mathfrak{m} \neq \{0\}$ of index of nilpotency e, where $1 < e \leq |R/\mathfrak{m}| + 1$, we show that the null ideal consisting of polynomials inducing the zero function on R satisfies this property. As an application, when R is a finite local ring with null ideal satisfying this property, we prove that the stabilizer group of R in the group of polynomial permutations on the ring $R[x]/(x^2)$, is isomorphic to a certain factor group of the null ideal.

Keywords. Commutative rings, polynomial ring, null ideal, null polynomials, Henselian ring, finite local ring, dual numbers, polynomial permutations, permutation polynomials, finite permutation groups

2010 Mathematics Subject Classification: Primary 13F20; Secondary 06B10, 13J15, 11T06, 05A05, 13B25, 20B35

4.1 Introduction

Let R be a commutative ring with unity $1 \neq 0$, and $R[x]$ be the polynomial ring over R of one indeterminate x. In addition to the usual operations on polynomials, $R[x]$ has a further operation, which appears in a normal way, namely the formal derivative of polynomials. Nöbauer used this operation to define the derivative of ideals with a certain property [68].

Another well known feature of $R[x]$ is that every polynomial $f(x) = \sum_{j=0}^{k} a_j x^j \in R[x]$ induces a function $F\colon R \longrightarrow R$, where $F(r) = \sum_{j=0}^{k} a_j r^j$ for all $r \in R$. In this case F is called a polynomial function on R. The set of all polynomial functions on R is a monoid via composition of functions. Moreover, when the function F is a bijection we say F is a polynomial permutation

while f is a permutation polynomial. Obviously, the set of all polynomial permutations is a group, which we denote by $\mathcal{P}(R)$. Further, $\mathcal{P}(R)$ forms the group of units of the monoid of polynomial functions.

If a polynomial $g \in R[x]$ induces the constant zero function over R, that is $g(r) = 0$ for each $r \in R$, then g is called a null polynomial over (on) R. The set of all null polynomials on R is an ideal of $R[x]$, which we denote by N_R and we call it the null ideal (on R). The null ideal N_R supplies the ring of polynomials $R[x]$ with an equivalence relation in which two polynomials $g, h \in R[x]$ are equivalent whenever $g - h \in N_R$. In other words, two polynomials are related in this relation if and only if they induce the same function on R. Moreover, every equivalence class corresponds to one polynomial function on R and vise versa.

This paper considers a property of the ideals of the ring $R[x]$ and its application to the group of polynomial permutations on finite rings. In particular, for a finite local ring R with null ideal having this property, we prove some facts about the permutation polynomials on the ring $R[x]/(x^2)$.

The property defined in the paper depends on the formal derivative of polynomials, however it is completely different from the one considered in [68].

Throughout this paper for a local ring R, let $\mathfrak{m}$ denote its maximal ideal and let $N(\mathfrak{m})$ be the set of all polynomials over R which vanish on the ideal $\mathfrak{m}$. Evidently, $N(\mathfrak{m})$ is an ideal in the polynomial ring $R[x]$ containing N_R. For $f \in R[x]$ with $f(x) = \sum_{i=0}^{n} a_i x^i$, let f' denote its formal derivative; i.e., $f'(x) = \sum_{i=1}^{n} i a_i x^{i-1}$.

4.2 The first derivative property and the null ideal

We begin this section with the definition of our property. Then we prove some supplementary results. Later, we show that the null ideal N_R has this property for a wide class of finite local rings with principal maximal ideals.

Definition 4.2.1. *Let R be a commutative ring. An ideal I of $R[x]$ satisfies the first derivative property if $g, h \in I$ implies that $g'h' \in I$.*

For shortness we use the abbreviation FDP for the first derivative property.

Proposition 4.2.2. *Let I, J be ideals of $R[x]$. Then:*

1. *I^2 satisfies FDP;*
2. *if I, J satisfy FDP, then IJ satisfies FDP.*

Proof. We prove (2) and leave (1) to the reader. Let $f, g \in IJ$. Then there exist polynomials $f_1, \ldots, f_n; g_1, \ldots, g_m \in I$ and $h_1, \ldots, h_n; k_1, \ldots, k_m \in J$ such that $f = \sum_{i=1}^{n} f_i h_i$ and $g = \sum_{j=1}^{m} g_j k_j$. So $f' = \sum_{i=1}^{n} f_i' h_i + \sum_{i=1}^{n} f_i h_i'$ and $g' = \sum_{j=1}^{m} g_j' k_j + \sum_{j=1}^{m} g_j k_j'$. Obviously, $\sum_{i=1}^{n} f_i h_i', \sum_{j=1}^{m} g_j k_j' \in I$ and

$\sum_{i=1}^{n} f_i'h_i, \sum_{j=1}^{m} g_j'k_j \in J$. On the other hand, by Definition 4.2.1, we have $f_i'g_j' \in I$ for every $1 \leq i \leq n; 1 \leq j \leq m$. Hence

$$(\sum_{i=1}^{n} f_i'h_i)(\sum_{j=1}^{m} g_j'k_j) = \sum_{i,j} f_i'g_j'h_ik_j \in IJ.$$

Similarly, $(\sum_{i=1}^{n} f_ih_i')(\sum_{j=1}^{m} g_jk_j') \in IJ$. Therefore

$$f'g' = (\sum_{i=1}^{n} f_i'h_i + \sum_{i=1}^{n} f_ih_i')(\sum_{j=1}^{m} g_j'k_j + \sum_{j=1}^{m} g_jk_j') \in IJ. \qquad \square$$

The following result gives a criterion for FDP for finitely generated ideals over $R[x]$.

Proposition 4.2.3. *Let I be an ideal of $R[x]$ and suppose that $I = (f_1, \ldots, f_n)$ for some $f_1, \ldots, f_n \in R[x]$. Then I satisfies FDP if and only if $f_i'f_j' \in I$ for all $i, j \in \{1, \ldots, n\}$.*

Proof. ($\Rightarrow$) Obvious.
($\Leftarrow$) Suppose that $f_i'f_j' \in I$ for any two generators $f_i, f_j \in I$. Let $g, h \in I$. Then there exist $g_1, \ldots, g_n; h_1, \ldots, h_n \in R[x]$ such that $g(x) = \sum_{i=1}^{n} g_if_i$ and $h(x) = \sum_{i=1}^{n} h_if_i$.
We have

$$g' = \sum_{i=1}^{n} g_i'f_i + \sum_{i=1}^{n} g_if_i' \quad \text{and} \quad h' = \sum_{i=1}^{n} h_i'f_i + \sum_{i=1}^{n} h_if_i'.$$

So

$$g'h' = (\sum_{i=1}^{n} g_i'f_i)h' + (\sum_{i=1}^{n} g_if_i')(\sum_{i=1}^{n} h_i'f_i) + (\sum_{i,j=1}^{n} g_ih_jf_i'f_j').$$

Clearly, $g'h' \in I$, and hence I satisfies FDP. $\square$

Remark 4.2.4. *Let R be a local ring with maximal ideal $\mathfrak{m}$ and residue field $\mathbb{F}_q$, and let $\lambda(x) = \prod_{i=1}^{q}(x - c_i)$, where $\{c_1, \ldots, c_q\}$ is any complete systems of residue modulo $\mathfrak{m}$. It is obvious that $c_i - c_j$ is a unit in R whenever $i \neq j$; hence for every $r \in R$ such that $r \equiv c_i \mod \mathfrak{m}$, $r - c_j$ is a unit. Then the following lemma follows.*

Lemma 4.2.5. *Let $r \in R$. Then $\lambda'(r)$ is a unit in R.*

Remark 4.2.6. *It is a celebrated fact that every finite local commutative ring is a Henselian ring, i.e., a local ring in which Hensel's lemma holds, (see for example, [57, Theorem. XIII.4]). This allows us to use some facts about the ideals $\mathfrak{m}, N_R$, when R is a Henselian ring, from [78] to improve our related ideas on finite local rings.*

Lemma 4.2.7. *[78, Corollary 2.11] Let R be a Henselian ring. Then $\lambda(R) = \mathfrak{m}$.*

Lemma 4.2.8. *[78, Theorem 4.2] Let R be a Henselian ring and $\lambda(x)$ as in Remark 4.2.4. If $N(\mathfrak{m}) = (F_1(x), \ldots, F_n(x))$, then $N_R = (F_1(\lambda(x)), \ldots, F_n(\lambda(x)))$.*

Recall from the introduction the definitions of the ideals $N_R, N(\mathfrak{m})$. The following result shows that, for a Henselian ring R and a finitely generated ideal $N(\mathfrak{m})$, either both $N(\mathfrak{m})$ and N_R satisfy FDP or neither satisfies FDP.

Theorem 4.2.9. *Let R be a Henselian ring and $\lambda(x)$ as in Remark 4.2.4. If $N(\mathfrak{m}) = (F_1(x), \ldots, F_n(x))$, then N_R satisfies FDP if and only if $N(\mathfrak{m})$ satisfies FDP.*

Proof. By Lemma 4.2.8, $N_R = (F_1(\lambda(x)), \ldots, F_n(\lambda(x)))$.

($\Leftarrow$) Suppose that $N(\mathfrak{m})$ satisfies FDP. Then for every $i, j \in \{1, \ldots, n\}$ there exists $h_{i,j} \in N(\mathfrak{m})$ such that $F_i'F_j' = h_{i,j}$. Hence $F_i'(\lambda(x))F_j'(\lambda(x)) = h_{i,j}(\lambda(x)) \in N_R$ since $\lambda(R) = \mathfrak{m}$ by Lemma 4.2.7.

Now

$$(F_i(\lambda(x)))'(F_j(\lambda(x)))' = (\lambda'(x))^2 F_i'(\lambda(x))F_j'(\lambda(x)) = (\lambda'(x))^2 h_{i,j}(\lambda(x)) \in N_R.$$

Thus N_R satisfies FDP by Proposition 4.2.3.

($\Rightarrow$) Suppose that N_R satisfies FDP. Then for every $i, j \in \{1, \ldots, n\}$ we have

$$(F_i(\lambda(x)))'(F_j(\lambda(x)))' = (\lambda'(x))^2 F_i'(\lambda(x))F_j'(\lambda(x)) \in N_R.$$

Now let $r \in R$ be arbitrary. Then, by the definition of N_R,

$$(\lambda'(r))^2 F_i'(\lambda(r))F_j'(\lambda(r)) = 0.$$

Hence $F_i'(\lambda(r))F_j'(\lambda(r)) = 0$ since $\lambda'(r)$ is a unit by Lemma 4.2.5, whence $F_i'(\lambda(x))F_j'(\lambda(x)) \in N_R$. But, $\lambda(R) = \mathfrak{m}$ by Lemma 4.2.7. Therefore $F_i'F_j' \in N(\mathfrak{m})$ for every $i, j \in \{1, \ldots, n\}$. Thus $N(\mathfrak{m})$ satisfies FDP by Proposition 4.2.3. □

Remark 4.2.10. *Notice that we don't require R to be Noetherian. In fact there exists a Henselian ring which is non-Noetherian with a finitely generated ideal $N(\mathfrak{m})$ (see for example, [78, Example 3.2]).*

Our aim now is to show that the null ideal N_R satisfies FDP for every finite local ring with a nonzero principal maximal ideal of index of nilpotency less than or equal $q + 1$, where q is the cardinality of the residue field $\mathbb{F}_q$. To do so, we need this lemma.

Lemma 4.2.11. *[78, Theorem 4.4] Let R be a finite local ring with principal maximal ideal $\mathfrak{m} = (m)$ and residue field $\mathbb{F}_q$. Suppose e is the index of nilpotency of $\mathfrak{m}$. If $e \leq q$, then $N(\mathfrak{m}) = (x, m)^e$; if $e = q + 1$, then $N(\mathfrak{m}) = (x, m)^e + (x^q - m^{q-1}x)$.*

Theorem 4.2.12. *Let R be a finite local ring with principal maximal ideal $\mathfrak{m} = (m)$ and residue field $\mathbb{F}_q$. Suppose e is the index of nilpotency of $\mathfrak{m}$. If $1 < e \leq q + 1$ then N_R satisfies FDP, provided $e \geq 4$ when $e = q + 1$.*

Proof. In view of Theorem 4.2.9, we need only to prove that $N(\mathfrak{m})$ satisfies FDP. Now $N(\mathfrak{m})$ is finitely generated since R is finite, so it is enough to show that $g'h' \in N(\mathfrak{m})$ for every pair of generators g, h of $N(\mathfrak{m})$ by Proposition 4.2.3. First assume that $1 < e < q+1$. By Lemma 4.2.11, $N(\mathfrak{m})$ is generated by the set $\{x^e, mx^{e-1}, \ldots, m^{e-1}x\}$. Let g, h be any generators of $N(\mathfrak{m})$. Then $g(x) = m^j x^{e-j}$ and $h(x) = m^i x^{e-i}$ for some $0 \leq i, j \leq e-1$. Therefore $g'(x)h'(x) = (e-i)(e-j)m^{i+j}x^{2e-i-j-2} \in N(\mathfrak{m})$ since $e \geq 2$, and so $N(\mathfrak{m})$ satisfies FDP.

We now consider the case $e = q+1$. By Lemma 4.2.11, $\mathfrak{m}$ is generated by the following set

$$\{x^e, mx^{e-1}, \ldots, m^{e-1}x, x^q - m^{q-1}x\}.$$

Since $q \in \mathfrak{m}$ we have $q = rm$ for some $r \in R$. Let g, h any two generators of $N(\mathfrak{m})$. We distinguish three main cases.

Case 1. $g(x) = h(x) = x^q - m^{q-1}x$. Then

$$g'(x)h'(x) = (qx^{q-1} - m^{q-1})^2 = q^2x^{2q-2} - 2qm^{q-1}x^{q-1} + m^{2q-2},$$

whence

$$g'(x)h'(x) = r^2m^2x^{2e-4} - 2rm^{e-1}x^{e-2} + m^{2e-4}.$$

Evidently, $r^2m^2x^{2e-4} - 2rm^{e-1}x^{e-2} \in N(\mathfrak{m})$ since $e = q+1 \geq 3$. Thus $g'h' \in N(\mathfrak{m})$ if and only if $m^{2e-4} \in N(\mathfrak{m})$ if and only if $m^{2e-4} = 0$, provided $e \geq 4$.

Case 2. $g(x) = x^q - m^{q-1}x$ and $h(x) = m^i x^{e-i}$ for some $0 \leq i \leq e-1$. Then

$$g'(x)h'(x) = (e-i)m^i x^{e-i-1}(qx^{q-1} - m^{q-1}) = (e-i)m^i x^{e-i-1}(rmx^{e-2} - m^{e-2}) =$$
$$(e-i)m^{i+1}x^{e-i-1}(rx^{e-2} - m^{e-3}) \in N(\mathfrak{m}) \text{ since } m^{i+1}x^{e-i-1} \in N(\mathfrak{m}) \text{ and } e \geq 4 > 3.$$

Case 3. $g(x) = m^j x^{e-j}$ and $h(x) = m^i x^{e-i}$ for some $0 \leq i, j \leq e-1$. Then

$$g'(x)h'(x) = (e-i)(e-j)m^{i+j}x^{2e-i-j-2} \in N(\mathfrak{m}) \text{ since } e \geq 4.$$

Therefore $N(\mathfrak{m})$ satisfies FDP. □

Remark 4.2.13.

1. *If $e = 1$, then $R = \mathbb{F}_q$. In this case $N_{\mathbb{F}_q} = (x^q - x)\mathbb{F}_q[x]$. But, $N_{\mathbb{F}_q}$ does not satisfy FDP. Because, if we take $g(x) = x^q - x$, then $(g'(x))^2 = (qx^{q-1} - 1)^2 = 1 \notin N_{\mathbb{F}_q}$.*

2. *Consider $g(x) = (x^2 - x)^2 - 2(x^2 - x) \in \mathbb{Z}_8[x]$, by Fermat's Theorem, one can show easily that $g(a) \equiv 0 \pmod 8$ for every $a \in \mathbb{Z}_8$, that is, $g \in N_{\mathbb{Z}_8}$. However, $N_{\mathbb{Z}_8}$ does not satisfy FDP since $(g')^2 \notin N_{\mathbb{Z}_8}$. Indeed, $(g'(1))^2 = 4 \not\equiv 0 \pmod 8$. Note that $e = q+1 = 3 < 4$.*

Corollary 4.2.14. *Let n be a positive integer and p a prime number.*

1. *If $p > 2$, then $N_{\mathbb{Z}_{p^n}}$ satisfies FDP for every $1 < n \leq p + 1$.*

2. *If $p = 2$, then $N_{\mathbb{Z}_4}$ satisfies FDP.*

Although we defined null ideals for finite rings, the definition is still true for infinite rings. We consider this fact in the following example.

Example 4.2.15. *Let R be a boolean ring (not necessary finite). By definition, $f = x^2 - x \in N_R$. But, $(f')^2 = (-1)^2 = 1 \notin N_R$.*

Right now we have achieved our first main goal, that is, showing the existence of a wide class of finite local rings with null ideals having FDP. In the next section, we employ FDP to infer some facts about a group of polynomial permutations over the ring $R[x]/(x^2)$.

4.3 Applications on the polynomial permutations of the ring $R[x]/(x^2)$

In this section, for a finite local commutative ring R with the null ideal N_R satisfying the first derivative property, we prove some facts about some kind of permutation polynomials on the ring $R[x]/(x^2)$.

Throughout this section all rings are finite.

Recall that $R[x]/(x^2)$ is isomorphic to the ring $R[\alpha] = \{a + b\alpha \colon a, b \in R\}$, where $\alpha \notin R$ and $\alpha^2 = 0$. Here are some easily verifiable facts about polynomials over $R[\alpha]$.

Fact 4.3.1. *Let $h \in R[x]$. Then $h(a + b\alpha) = h(a) + bh'(a)\alpha$ for each $a, b \in R$.*

Fact 4.3.2. *Let $g \in R[\alpha][x]$. Then $g = g_1 + g_2\alpha$ for some $g_1, g_2 \in R[x]$.*

Recall from the introduction that $\mathcal{P}(R[\alpha])$ denotes the group of polynomial permutations on the ring $R[\alpha]$.

Definition 4.3.3. *Let $St_\alpha(R) = \{F \in \mathcal{P}(R[\alpha]) \colon F(r) = r \text{ for each } r \in R\}$.*

Obviously, $St_\alpha(R)$ is a nonempty finite subset of $\mathcal{P}(R[\alpha])$. Further, it is closed under the composition of functions. Therefore $St_\alpha(R)$ is a subgroup of $\mathcal{P}(R[\alpha])$. The group $St_\alpha(R)$ by definition stabilizes every element of R; for this we call it the stabilizer group of R in the group of polynomial permutations of $R[\alpha]$ or more shortly the stabilizer group.

Lemma 4.3.4. *Let A be a ring and $g, h \in A[x]$. If g and h induce the same function over A, then there exists $f \in N_A$ such that $g = h + f$.*

Proof. Take $f = g - h$. Then $f \in N_A$. □

We need some facts from [2]. However, we prove these facts as the proofs do not depend on extra materials.

Lemma 4.3.5. *[2, Lemma 3.4] Let $h \in N_R$. Then $h\alpha$ induces the zero function over $R[\alpha]$.*

Proof. By Fact 4.3.1, $h(a+b\alpha)\alpha = (h(a)+bh'(a)\alpha)\alpha = h(a)\alpha + 0 = 0\alpha = 0$ for all $a, b \in R$. □

Proposition 4.3.6. *[2, Proposition 4.6] Let R be a ring. Then*

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

Proof. It is obvious that

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

Now let $F \in \mathcal{P}(R[\alpha])$ such that $F(r) = r$ for each $r \in R$. Since F is a polynomial permutation over $R[\alpha]$, F is induced by a polynomial $g \in R[\alpha][x]$. By Fact 4.3.2, $g = g_0 + g_1\,\alpha$, where $g_0, g_1 \in R[x]$. Now $r = F(r) = g(r) = g_0(r) + g_1(r)\,\alpha$ for each $r \in R$. Then $g_1(r)\,\alpha = 0$, and so $g_1(r) = 0$ for each $r \in R$, i.e., $g_1 \in N_R$. Hence, $g_1\alpha$ is a null polynomial over $R[\alpha]$ by Lemma 4.3.5. Thus g_0 and $g_0 + g_1\alpha$ both induce F on $R[\alpha]$, i.e., F is induced by g_0. Further, $g_0 \equiv x \mod N_R$, i.e., g_0 induces the identity on R, and therefore $g_0(x) = x + h(x)$ for some $h \in N_R$ by Lemma 4.3.4. This shows the other inclusion. □

Lemma 4.3.7. *Let $F \in St_\alpha(R)$. Suppose that $x + f(x)$ induces F, where $f \in N_R$. Then the following statements are equivalent*

1. *$(f')^2 \in N_R$;*
2. *$x - f(x)$ induces F^{-1};*
3. *$F^k = \underbrace{F \circ F \circ \cdots \circ F}_{k \text{ times}}$ is induced by $x + kf(x)$ for every $k \in \mathbb{N}$.*

Proof. (1)⇒ (2) Let G be the function induced by $x - f(x)$. Then for every $r, s \in R$ we have

$$\begin{aligned}
G \circ F(r + s\,\alpha) &= G \circ (r + s\,\alpha + f(r + s\,\alpha)) \\
&= G \circ (r + s\,\alpha + f(r) + sf'(r)\,\alpha) \text{ (by Fact 4.3.1)} \\
&= G \circ (r + s\,\alpha + sf'(r)\,\alpha) \quad \text{(since } f \text{ is null)} \\
&= (r + s\,\alpha + sf'(r)\,\alpha) - f(r + (s + sf'(r))\,\alpha) \\
&= (r + s\,\alpha + sf'(r)\,\alpha) - \big(f(r) + (s + sf'(r))f'(r)\,\alpha\big) \text{ (by Fact 4.3.1)} \\
&= r + s\,\alpha + sf'(r)\,\alpha - sf'(r)\,\alpha \quad \text{(since } (f')^2 \in N_R) \\
&= r + s\,\alpha\,.
\end{aligned}$$

Thus $F^{-1} = G$, whence $x - f(x)$ induces F^{-1}.

(2)⇒ (1) If $x - f(x)$ induces F^{-1}, then one can use the previous calculations to get that for every $r, s \in R$, $r + s\alpha = F^{-1} \circ F(r + s\,\alpha) = r + s\,\alpha - s(f'(r))^2\alpha$.

Hence $s(f'(r))^2\alpha = 0$, whence $(f'(r))^2 s = 0$ for every $r, s \in R$. So if $s = 1$, we have $(f'(r))^2 = 0$ for every $r \in R$. Therefore $(f')^2 \in N_R$.

(1)⇒(3) By induction on k.

(3)⇒(1) Let $k = 2$. Then F^2 is induced by $x + 2f(x)$, and so that

$$F^2(r + s\,\alpha) = r + s\,\alpha + 2f'(r)s\,\alpha\,.$$

While, by successive calculations,

$$F^2(r + s\,\alpha) = F \circ F(r + s\,\alpha) = F(r + s\,\alpha + sf'(r)\,\alpha) = r + s\,\alpha + s(2f'(r) + (f'(r))^2)\alpha.$$

Then from the two expression of $F^2(r + s\,\alpha)$ follows that $s(f'(r))^2 = 0$ for every $r, s \in R$. Thus $(f'(r))^2 = 0$ for every $r \in R$, and hence $(f')^2 \in N_R$. □

In the following proposition, we show that how FDP is useful in describing the behavior of the elements of the stabilizer group $St_\alpha(R)$ in connection with their polynomial expressions.

Proposition 4.3.8. *Let $F \in St_\alpha(R)$. Suppose that $x + f(x)$ induces F, where $f \in N_R$. If N_R satisfies FDP, then the following statements hold:*

1. *$x - f(x)$ induces F^{-1};*
2. *$F^k = \underbrace{F \circ F \circ \cdots \circ F}_{k \text{ times}}$ is induced by $x + kf(x)$ for every $k \in \mathbb{N}$;*
3. *if $G \in St_\alpha(R)$ is induced by $x + g(x)$, where $g \in N_R$, then $x + f(x) + g(x)$ induces $F \circ G$.*

Proof. Since N_R satisfies FDP, we have $(f')^2 \in N_R$, and hence (1) and (2) hold by Lemma 4.3.7.

(3) Let $G \in St_\alpha(R)$ be induced by $x + g(x)$, where $g \in N_R$. Then by FDP, $f'g' \in N_R$. Now we have for every $r, s \in R$, by Fact 4.3.1 and since $f, g \in N_R$,

$$\begin{aligned} G \circ F(r + s\,\alpha) &= G \circ (r + s\,\alpha + sf'(r)\,\alpha) \\ &= (r + s\,\alpha + sf'(r)\,\alpha) + g(r + s\,\alpha + sf'(r)\,\alpha) \\ &= (r + s\,\alpha + sf'(r)\,\alpha) + (s + sf'(r))g'(r)\,\alpha \\ &= r + s\,\alpha + sf'(r)\,\alpha + sg'(r)\,\alpha \ \text{(by FDP)}. \end{aligned}$$

Therefore $G \circ F$ is induced by the polynomial $x + f(x) + g(x)$. □

We prove now a special case of [2, Theorem 4.1].

Lemma 4.3.9. *Let $g \in R[x]$. Then g is a permutation polynomial on $R[\alpha]$ if and only if g is a permutation polynomial on R and $g'(r)$ is a unit for every $r \in R$.*

Proof. (⇒) Let $c \in R$. Then $c \in R[\alpha]$. Since g is a permutation polynomial over $R[\alpha]$, there exist $a, b \in R$ such that $g(a + b\alpha) = c$. Thus $g(a) + bg'(a)\alpha = c$ by Fact 4.3.1. So $g(a) = c$, whence g is surjective on the ring R. Hence g is a permutation polynomial on R.

Let $a \in R$ and suppose that $g'(a)$ is a non-unit in R. Then $g'(a)$ is a zerodivisor of R. Let $b \in R$, $b \neq 0$, such that $bg'(a) = 0$. Then $g(a+b\alpha) = g(a)+bg'(a)\alpha = g(a)$, so g is not injective, which contradicts to the fact being bijective over R.
($\Leftarrow$) We need only to prove that g is injective. For this let $a, b, c, d \in R$ such that $g(a + b\alpha) = g(c + d\alpha)$. Then $g(a) + bg'(a)\alpha = g(c) + dg'(c)\alpha$ by Fact 4.3.1. Thus we have $g(a) = g(c)$ and $bg'(a) = dg'(c)$. Hence $a = c$ since g is a permutation polynomial on R. So, since $g'(a)$ is a unit in R, $b = d$ follows. □

We recall the following well-known result.

Lemma 4.3.10. *[63, Theorem 3] Let R be a local ring with nonzero maximal ideal $\mathfrak{m}$, and $g \in R[x]$. Then g is a permutation polynomial on R if and only if the following conditions hold:*

1. *g is a permutation polynomial on $R/\mathfrak{m}$;*
2. *$g'(r) \not\equiv 0 \mod \mathfrak{m}$, for all $r \in R$.*

Lemma 4.3.11. *Let R be a local ring with nonzero maximal ideal $\mathfrak{m}$, and $g \in R[x]$. Then g is a permutation polynomial on $R[\alpha]$ if and only if g is a permutation polynomial on R.*

Proof. ($\Rightarrow$) Follows by Lemma 4.3.9.
($\Leftarrow$) Suppose that g is a permutation polynomial on R. Then for all $a \in R$, $g'(a) \not\equiv 0 \mod \mathfrak{m}$ by Lemma 4.3.10. Thus for all $a \in R$, $g'(a)$ is a unit in R since R is a local ring. Hence g is a permutation polynomial on $R[\alpha]$ by Lemma 4.3.9. □

Corollary 4.3.12. *Let R be a local ring with nonzero maximal ideal $\mathfrak{m}$ and let $f \in N_R$. If F is the function induced by $x + f(x)$, then $F \in St_\alpha(R)$.*

In the rest of the paper let $N'_R = \{f \in N_R \colon f' \in N_R\}$. It is evident that N'_R is an ideal of $R[x]$ contained in N_R.

Lemma 4.3.13. *Let $g \in R[x]$. Then g is a null polynomial on $R[\alpha]$ if and only if $g \in N'_R$.*

Proof. By Fact 4.3.1, $g(a + b\alpha) = g(a) + bg'(a)\alpha$ for every $a, b \in R$.
($\Leftarrow$) Immediately.
($\Rightarrow$) Since g is null on $R[\alpha]$ we have that $g(a) + bg'(a)\alpha = 0$ for every $a, b \in R$. This is equivalent to $g(a) = bg'(a) = 0$ for every $a, b \in R$. Thus if $b = 1$, we have $g(a) = g'(a) = 0$ for very $a \in R$. Hence $g \in N'_R$. □

We are now ready to prove our main result for this section.

Proposition 4.3.14. *Let R be a local ring with nonzero maximal ideal $\mathfrak{m}$. If N_R satisfies FDP, then*

$$St_\alpha(R) \cong N_R/N'_R.$$

Proof. Let $f \in N_R$, then obviously $[x + f(x)] \in St_\alpha(R)$ by Corollary 4.3.12, where $[x + f(x)]$ denotes the function induced by $x + f(x)$ on $R[\alpha]$. Now define a function $\psi\colon N_R \longrightarrow St_\alpha(R)$ by $\psi(f) = [x + f(x)]$. By Proposition 4.3.6, ψ is surjective. Let $g \in N_R$. Then set

$$F_1 = [x + f(x)], \quad F_2 = [x + g(x)] \quad \text{and} \quad F_3 = [x + f(x) + g(x)].$$

By Proposition 4.3.8, $F_1 \circ F_2 = F_3$. Therefore $\psi(f + g) = \psi(f) \circ \psi(g)$, whence ψ is a homomorphism. Hence $N_R/\ker\psi \cong St_\alpha(R)$ by the first isomorphism theorem.

Now,

$$\ker\psi = \{f \in N_R\colon [x + f(x)] \text{ is the identity permutation on } R[\alpha]\}.$$

By Lemma 4.3.13, $N_R' \subseteq \ker\psi$. On the other, if $f \in \ker\psi$, then $x + f(x)$ induces the identity on $R[\alpha]$. Hence $x + f(x) = x + h(x)$ for some null polynomial (on $R[\alpha]$) $h \in R[\alpha][x]$ by Lemma 4.3.4. Thus $f = h$ and f is a null polynomial on $R[\alpha]$. Since $f \in R[x]$ we have $f \in N_R'$ by Lemma 4.3.13. Therefore $\ker\psi \subseteq N_R'$. □

Remark 4.3.15. *In [2], for the case $R = \mathbb{Z}_{p^n}$ the ring of integers modulo p^n, it was only proved that $|St_\alpha(\mathbb{Z}_{p^n})| = [N_{\mathbb{Z}_{p^n}} : N'_{\mathbb{Z}_{p^n}}]$, for every $n > 1$, and it was unclear whether $St_\alpha(\mathbb{Z}_{p^n})$ and $N_{\mathbb{Z}_{p^n}}/N'_{\mathbb{Z}_{p^n}}$ are isomorphic or not. But, now Proposition 4.3.14 tells us they are isomorphic via a map induced by the function ψ defined in the above proof, when N_R satisfies FDP.*

Corollary 4.3.16. *Let R be a local ring with nonzero maximal ideal $\mathfrak{m}$. The function $\psi\colon N_R \longrightarrow St_\alpha(R)$, defined by $\psi(f) = [x + f(x)]$ for every $f \in N_R$, is a homomorphism if and only if N_R satisfies FDP.*

Proof. ($\Leftarrow$) Follows by the same argument given in the proof of the previous proposition.

($\Rightarrow$) Assume that ψ is a homomorphism. Let $f, g \in N_R$. Put $F_1 = [x + f(x)], F_2 = [x + g(x)]$ and $F_3 = [x + f(x) + g(x)]$. Then $F_1, F_2, F_3 \in St_\alpha(R)$ by Corollary 4.3.12. We now consider $\psi(f + g) = [x + f(x) + g(x)] = F_3$. But, since ψ is a homomorphism by assumption, we have that $\psi(f + g) = \psi(f) \circ \psi(g) = F_1 \circ F_2$. Thus $F_1 \circ F_2 = F_3$. Now, for every $a, b \in R$, we have

$$F_1 \circ F_2(a + b\alpha) = a + b\alpha + b(g'(a) + f'(b) + f'(a)g'(a))\alpha,$$

and $F_3(a + b\alpha) = a + b\alpha + b(f'(a) + g'(a))\alpha$. Hence $bf'(a)g'(a)\alpha = 0$ for every $a, b \in R$, which implies that $f'(a)g'(a) = 0$ for every $a \in R$. Thus $f'g' \in N_R$, and so N_R satisfies FDP. □

Remark 4.3.17. *The function ψ defined in Corollary 4.3.16 seems natural in the sense that it sends every polynomial $g \in N_R$ to the function induced by $x + g(x)$ over $R[\alpha]$, however, we notice the following.*

1. *When $R = \mathbb{F}_q$, the function ψ is not defined. For instance, take $f(x) = x^q - x \in N_{\mathbb{F}_q}$, but $F = [f(x) + x] = [x^q] \notin St_\alpha(\mathbb{F}_q)$ since F is not a permutation as $F(0) = F(\alpha) = 0$ (compare this with Remark 4.2.13-(1)).*

2. *If $R = \mathbb{Z}_8$, the function ψ can be defined by Corollary 4.3.12. But, by Remark 4.2.13-(2), $N_{\mathbb{Z}_8}$ does not satisfy FDP. So ψ is not a homomorphism by Corollary 4.3.16.*

Applying Proposition 4.3.14 to Corollary 4.2.14 gives the following result.

Corollary 4.3.18. *Let p be a prime number and n a positive integer.*

1. *If $p > 2$, then $St_\alpha(\mathbb{Z}_{p^n}) \cong N_{\mathbb{Z}_{p^n}} / N'_{\mathbb{Z}_{p^n}}$ for every $1 < n \leq p + 1$.*

2. *If $p = 2$, then $St_\alpha(\mathbb{Z}_4) \cong N_{\mathbb{Z}_4} / N'_{\mathbb{Z}_4}$.*

We conclude the paper by showing that the null ideal on dual numbers satisfies FDP. For this we recall the following fact from [2].

Lemma 4.3.19. *[2, Theorem 3.5] Let R be a commutative ring and let $A = R[\alpha]$ be the ring of dual numbers over R. Let $f = f_1 + f_2\,\alpha$, where $f_1, f_2 \in R[x]$. Then $f \in N_A$ if and only if $f_1 \in N'_R$ and $f_2 \in N_R$.*

Proposition 4.3.20. *Let R be a commutative ring and let $A = R[\alpha]$ be the ring of dual numbers over R. Then N_A satisfies FDP.*

Proof. Let $f, g \in N_A$. Then $f = f_1 + f_2\,\alpha$ and $g = g_1 + g_2\,\alpha$ for some $f_1, f_2, g_1, g_2 \in R[x]$ such that $f_1, g_1 \in N'_R$ and $f_2, g_2 \in N_R$ by Fact 4.3.2 and Lemma 4.3.19, respectively. But then $f'_1 g'_1 \in N'_R$ and $f'_1 g'_2 + f'_2 g'_1 \in N_R$ by the definitions of N'_R and N_R. Thus, by Lemma 4.3.19,

$$f'g' = f'_1 g'_1 + (f'_1 g'_2 + f'_2 g'_1)\,\alpha \in N_A.$$

□

5 Polynomial functions over dual numbers of several variables

The content of this chapter is the submitted paper [5].

Abstract

Let k be a positive integer. For a commutative ring R, the ring of dual numbers of k variables over R is the quotient ring $R[x_1, \ldots, x_k]/I$, where I is the ideal generated by the set $\{x_i x_j \colon i, j = 1, \ldots, k\}$. This ring can be viewed as $R[\alpha_1, \ldots, \alpha_k]$ with $\alpha_i \, \alpha_j = 0$, where $\alpha_i = x_i + I$ for $i, j = 1, \ldots, k$. We investigate the polynomial functions of $R[\alpha_1, \ldots, \alpha_k]$ whenever R is a finite commutative ring. We derive counting formulas for the number of polynomial functions and polynomial permutations on $R[\alpha_1, \ldots, \alpha_k]$ depending on the order of the pointwise stabilizer of the subring of constants R in the group of polynomial permutations of $R[\alpha_1, \ldots, \alpha_k]$. Further, we show that the stabilizer group of R is independent of the number of variables k. Moreover, we prove that a function F on $R[\alpha_1, \ldots, \alpha_k]$ is a polynomial function if and only if a system of linear equations on R that depends on F has a solution.

Keywords. Finite commutative rings, dual numbers, polynomials, polynomial functions, polynomial permutations, permutation polynomials, null polynomials, finite permutation groups

5.1 Introduction

Let R be a finite commutative ring with unity. Then a function $F \colon R \longrightarrow R$ is said to be a polynomial function on R if there exists a polynomial $f \in R[x]$ such that $f(a) = F(a)$ for every $a \in R$. In this case, we say that F is the induced function of f on R and f represents (induces) F. Moreover, if F is a bijection, we say that F is a *polynomial permutation* and f is a *permutation polynomial*. If R is a finite field, it can be shown easily by using Lagrange interpolation that every function on R is a polynomial function. The situation is different when R is not a field and it is somewhat more complicated to study the properties of polynomial functions on such a ring. We denote by $\mathcal{F}(R)$ the set of polynomial functions on R, which is evidently a monoid under the composition of functions. Moreover, its subset of polynomial permutations forms a group and we denote it by $\mathcal{P}(R)$.

Kempner [43] was the first mathematician who studied polynomial functions on a finite ring which is not a field. He studied extensively the polynomial functions on $\mathbb{Z}_m$, the ring of integers modulo m. However, his arguments and results were somewhat lengthy and sophisticated. Therefore, for a long time some researchers [41, 81, 62] followed his work, obtained simpler proofs and contributed to the subject as well. Meanwhile, some others were interested in the group of polynomial permutations modulo p^n [65, 33]. Other mathematicians have generalized the concepts of polynomial functions on $\mathbb{Z}_m$ into other rings, for example, local principal ideal rings [63] and Galois rings [15]. Later, Frisch [29] characterized the polynomial functions over a more general class of local rings. Surprisingly, all rings examined in [15, 63, 43] are contained in this class.

In a recent paper [2], the authors considered the polynomial functions of the ring $R[x]/(x^2)$, the ring of dual numbers over R. In particular, they examined extensively the properties of the polynomial functions on dual numbers over the integers modulo p^n by relating them to the polynomial functions modulo p^n. However, dual numbers are not contained in the class of rings covered in [29], except for some trivial cases.

It should be mentioned that around forty years ago some mathematicians studied the properties of polynomial functions on weaker structures such as semi groups [45] and monoids [86].

The importance of studying polynomial functions emanates from their intrinsic applications in other areas. For example, permutation polynomials modulo p^n have been employed widely in computer science (see for example [83, 85]). Also, they occur as isomorphisms of combinatorial objects with vertex set $\mathbb{Z}_{p^n}$ [10, 11]. For this reason, we think that investigating the polynomial functions on new structures will give a good chance for new applications to come out.

In this paper, we are interested in the polynomial functions of the ring of dual numbers of several variables over a finite local ring R, that is, the ring $R[x_1, \ldots, x_k]/I$, where I is the ideal generated by the set $\{x_i x_j \colon i, j \in \{1, \ldots, k\}\}$, alternatively, the ring $R[\alpha_1, \ldots, \alpha_k]$ with $\alpha_i \, \alpha_j = 0$. We find that the construction of the polynomial functions on such a ring depends only on the polynomial functions on R. Furthermore, we show that the order of a subgroup of polynomial permutations on $R[\alpha_1, \ldots, \alpha_k]$ plays an essential role in the counting formulas of the polynomial functions and the polynomial permutations on $R[\alpha_1, \ldots, \alpha_k]$. More generally, we show that the properties of the polynomial functions on $R[x]/(x^2)$ discussed in [2] can be carried over to those on the ring $R[\alpha_1, \ldots, \alpha_k]$.

Here is a summary of the paper. Section 5.2 contains some basics and notations. In Section 5.3, we characterize null polynomials and permutation polynomials on $R[\alpha_1, \ldots, \alpha_k]$, and we develop the ideas needed in section 5.4. Then, in Section 5.4, we consider a group of polynomial permutations on $R[\alpha_1, \ldots, \alpha_k]$ that stabilizes (fixes) the elements of R pointwisely, and derive some counting formulas in terms of the order of this stabilizer group. Finally, we obtain necessary and sufficient conditions for polynomial functions on $R[\alpha_1, \ldots, \alpha_k]$ in section 5.5

5.2 Basics

In this section, we introduce some definitions and facts that appear in the paper frequently. Throughout this paper, let k be a positive integer, and for $f \in R[x]$ let f' denote its first formal derivative.

Definition 5.2.1. *Let S be a commutative ring, R an S-algebra and $f \in S[x]$. Then:*

1. *The polynomial f gives rise to a polynomial function on R. We use the notation $[f]_R$ for this function. We just write $[f]$ instead of $[f]_R$, when there is no confusion.*
2. *If $[f]_R$ is a permutation on R, then we call f a permutation polynomial on R.*
3. *If $g \in S[x]$ and $[f]_R = [g]_R$, this means that f and g induce the same function on R and we abbreviate this with $f \triangleq g$ on R.*

Remark 5.2.2. *Clearly, $\triangleq$ is an equivalence relation on $R[x]$. For the case when $S = R$, there is a bijective correspondence between the equivalence classes of $\triangleq$ and the polynomial functions on R. In particular, if R is finite, then the number of different polynomial functions on R equals the number of equivalence classes of $\triangleq$ on $R[x]$.*

Definition 5.2.3. *For a commutative ring R, the ring of dual numbers of k variables over R is the quotient ring $R[x_1, \ldots, x_k]/I$, where I is the ideal generated by the set $\{x_i x_j \colon i, j \in \{1, \ldots, k\}\}$; that is, the ring*

$$R[\alpha_1, \ldots, \alpha_k] = \{r_0 + \sum_{i=1}^{k} r_i \alpha_i \colon r_0, r_i \in R, \text{ with } \alpha_i \alpha_j = 0 \text{ for } i, j = 1, \ldots, k\};$$

where α_i stands for $x + I$, for $i = 1, \ldots, k$.

Remark 5.2.4. *Note that R is canonically embedded as a subring in $R[\alpha_1, \ldots, \alpha_k]$. Furthermore, $R[\alpha_1, \ldots, \alpha_k]$ is an R-algebra with basis $\{1, \alpha_1, \ldots, \alpha_k\}$.*

The following proposition summarizes some properties of $R[\alpha_1, \ldots, \alpha_k]$, which is straightforward from Definition 5.2.3.

Proposition 5.2.5. *Let R be a commutative ring. Then the following hold.*

1. *For $a_0, \ldots, a_k, b_0, \ldots, b_k \in R$, we have:*

   a) $(a_0 + \sum_{i=1}^{k} a_i \alpha_i)(b_0 + \sum_{i=1}^{k} b_i \alpha_i) = a_0 b_0 + \sum_{i=1}^{k} (a_0 b_i + b_0 a_i) \alpha_i$;

   b) $a_0 + \sum_{i=1}^{k} a_i \alpha_i$ *is a unit in* $R[\alpha_1, \ldots, \alpha_k]$ *if and only if* a_0 *is a unit in* R. *In this case,* $(a_0 + \sum_{i=1}^{k} a_i \alpha_i)^{-1} = a_0^{-1} - \sum_{i=1}^{k} a_0^{-2} a_i \alpha_i$.

2. *$R[\alpha_1, \ldots, \alpha_k]$ is a local ring if and only if R is a local ring.*

3. *If R is a local ring with a maximal ideal $\mathfrak{m}$ of nilpotency n, then $R[\alpha_1, \ldots, \alpha_k]$ is a local ring whose maximal ideal $\mathfrak{m} + \sum_{i=1}^{k} \alpha_i R$ has nilpotency $n+1$.*

We use the following lemma frequently.

Lemma 5.2.6. *Let R be a commutative ring and $a_0, \ldots, a_k \in R$.*

1. *If $f \in R[x]$, then*
$$f(a_0 + \sum_{i=1}^{k} a_i \alpha_i) = f(a_0) + \sum_{i=1}^{k} a_i f'(a_0)\, \alpha_i \,.$$

2. *If $f \in R[\alpha_1, \ldots, \alpha_k][x]$, then there exist unique $f_0, \ldots, f_k \in R[x]$ such that*
$$f = f_0 + \sum_{i=1}^{k} f_i\, \alpha_i \;\; \textit{and} \; f(a_0 + \sum_{i=1}^{k} a_i\, \alpha_i) = f_0(a_0) + \sum_{i=1}^{k} (a_i f_0'(a_0) + f_i(a_0))\, \alpha_i \,.$$

Proof. (1) Follows from Taylor expansion and the fact that $\alpha_i \alpha_j = 0$ for $i, j = 1, \ldots, k$.
(2) Let $f \in R[\alpha_1, \ldots, \alpha_k][x]$. Then $f(x) = \sum_{j=0}^{n} (c_{0\,j} + \sum_{i=1}^{k} c_{i\,j}\, \alpha_i) x^j$, where $c_{i\,j} \in R$ for $i = 0, \ldots, k$; $j = 0, \ldots, n$. So set $f_i = \sum_{j=0}^{n} c_{i\,j} x^j \in R[x]$ for $i = 0, \ldots, k$. Hence $f = f_0 + \sum_{i=1}^{k} f_i\, \alpha_i$. Evidently, the polynomials $f_0, \ldots, f_k$ are unique since $R[\alpha_1, \ldots, \alpha_k]$ is an R-algebra with basis $\{1, \alpha_1, \ldots, \alpha_k\}$. The other part follows from (1). □

The above lemma yields a necessary conditions for a function $F\colon R[\alpha_1, \ldots, \alpha_k] \longrightarrow R[\alpha_1, \ldots, \alpha_k]$ to be a polynomial function.

Corollary 5.2.7. *Let $F\colon R[\alpha_1, \ldots, \alpha_k] \longrightarrow R[\alpha_1, \ldots, \alpha_k]$ be a polynomial function. Let $a_i, b_i, c_i, d_i \in R, i = 0, \ldots, k$, such that*
$$F(a_0 + \sum_{i=1}^{k} a_i\, \alpha_i) = c_0 + \sum_{i=1}^{k} c_i\, \alpha_i, \quad \textit{and} \quad F(b_0 + \sum_{i=1}^{k} b_i\, \alpha_i) = d_0 + \sum_{i=1}^{k} d_i\, \alpha_i \,.$$
Then:

1. *$a_0 = b_0$ implies that $c_0 = d_0$;*

2. *$a_0 = b_0$ and $a_i = b_i$ for some $i \neq 0$ imply that $c_0 = d_0$ and $c_i = d_i$.*

Definition 5.2.8. *[29]. Let R be a finite commutative local ring with a maximal ideal $\mathfrak{m}$ and $L \in \mathbb{N}$ minimal with $\mathfrak{m}^L = (0)$. We call R suitable, if for all $a, b \in R$ and all $l \in \mathbb{N}$, $ab \in \mathfrak{m}^l \Rightarrow a \in \mathfrak{m}^i$ and $b \in \mathfrak{m}^j$ with $i + j \geq min(L, l)$.*

The following proposition shows that $R[\alpha_1, \ldots, \alpha_k]$ is not in the class of rings covered in [29] unless R is a finite field.

Proposition 5.2.9. *Let R be a finite local ring. Then $R[\alpha_1, \ldots, \alpha_k]$ is suitable if and only if R is a finite field.*

Proof. Since R is a local ring with a maximal ideal $\mathfrak{m}$ and nilpotency n, $R[\alpha_1, \ldots, \alpha_k]$ is a local ring with maximal ideal $\mathfrak{m}_1 = \mathfrak{m} + \sum_{i=1}^{k} \alpha_i R$ and nilpotency $L = n + 1$ by Proposition 5.2.5. Now if R is a field, the result follows easily since $\mathfrak{m}_1^2 = (0)$. If R is not a field, we notice that $L = n + 1 > 2$, then $\alpha_1 \in \mathfrak{m}_1$ and $\alpha_1 \notin \mathfrak{m}_1^j$ for $j > 1$, but $\alpha_1^2 = 0 \in \mathfrak{m}_1^{n+1}$. Hence $R[\alpha_1, \ldots, \alpha_k]$ is not suitable, when R is not a field. □

5.3 Polynomial functions and permutation polynomials on $R[\alpha_1, \ldots, \alpha_k]$

From now on, let R be a finite commutative ring with unity. A polynomial $f \in R[x]$ is called a null polynomial on R if f induces the zero function; in this case we write $f \triangleq 0$ on R. In this section, we determine when a given polynomial is a null polynomial on $R[\alpha_1, \ldots, \alpha_k]$, and whether two polynomials induce the same function on $R[\alpha_1, \ldots, \alpha_k]$. Then we apply these results to obtain a counting formula, for the number of polynomial functions on $R[\alpha_1, \ldots, \alpha_k]$, depending on the indices of the ideals N_R, N'_R in $R[x]$ (defined below). Later, we dedicate the last part of this section to the group of polynomial permutations on $R[\alpha_1, \ldots, \alpha_k]$, characterize permutation polynomials and provide supplementary results about this group.

Definition 5.3.1. *We define N_R, N'_R as:*

1. $N_R = \{f \in R[x] \colon f \triangleq 0 \text{ on } R\}$;
2. $N'_R = \{f \in R[x] \colon f \triangleq 0 \text{ and } f' \triangleq 0 \text{ on } R\}$.

Remark 5.3.2. *It is evident that N_R and N'_R are ideals of $R[x]$ with $N'_R \subseteq N_R$.*

Lemma 5.3.3. *Let $f \in R[x]$. Then:*

1. *f is a null polynomial on $R[\alpha_1, \ldots, \alpha_k]$ if and only if $f \in N'_R$;*
2. *$f\,\alpha_i$ is a null polynomial on $R[\alpha_1, \ldots, \alpha_k]$ for every $1 \leq i \leq k$ if and only if $f \in N_R$.*

Proof. (1) By Lemma 5.2.6, for every $a_0, \ldots, a_k \in R$, $f(a_0 + \sum_{i=1}^{k} a_i\,\alpha_i) = f(a_0) + \sum_{i=1}^{k} a_i f'(a_0)\,\alpha_i$. Thus the fact that f is a null polynomial on $R[\alpha_1, \ldots, \alpha_k]$ is equivalent to

$$f(a_0 + \sum_{i=1}^{k} a_i\,\alpha_i) = f(a_0) + \sum_{i=1}^{k} a_i f'(a_0)\,\alpha_i = 0 \text{ for all } a_0, \ldots, a_k \in R.$$

But this is equivalent to $f(a_0) = 0$ and $a_i f'(a_0) = 0$ for all $a_0, a_i \in R$ and $i = 1, \ldots, k$, which implies that $f(a_0) = 0$ and $f'(a_0) = 0$ for all $a_0 \in R$. Hence f and f' are null polynomials on R, which means that $f \in N'_R$.
(2) Follows immediately from Lemma 5.2.6. □

Theorem 5.3.4. *Let $f \in R[\alpha_1, \ldots, \alpha_k][x]$. We write $f = f_0 + \sum_{i=1}^{k} f_i \, \alpha_i$, where $f_0, \ldots, f_k \in R[x]$. Then f is a null polynomial on $R[\alpha_1, \ldots, \alpha_k]$ if and only if $f_0 \in N'_R$ and $f_i \in N_R$ for $i = 1, \ldots, k$.*

Proof. By Lemma 5.2.6, $f(a_0 + \sum_{i=1}^{k} a_i \, \alpha_i) = f_0(a_0) + \sum_{i=1}^{k} (a_i f'_0(a_0) + f_i(a_0)) \, \alpha_i$ for all $a_0, \ldots, a_k \in R$. This immediately implies the "if" direction. To see the "only if", suppose that f is a null polynomial on $R[\alpha_1, \ldots, \alpha_k]$. Then

$$f_0(a_0) + \sum_{i=1}^{k} (a_i f'_0(a_0) + f_i(a_0)) \, \alpha_i = 0 \text{ for all } a_0, \ldots, a_k \in R.$$

Clearly, f_0 is a null polynomial on R. Substituting first 0, then 1, for a_i, $i = 1, \ldots, k$, we find that f_i and f'_0 are null polynomials on R. Therefore $f_0 \in N'_R$ and $f_i \in N_R$ for $i = 1, \ldots, k$. □

Combining Lemma 5.3.3 with Theorem 5.3.4 gives the following criterion.

Corollary 5.3.5. *Let $f = f_0 + \sum_{i=1}^{k} f_i \, \alpha_i$, where $f_0, \ldots, f_k \in R[x]$. Then f is a null polynomial on $R[\alpha_1, \ldots, \alpha_k]$ if and only if f_0 and $f_i \, \alpha_i$ are null polynomials on $R[\alpha_1, \ldots, \alpha_k]$ for $i = 1, \ldots, k$.*

Theorem 5.3.4 implies the following corollary, which determines whether two polynomials $f, g \in R[\alpha_1, \ldots, \alpha_k][x]$ induce the same function on $R[\alpha_1, \ldots, \alpha_k]$.

Corollary 5.3.6. *Let $f = f_0 + \sum_{i=1}^{k} f_i \, \alpha_i$ and $g = g_0 + \sum_{i=1}^{k} g_i \, \alpha_i$, where $f_0, \ldots, f_k, g_0, \ldots, g_k \in R[x]$. Then $f \triangleq g$ on $R[\alpha_1, \ldots, \alpha_k]$ if and only if the following conditions hold:*

1. *$[f_i]_R = [g_i]_R$ for $i = 0, \ldots, k$;*
2. *$[f'_0]_R = [g'_0]_R$.*

In other words, $f \triangleq g$ on $R[\alpha_1, \ldots, \alpha_k]$ if and only if the following congruences hold:

1. *$f_i \equiv g_i \mod N_R$ for $i = 1, \ldots, k$;*
2. *$f_0 \equiv g_0 \mod N'_R$.*

Proof. It is sufficient to consider the polynomial $h = f - g$ and notice that $f \triangleq g$ on $R[\alpha_1, \ldots, \alpha_k]$ if and only if $h \triangleq 0$ on $R[\alpha_1, \ldots, \alpha_k]$. □

Recall that $\mathcal{F}(R[\alpha_1, \ldots, \alpha_k])$ denotes the set of polynomial functions on $R[\alpha_1, \ldots, \alpha_k]$. In the following proposition, we derive a counting formula for $\mathcal{F}(R[\alpha_1, \ldots, \alpha_k])$ depending on the indices of the ideals N_R, N'_R.

Proposition 5.3.7. *The number of polynomial functions on $R[\alpha_1, \ldots, \alpha_k]$ is given by*

$$|\mathcal{F}(R[\alpha_1, \ldots, \alpha_k])| = \big[R[x]\colon N'_R\big]\big[R[x]\colon N_R\big]^k.$$

Moreover, $[R[x]\colon N'_R]$ is the number of pairs of functions (F, E) with $F\colon R \longrightarrow R$, $G\colon R \longrightarrow R$, arising as $([f]_R, [f']_R)$ for some $f \in R[x]$, and $[R[x]\colon N_R]$ is the number of polynomial functions on R.

Proof. Let $f = f_0 + \sum_{i=1}^{k} f_i\,\alpha_i$ and $g = g_0 + \sum_{i=1}^{k} g_i\,\alpha_i$ where $f_0, \ldots, f_k, g_0, \ldots, g_k \in R[x]$. Then by Corollary 5.3.6, $f \triangleq g$ on $R[\alpha_1, \ldots, \alpha_k]$ if and only if $f_0 \equiv g_0 \mod N'_R$ and $f_i \equiv g_i \mod N_R$ for $i = 1, \ldots, k$.

Define $\varphi\colon \bigtimes_{i=0}^{k} R[x] \longrightarrow \mathcal{F}(R[\alpha_1, \ldots, \alpha_k])$ by $\varphi(f_0, \ldots, f_k) = [f]$, where $[f]$ is the function induced on $R[\alpha_1, \ldots, \alpha_k]$ by $f = f_0 + \sum_{i=1}^{k} f_i\,\alpha_i$. Then φ is a group epimorphism with $\ker\varphi = N'_R \times \bigtimes_{i=1}^{k} N_R$ by Theorem 5.3.4. Hence

$$|\mathcal{F}(R[\alpha_1, \ldots, \alpha_k])| = [\bigtimes_{i=0}^{k} R[x]\colon N'_R \times \bigtimes_{i=1}^{k} N_R] = [R[x]\colon N'_R][R[x]\colon N_R]^k.$$

Next, we set

$$\mathcal{A} = \{(F, E) \in \mathcal{F}(R) \times \mathcal{F}(R)\colon \exists f \in R[x] \text{ such that } f, f' \text{ induce } F, E \text{ respectively}\}.$$

Define $\psi\colon R[x] \longrightarrow \mathcal{A}$ by $\psi(f) = ([f]_R, [f']_R)$. It is a routine verification to show that ψ is a group epimorphism with $\ker\psi = N'_R$. Hence by the First Isomorphism Theorem of groups, we get $[R[x]\colon N'_R] = |\mathcal{A}|$. A similar argument proves that $|\mathcal{F}(R)| = [R[x]\colon N_R]$. □

The following proposition gives an upper bound for the degree of a representative of a polynomial function on $R[\alpha_1, \ldots, \alpha_k]$.

Proposition 5.3.8. *Let $h_1 \in R[\alpha_1, \ldots, \alpha_k][x]$ and $h_2 \in R[x]$ be monic null polynomials on $R[\alpha_1, \ldots, \alpha_k]$ and R, respectively, such that $\deg h_1 = d_1$ and $\deg h_2 = d_2$. Then every polynomial function $F\colon R[\alpha_1, \ldots, \alpha_k] \longrightarrow R[\alpha_1, \ldots, \alpha_k]$ is induced by a polynomial $f = f_0 + \sum_{i=1}^{k} f_i\,\alpha_i$, where $f_0, \ldots, f_k \in R[x]$ such that $\deg f_0 < d_1$ and $\deg f_i < d_2$ for $i = 1, \ldots, k$. Moreover, if F is induced by a polynomial $f \in R[x]$ and $h_1 \in R[x]$ (rather than in $R[\alpha_1, \ldots, \alpha_k][x]$), then 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. Suppose that $h_1 \in R[\alpha_1, \ldots, \alpha_k][x]$ is a monic null polynomial on $R[\alpha_1, \ldots, \alpha_k]$ of degree d_1. Let $g \in R[\alpha_1, \ldots, \alpha_k][x]$ be a polynomial that represents F. By the division algorithm, we have $g(x) = q(x)h_1(x) + r(x)$ for some $r, q \in R[\alpha_1, \ldots, \alpha_k][x]$, where $\deg r \leq d_1 - 1$. Then

clearly, $r(x)$ represents F. By Lemma 5.2.6, $r = f_0 + \sum_{i=1}^{k} r_i\,\alpha_i$ for some $f_0, r_1, \ldots, r_k \in R[x]$, and it is obvious that $\deg f_0, \deg r_i \leq d_1 - 1$ for $i = 1, \ldots, k$. Now let $h_2 \in R[x]$ be a monic null polynomial on R of degree d_2. Again, by the division algorithm, we have for $i = 1, \ldots, k$, $r_i(x) = q_i(x)h_2(x) + f_i(x)$ for some $f_i, q_i \in R[x]$, where $\deg f_i \leq d_2 - 1$. Then by Corollary 5.3.6, $r_i\,\alpha_i \triangleq f_i\,\alpha_i$ on $R[\alpha_1, \ldots, \alpha_k]$. Thus $f = f_0 + \sum_{i=1}^{k} f_i\,\alpha_i$ is the desired polynomial.
For the second part, the existence of $g \in R[x]$ with $\deg g < d_1$ such that $f \triangleq g$ on $R[\alpha_1, \ldots, \alpha_k]$ follows by the same argument given in the previous part. By Corollary 5.3.6, $[g]_R = [f]_R$ and $[g']_R = [f']_R$. □

Remark 5.3.9. *Let $h(x) = \prod_{r \in R} (x - r)^2$. Then h is a monic polynomial in $R[x]$, and by Lemma 5.3.3, it is a null polynomial on $R[\alpha_1, \ldots, \alpha_k]$. This shows that the polynomial mentioned in the last part of Proposition 5.3.8 always exists.*

We devote the rest of this section to the group of polynomial permutations on $R[\alpha_1, \ldots, \alpha_k]$.

Theorem 5.3.10. *Let R be a finite ring. Let $f = f_0 + \sum_{i=1}^{k} f_i\,\alpha_i$, where $f_0, \ldots, f_k \in R[x]$. Then f is a permutation polynomial on $R[\alpha_1, \ldots, \alpha_k]$ if and only if the following conditions hold:*

1. *f_0 is a permutation polynomial on R;*
2. *for all $a \in R$, $f_0'(a)$ is a unit in R.*

Proof. ($\Rightarrow$) Let $c \in R$. Then $c \in R[\alpha_1, \ldots, \alpha_k]$. Since f is a permutation polynomial on $R[\alpha_1, \ldots, \alpha_k]$, there exist $a_0, \ldots, a_k \in R$ such that $f(a_0 + \sum_{i=1}^{k} a_i\,\alpha_i) = c$. Thus, by Lemma 5.2.6,

$$f_0(a_0) + \sum_{i=1}^{k} (a_i f_0'(a_0) + f_i(a_0))\,\alpha_i = c.$$

So $f_0(a_0) = c$, therefore f_0 is onto, and hence a permutation polynomial on R.

Let $a \in R$ and suppose that $f_0'(a)$ is a non-unit in R. Then $f_0'(a)$ is a zerodivisor of R. Let $b \in R$, $b \neq 0$, such that $bf_0'(a) = 0$. Then, by Lemma 5.2.6,

$$f(a + \sum_{i=1}^{k} b\,\alpha_i) = f_0(a) + \sum_{i=1}^{k} (bf_0'(a) + f_i(a))\,\alpha_i = f_0(a) + \sum_{i=1}^{k} f_i(a)\,\alpha_i = f(a).$$

So f is not one-to-one, which is a contradiction. This proves (2).
($\Leftarrow$) It is enough to show that f is one-to-one. Let $a_0, \ldots, a_k, b_0, \ldots, b_k \in R$ such that

$$f(a_0 + \sum_{i=1}^{k} a_i\,\alpha_i) = f(b_0 + \sum_{i=1}^{k} b_i\,\alpha_i),$$

that is,

$$f_0(a_0) + \sum_{i=1}^{k} (a_i f_0'(a_0) + f_i(a_0))\,\alpha_i = f_0(b_0) + \sum_{i=1}^{k} (b_i f_0'(b_0) + f_i(b_0))\,\alpha_i$$

by Lemma 5.2.6. Then we have $f_0(a_0) = f_0(b_0)$ and $a_i f_0'(a_0) + f_i(a_0) = b_i f_0'(b_0) + f_i(b_0)$ for $i = 1, \ldots, k$. Hence $a_0 = b_0$ since f_0 is a permutation polynomial on R. Then, since $f_0'(a_0)$ is a unit in R, $a_i = b_i$ follows for $i = 1, \ldots, k$. □

Theorem 5.3.10 shows that the criterion to be a permutation polynomial on $R[\alpha_1, \ldots, \alpha_k]$ depends only on f_0, and implies the following corollary.

Corollary 5.3.11. *Let $f = f_0 + \sum_{i=1}^{k} f_i\,\alpha_i$, where $f_0, \ldots, f_k \in R[x]$. Then the following statements are equivalent:*

1. *f is a permutation polynomial on $R[\alpha_1, \ldots, \alpha_k]$;*
2. *$f_0 + f_i\,\alpha_i$ is a permutation polynomial on $R[\alpha_i]$ for every $i \in \{1, \ldots, k\}$;*
3. *f_0 is a permutation polynomial on $R[\alpha_1, \ldots, \alpha_k]$;*
4. *f_0 is a permutation polynomial on $R[\alpha_i]$ for every $i \in \{1, \ldots, k\}$.*

Recall that, for any finite commutative ring A, $\mathcal{P}(A)$ denotes the group of polynomial permutations on A.

Corollary 5.3.12. *The group $\mathcal{P}(R[\alpha_i])$ is embedded in $\mathcal{P}(R[\alpha_1, \ldots, \alpha_k])$ for every $i = 1, \ldots, k$.*

Proof. Fix $i \in \{1, \ldots, k\}$ and let $F \in \mathcal{P}(R[\alpha_i])$. Then F is induced by $f = f_0 + f_i\,\alpha_i$ for some $f_0, f_i \in R[x]$. Furthermore, $f_0 + f_i\,\alpha_i$ is permutation polynomial on $R[\alpha_1, \ldots, \alpha_k]$ by Corollary 5.3.11. Define a function $\psi\colon \mathcal{P}(R[\alpha_i]) \longrightarrow \mathcal{P}(R[\alpha_1, \ldots, \alpha_k])$ by $\psi(F) = [f]_{R[\alpha_1,\ldots,\alpha_k]}$, where $[f]_{R[\alpha_1,\ldots,\alpha_k]}$ denotes the function induced by f on $R[\alpha_1, \ldots, \alpha_k]$. By Corollary 5.3.6, ψ is well defined and one-to-one. Now if $F_1 \in \mathcal{P}(R[\alpha_i])$ is induced by $g \in R[\alpha_i][x]$, then $f \circ g$ induces $F \circ F_1$ on $R[\alpha_i]$. Hence,

$$\begin{aligned}
\psi(F \circ F_1) &= [f \circ g]_{R[\alpha_1,\ldots,\alpha_k]} \\
&= [f]_{R[\alpha_1,\ldots,\alpha_k]} \circ [g]_{R[\alpha_1,\ldots,\alpha_k]} \text{ since } f, g \in R[\alpha_1, \ldots, \alpha_k][x] \\
&= \psi(F) \circ \psi(F_1).
\end{aligned}$$

This completes the proof. □

Remark 5.3.13. *We will show in Proposition 5.3.16 that the condition on the derivative in Theorem 5.3.10 is redundant, when R is a direct sum of local rings none of which is a field.*

Lemma 5.3.14. *[63, Theorem 3] Let R be a finite local ring with a maximal ideal $M \neq \{0\}$ and suppose that $f \in R[x]$. 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 5.3.15. *Let R be a finite ring and suppose that $R = \oplus_{i=1}^{n} R_i$, where R_i is local for $i = 1, \ldots, n$. Let $f = (f_1, \ldots, f_n) \in R[x]$, where $f_i \in R_i[x]$. Then f is a permutation polynomial on R if and only if f_i is a permutation polynomial on R_i for $i = 1, \ldots, n$.*

Proof. ($\Rightarrow$) Suppose that f is a permutation polynomial on R and fix an i. Let $b_i \in R_i$. Then $(0, \ldots, b_i, \ldots, 0) \in R$. Thus there exists $a = (a_1, \ldots, a_i, \ldots, a_n) \in R$, where $a_j \in R_j$, $j = 1, \ldots, n$ such that $f(a) = (f_1(a_1), \ldots, f_i(a_i), \ldots, f_n(a_n)) = (0, \ldots, b_i, \ldots, 0)$. Hence $f_i(a_i) = b_i$, and therefore f_i is surjective, whence f_i is a permutation polynomial on R_i.

($\Leftarrow$) Easy and left to the reader. □

From now on, let $R^\times$ denote the group of units of R.

Proposition 5.3.16. *Let R be a finite ring which is a direct sum of local rings which are not fields, and let $f = f_0 + \sum_{i=1}^{k} f_i \alpha_i$, where $f_0, \ldots, f_k \in R[x]$. Then f is a permutation polynomial on $R[\alpha_1, \ldots, \alpha_k]$ if and only if f_0 is a permutation polynomial on R.*

Proof. ($\Rightarrow$) Follows by Theorem 5.3.10.

($\Leftarrow$) Assume that f_0 is a permutation polynomial on R. By Theorem 5.3.10, we need only show that $f_0'(r) \in R^\times$ for every $r \in R$. Write $f_0 = (g_1, \ldots, g_n)$, where $g_i \in R_i[x]$ for $i = 1, \ldots, n$. Then g_i is a permutation polynomial on R_i for $i = 1, \ldots, n$ by Lemma 5.3.15. Now let $r \in R$, so $r = (r_1, \ldots, r_n)$, where $r_i \in R_i$. Hence $f_0'(r) = (g_1'(r_1), \ldots, g_n'(r_n))$ but $g_i'(r_i) \in R_i^\times$ by Lemma 5.3.14 for $i = 1, \ldots, n$. Therefore $f_0'(r) = (g_1'(r_1), \ldots, g_n'(r_n)) \in R^\times$, i.e, $f_0'(r)$ is a unit in R for every $r \in R$. Thus f_0 satisfies the conditions of Theorem 5.3.10. Therefore f is a permutation polynomial on $R[\alpha_1, \ldots, \alpha_k]$. □

Corollary 5.3.17. *Let R be a finite ring which is a direct sum of local rings which are not fields. Let $f \in R[x]$ be a permutation polynomial on $R[\alpha_1, \ldots, \alpha_k]$. Then $f + h$ is a permutation polynomial on $R[\alpha_1, \ldots, \alpha_k]$ for every $h \in N_R$. In particular, $x + h$ is a permutation polynomial on $R[\alpha_1, \ldots, \alpha_k]$ for every $h \in N_R$.*

Recall that $\mathcal{P}(R[\alpha_1, \ldots, \alpha_k])$ denotes the group of permutation polynomials on $R[\alpha_1, \ldots, \alpha_k]$.

Proposition 5.3.18. *Let R be a finite ring. Let B denote the number of pairs of functions (H, G) with*

$$H \colon R \longrightarrow R \text{ bijective and } G \colon R \longrightarrow R^\times$$

that occur as $([g], [g'])$ for some $g \in R[x]$. Then the number of polynomial permutations on $R[\alpha_1, \ldots, \alpha_k]$ is given by

$$|\mathcal{P}(R[\alpha_1, \ldots, \alpha_k])| = B \cdot |\mathcal{F}(R)|^k.$$

Proof. Let $F \in \mathcal{P}(R[\alpha_1, \ldots, \alpha_k])$. Then by definition F is induced by a polynomial f, where by Lemma 5.2.6 $f = f_0 + \sum_{i=1}^{k} f_i \, \alpha_i$ for $f_0, \ldots, f_k \in R[x]$. By Theorem 5.3.10,

$$[f_0] \colon R \longrightarrow R \text{ bijective, } [f_0'] \colon R \longrightarrow R^\times \text{ and } [f_i] \text{ is arbitrary in } \mathcal{F}(R) \text{ for } i = 1, \ldots, k.$$

The rest follows by Corollary 5.3.6. □

In the next section, we show that the number B of Proposition 5.3.18 depends on the order of a subgroup of $\mathcal{P}(R[\alpha_1, \ldots, \alpha_k])$, which fixes every element of R. However, when R is a finite field, we can find explicitly this number. For this, we need the following well known lemma.

Lemma 5.3.19. *Let $\mathbb{F}_q$ be a finite field with q elements. Then for all functions*

$$F, G \colon \mathbb{F}_q \longrightarrow \mathbb{F}_q,$$

there exists $f \in \mathbb{F}_q[x]$ such that

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

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

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

Thus $[f] = [f_0] = F$ and $[f'] = [f_1] = G$ since $(x^q - x)$ is a null polynomial on $\mathbb{F}_q$. Moreover, since $(x^q - x)$ is a null polynomial on $\mathbb{F}_q$, we can choose f_0, f_1 such that $\deg f_0, \deg f_1 < q$. Hence $\deg f < 2q$. □

Proposition 5.3.20. *Let $\mathbb{F}_q$ be a finite field with q elements. The number of polynomial permutations on $\mathbb{F}_q[\alpha_1, \ldots, \alpha_k]$ is given by*

$$|\mathcal{P}(\mathbb{F}_q[\alpha_1, \ldots, \alpha_k])| = q!(q-1)^q q^{kq}.$$

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

$$F \colon \mathbb{F}_q \longrightarrow \mathbb{F}_q \text{ bijective and } G \colon \mathbb{F}_q \longrightarrow \mathbb{F}_q \setminus \{0\}.$$

By Lemma 5.3.19, each $(F, G) \in \mathcal{B}$ arises as $([f], [f'])$ for some $f \in \mathbb{F}_q[x]$. Thus by Proposition 5.3.18, $|\mathcal{P}(\mathbb{F}_q[\alpha_1, \ldots, \alpha_k])| = |\mathcal{B}| \cdot |\mathcal{F}(\mathbb{F}_q)|^k$. Clearly $|\mathcal{B}| = q!(q-1)^q$ and $|\mathcal{F}(\mathbb{F}_q)|^k = q^{kq}$. □

5.4 The stabilizer of R in the group of polynomial permutations of $R[\alpha_1, \ldots, \alpha_k]$

The main object of this section is to describe the order of the subgroup of polynomial permutations on $R[\alpha_1, \ldots, \alpha_k]$ that fixes pointwise each element of R, and then to use this order to find a counting formula for the number of polynomial permutations on $R[\alpha_1, \ldots, \alpha_k]$.

Definition 5.4.1. *Let* $St_{\alpha_1,\ldots,\alpha_k}(R) = \{F \in \mathcal{P}(R[\alpha_1, \ldots, \alpha_k])\colon F(a) = a \text{ for every } a \in R\}$.

Evidently, $St_{\alpha_1,\ldots,\alpha_k}(R)$ is a subgroup of $\mathcal{P}(R[\alpha_1, \ldots, \alpha_k])$ that stabilizes each element of R pointwisely.

Lemma 5.4.2. *Let* $f, g \in R[x]$ *with* $f \triangleq g$ *on* R. *There exists* $h \in N_R$ *such that* $f = g + h$.

Proof. Let $h = f - g$. Then h has the desired property. □

Proposition 5.4.3. *Let* R *be a finite ring. Then*

$$St_{\alpha_1,\ldots,\alpha_k}(R) = \{F \in \mathcal{P}(R[\alpha_1, \ldots, \alpha_k])\colon F \text{ is induced by } x + h(x), h \in N_R\}.$$

Proof. It is obvious that

$$St_{\alpha_1,\ldots,\alpha_k}(R) \supseteq \{F \in \mathcal{P}(R[\alpha_1, \ldots, \alpha_k])\colon F \text{ is induced by } x + h(x), h \in N_R\}.$$

For the other inclusion, let $F \in \mathcal{P}(R[\alpha_1, \ldots, \alpha_k])$ such that $F(a) = a$ for every $a \in R$. Then F is represented by $f_0 + \sum_{i=1}^{k} f_i\,\alpha_i$, where $f_0, \ldots, f_k \in R[x]$, and $a = F(a) = f_0(a) + \sum_{i=1}^{k} f_i(a)\,\alpha_i$ for every $a \in R$. It follows that $f_i(a) = 0$ for every $a \in R$, i.e., f_i is a null polynomial on R for $i = 1, \ldots, k$. Thus $f_0 + \sum_{i=1}^{k} f_i\,\alpha_i \triangleq f_0$ on $R[\alpha_1, \ldots, \alpha_k]$ by Corollary 5.3.6, that is, F is represented by f_0. Also, $f_0 \triangleq id_R$ on R, where id_R is the identity function on R, and therefore $f_0(x) = x + h(x)$ for some $h \in N_R$ by Lemma 5.4.2. □

We have the following theorem, when R is a finite field, which describes the order of $St_{\alpha_1,\ldots,\alpha_k}(\mathbb{F}_q)$. The proof is almost the same as in [2, Theorem 4.11].

Theorem 5.4.4. *Let* $\mathbb{F}_q$ *be a finite field with* q *elements. Then:*

1. $|St_{\alpha_1,\ldots,\alpha_k}(\mathbb{F}_q)| = |\{[f']_{\mathbb{F}_q}\colon f \in N_{\mathbb{F}_q} \text{ and for every } a \in \mathbb{F}_q, f'(a) \neq -1\}|$;
2. $|St_{\alpha_1,\ldots,\alpha_k}(\mathbb{F}_q)| = |\{[f']_{\mathbb{F}_q}\colon f \in N_{\mathbb{F}_q}, \deg f < 2q \text{ and for every } a \in \mathbb{F}_q, f'(a) \neq -1\}|$;
3. $|St_{\alpha_1,\ldots,\alpha_k}(\mathbb{F}_q)| = (q-1)^q$.

Proof. We begin with the proof of (1) and (2). Set

$$A = \{[f']_{\mathbb{F}_q} \colon f \in N_{\mathbb{F}_q} \text{ and for every } a \in \mathbb{F}_q, f'(a) \neq -1\}.$$

We define a bijection φ from $St_{\alpha_1,\ldots,\alpha_k}(\mathbb{F}_q)$ to the set A. If $F \in St_{\alpha_1,\ldots,\alpha_k}(\mathbb{F}_q)$, then it is represented by $x + h(x)$, where $h \in \mathbb{F}_q[x]$ is a null polynomial on $\mathbb{F}_q$, by Proposition 5.4.3. Now $h'(a) \neq -1$ for every $a \in \mathbb{F}_q$, by Theorem 5.3.10, whence $[h']_{\mathbb{F}_q} \in A$. Now, set $\varphi(F) = [h']_{\mathbb{F}_q}$. Then Corollary 5.3.6 shows that φ is well-defined and injective. To show φ is surjective, let $[h']_{\mathbb{F}_q} \in A$, where $h \in N_{\mathbb{F}_q}$. Then, by Theorem 5.3.10 and Proposition 5.4.3, $F = [x + h]_{\mathbb{F}_q[\alpha_1,\ldots,\alpha_k]} \in St_{\alpha_1,\ldots,\alpha_k}(\mathbb{F}_q)$. Thus $\varphi(F) = [h']_{\mathbb{F}_q}$. Moreover, by Lemma 5.3.19, h can be chosen such that $\deg h < 2q$.

Next, we prove (3). By (1),

$$|St_{\alpha_1,\ldots,\alpha_k}(\mathbb{F}_q)| \leq |\{G \colon \mathbb{F}_q \longrightarrow \mathbb{F}_q \setminus \{-1\}\}| = (q-1)^q.$$

Now for every function $G \colon \mathbb{F}_q \longrightarrow \mathbb{F}_q \setminus \{-1\}$ there exists a polynomial $f \in N_{\mathbb{F}_q}$ such that $[f']_{\mathbb{F}_q} = G$ by Lemma 5.3.19. Thus $f(x) + x$ is a permutation polynomial on $\mathbb{F}_q[\alpha_1, \ldots, \alpha_k]$ by Theorem 5.3.10. Obviously, $x + f(x)$ induces the identity on $\mathbb{F}_q$, and hence $[x + f(x)]_{\mathbb{F}_q[\alpha_1,\ldots,\alpha_k]} \in St_{\alpha_1,\ldots,\alpha_k}(\mathbb{F}_q)$. Therefore every element of the set $\{G \colon \mathbb{F}_q \longrightarrow \mathbb{F}_q \setminus \{-1\}\}$ corresponds to an element of $St_{\alpha_1,\ldots,\alpha_k}(\mathbb{F}_q)$, from which we conclude that $|St_{\alpha_1,\ldots,\alpha_k}(\mathbb{F}_q)| \geq (q-1)^q$. This completes the proof. □

Notation 5.4.5. *Let*

$$\mathcal{P}_R(R[\alpha_1, \ldots, \alpha_k]) = \{F \in \mathcal{P}(R[\alpha_1, \ldots, \alpha_k]) \colon F = [f]_{R[\alpha_1,\ldots,\alpha_k]} \text{ for some } f \in R[x]\}.$$

In similar manner, let $\mathcal{P}_R(R[\alpha_i]) = \{F \in \mathcal{P}(R[\alpha_i]) \colon F = [f]_{R[\alpha_i]} \text{ for some } f \in R[x]\}$.

We now show that $\mathcal{P}_R(R[\alpha_1, \ldots, \alpha_k])$ is a subgroup of $\mathcal{P}(R[\alpha_1, \ldots, \alpha_k])$.

Proposition 5.4.6. *The set* $\mathcal{P}_R(R[\alpha_1, \ldots, \alpha_k])$ *is a subgroup of* $\mathcal{P}(R[\alpha_1, \ldots, \alpha_k])$ *and* $\mathcal{P}_R(R[\alpha_1, \ldots, \alpha_k]) \cong \mathcal{P}_R(R[\alpha_i])$ *for* $i = 1, \ldots, k$.

Proof. It is clear that $\mathcal{P}_R(R[\alpha_1, \ldots, \alpha_k])$ is closed under composition. Since it is finite, it is a subgroup of $\mathcal{P}(R[\alpha_1, \ldots, \alpha_k])$. Let $F \in \mathcal{P}_R(R[\alpha_1, \ldots, \alpha_k])$ and suppose that F is induced by $f \in R[x]$. Define

$$\psi \colon \mathcal{P}_R(R[\alpha_1, \ldots, \alpha_k]) \longrightarrow \mathcal{P}_R(R[\alpha_i]), \quad F \mapsto [f]_{R[\alpha_i]}.$$

Then ψ is well defined by Corollary 5.3.6, and evidently it is a homomorphism. By Corollary 5.3.11, ψ is surjective. To show that ψ is one-to-one, let $F_1 \in \mathcal{P}_R(R[\alpha_1, \ldots, \alpha_k])$ be induced by $g \in R[x]$ with $F \neq F_1$. Then either $f \not\triangleq g$ on R or $f' \not\triangleq g'$ on R by Corollary 5.3.6. Thus $\psi(F) = [f]_{R[\alpha_i]} \neq \psi(F_1) = [g]_{R[\alpha_i]}$. □

We will see that $St_{\alpha_1,\ldots,\alpha_k}(R)$ is a normal subgroup of $\mathcal{P}_R(R[\alpha_1, \ldots, \alpha_k])$. But first we prove the following fact.

Proposition 5.4.7. *Let R be a finite ring. Then for every $F \in \mathcal{P}(R)$ there exists a polynomial $f \in R[x]$ such that F is induced by f and $f'(r) \in R^\times$ for every $r \in R$.*

Proof. Set $\mathcal{P}_u(R) = \{F \in \mathcal{P}(R) \colon F \text{ is induced by } f \in R[x], f' \colon R \longrightarrow R^\times\}$. By definition $\mathcal{P}_u(R) \subseteq \mathcal{P}(R)$. Let $F \in \mathcal{P}(R)$. Then F is induced by $f \in R[x]$. Since R is finite, $R = \oplus_{i=1}^n R_i$, where R_i are local rings. We distinguish two cases. For the first case, we suppose that every R_i is not a field. Then f is a permutation polynomial on $R[\alpha_1, \ldots, \alpha_k]$ by Proposition 5.3.16. Hence $f'(a) \in R^\times$ for every $a \in R$ by Theorem 5.3.10. So $F \in \mathcal{P}_u(R)$. For the second case, we assume without loss of generality that $R_1, \ldots, R_r$ are fields and none of $R_{r+1}, \ldots, R_n$ is a field for some $r \geq 1$. Then write $f = (f_1, \ldots, f_n)$ where $f_i \in R_i$ for $i = 1, \ldots, n$. By Lemma 5.3.15, f_i is a permutation polynomial on R_i, for $i = 1, \ldots, n$. Now a similar argument like the one given in the first case shows that $f_i'(a_i) \in R_i^\times$ for every $a_i \in R_i$ for $i = r+1, \ldots, n$. On the other hand, there exists $g_j \in R_j[x]$ such that $g_j \triangleq f_j$ on R_j and $g_j'(a_j) \in R_j^\times$ for every $a_j \in R_j$, $j = 1, \ldots, r$ by Lemma 5.3.19. Then take $g = (g_1, \ldots, g_r, f_{r+1}, \ldots, f_n)$. Thus $g \triangleq f$ on R and $g'(r) \in R^\times$ for every $r \in R$. Therefore g induces F and $F \in \mathcal{P}_u(R)$. □

Proposition 5.4.8. *Let R be a finite ring. Then:*

1. *every element of $\mathcal{P}(R)$ occurs as the restriction to R of some $F \in \mathcal{P}_R(R[\alpha_1, \ldots, \alpha_k])$;*
2. *$\mathcal{P}_R(R[\alpha_1, \ldots, \alpha_k])$ contains $St_{\alpha_1,\ldots,\alpha_k}(R)$ as a normal subgroup and*

$$\mathcal{P}_R(R[\alpha_1, \ldots, \alpha_k]) \big/ St_{\alpha_1,\ldots,\alpha_k}(R) \cong \mathcal{P}(R).$$

Proof. (1) This is obvious from Proposition 5.4.7.

(2) $St_{\alpha_1,\ldots,\alpha_k}(R)$ is contained in $\mathcal{P}_R(R[\alpha_1, \ldots, \alpha_k])$, because every element of $St_{\alpha_1,\ldots,\alpha_k}(R)$ can be represented by a polynomial with coefficients in R by Proposition 5.4.3. Let $F \in \mathcal{P}_R(R[\alpha_1, \ldots, \alpha_k])$ be represented by $f \in R[x]$. Then define $\varphi \colon \mathcal{P}_R(R[\alpha_1, \ldots, \alpha_k]) \longrightarrow \mathcal{P}(R)$ by $\varphi(F) = [f]_R$. Now φ is well defined by Corollary 5.3.6, and it is a group homomorphism with $\ker \varphi = St_{\alpha_1,\ldots,\alpha_k}(R)$. By Proposition 5.4.7, φ is surjective. □

Corollary 5.4.9. *For any fixed $F \in \mathcal{P}(R)$,*

$$|St_{\alpha_1,\ldots,\alpha_k}(R)| = \left|\{([f]_R, [f']_R) \colon f \in R[x], [f] \in \mathcal{P}_R(R[\alpha_1, \ldots, \alpha_k]) \text{ and } [f]_R = F\}\right|.$$

Proof. Let $f \in R[x]$ be a permutation polynomial on $R[\alpha_1, \ldots, \alpha_k]$ with $[f]_R = F$. Such an f exists by Lemma 5.4.8 (1). We denote by $[f]$ the permutation induced by f on $R[\alpha_1, \ldots, \alpha_k]$. Then the coset of $[f]$ with respect to $St_{\alpha_1,\ldots,\alpha_k}(R)$ has $|St_{\alpha_1,\ldots,\alpha_k}(R)|$ elements. By Lemma 5.4.8 (2), this coset consists of all polynomial permutations $G \in \mathcal{P}_R(R[\alpha_1, \ldots, \alpha_k])$ with $[f]_R = G\big|_R$, where $G\big|_R$ is the restriction of the function G to R. Let $g \in R[x]$ with $[g] = G$. By Corollary 5.3.6, $G \neq [f]$ if and only if the pair $([f]_R, [f']_R)$ does not equal the pair $([g]_R, [g']_R)$. Thus we have a bijection between the coset of $[f]$ with respect to $St_{\alpha_1,\ldots,\alpha_k}(R)$ and the set

of pairs $([g]_R, [g']_R)$ occurring for $g \in R[x]$ such that $[g] = G$ permutes $R[\alpha_1, \ldots, \alpha_k]$ and $[f]_R = [g]_R$. □

When R is a finite ring which is a direct sum of local rings that are not fields, Corollary 5.4.9 is a special case of a general result (see Proposition 5.4.14).

We now employ Corollary 5.4.9 to find the number of permutation polynomials on $R[\alpha_1, \ldots, \alpha_k]$ in terms of $|St_{\alpha_1,\ldots,\alpha_k}(R)|$ in the following theorem.

Theorem 5.4.10. *Let R be a finite ring. For any integer $k \geq 1$,*

$$|\mathcal{P}(R[\alpha_1, \ldots, \alpha_k])| = |\mathcal{F}(R)|^k \cdot |\mathcal{P}(R)| \cdot |St_{\alpha_1,\ldots,\alpha_k}(R)|.$$

Proof. For $f \in R[x]$, let $[f]$ be the function induced by f on $R[\alpha_1, \ldots, \alpha_k]$.

Set $B = \bigcup_{F \in \mathcal{P}(R)} \{([f]_R, [f']_R) \colon f \in R[x], [f] \in \mathcal{P}_R(R[\alpha_1, \ldots, \alpha_k]) \text{ and } [f]_R = F\}$.
Then $|B| = |\mathcal{P}(R)| \cdot |St_{\alpha_1,\ldots,\alpha_k}(R)|$ by Corollary 5.4.9.

Now we define a function $\Psi \colon \mathcal{P}(R[\alpha_1, \ldots, \alpha_k]) \longrightarrow B \times \bigtimes_{i=1}^{k} \mathcal{F}(R)$ as follows: if $G \in \mathcal{P}(R[\alpha_1, \ldots, \alpha_k])$ is induced by $g = g_0 + \sum_{i=1}^{k} g_i \alpha_i$, where $g_0, \ldots, g_k \in R[x]$, we let $\Psi(G) = (([g_0]_R, [g_0']_R), [g_1]_R, \ldots, [g_k]_R)$. By Theorem 5.3.10 and Corollary 5.3.6, Ψ is well-defined and one-to-one. The surjectivity of Ψ follows by Proposition 5.4.8 and Theorem 5.3.10. Therefore

$$|\mathcal{P}(R[\alpha_1, \ldots, \alpha_k])| = |B \times \bigtimes_{i=1}^{k} \mathcal{F}(R)| = |\mathcal{P}(R)| \cdot |St_{\alpha_1,\ldots,\alpha_k}(R)| \cdot |\mathcal{F}(R)|^k.$$

□

Definition 5.4.11. *Let $N_R(< n) = \{f \in R[x] \colon f \in N_R \text{ with } \deg f < n\}$, and*

$$N_R'(< n) = \{f \in R[x] \colon f \in N_R' \text{ with } \deg f < n\}.$$

In the following theorem, we obtain several descriptions for the order of the group $St_{\alpha_1,\ldots,\alpha_k}(R)$ whenever R is a direct sum of local rings which are not fields.

Theorem 5.4.12. *Let R be a finite ring which is a direct sum of local rings that are not fields. Then the following hold.*

1. $|St_{\alpha_1,\ldots,\alpha_k}(R)| = |\{[f']_R \colon f \in N_R\}|$.
2. *Let $h \in R[x]$ be a monic polynomial null polynomial on $R[\alpha_1, \ldots, \alpha_k]$ of degree n. Then:*
   a) $|St_{\alpha_1,\ldots,\alpha_k}(R)| = |\{[f']_R \colon f \in N_R \text{ with } \deg f < n\}|$;
   b) $|St_{\alpha_1,\ldots,\alpha_k}(R)| = [N_R \colon N_R'] = \frac{|N_R(<n)|}{|N_R'(<n)|}$.

Proof. (1) We define a bijection φ from $St_{\alpha_1,\dots,\alpha_k}(R)$ to the set of different functions induced on R by the first derivative of the null polynomials on R. By Proposition 5.4.3, every $F \in St_{\alpha_1,\dots,\alpha_k}(R)$ is represented by $x+f(x)$, where $f \in R[x]$ is a null polynomial on R. We set $\varphi(F) = [f']_R$. Then Corollary 5.3.6 shows that φ is well-defined and injective, and Corollary 5.3.17 shows that it is surjective.
(2) Such a null polynomial $h \in R[x]$ exists by Remark 5.3.9.

(2a) If $g \in N_R$, then by Proposition 5.3.8, there exists $f \in R[x]$ with $\deg f < n$ such that $[f]_R = [g]_R$ and $[f']_R = [g']_R$. Evidently, $f \in N_R$.

(2b) For the index, define $\varphi\colon N_R \longrightarrow \mathcal{F}(R)$ by $\varphi(f) = [f']_R$. Clearly, φ is a homomorphism of additive groups. Furthermore,

$$\ker\varphi = N_R' \text{ and } \operatorname{Im}\varphi = \{[f']_R\colon f \in N_R\},$$

and hence ${}^{N_R}\!/_{N_R'} \cong \{[f']_R\colon f \in N_R\}$. Therefore $|St_{\alpha_1,\dots,\alpha_k}(R)| = [N_R\colon N_R']$ by (1).
For the ratio, consider the sets $N_R(<n)$ and $N_R'(<n)$ as defined in Definition 5.4.11. The equivalence relation in Definition 5.2.1 restricted to these two additive subgroups and the analogous proof to the previous part show that

$$|St_{\alpha_1,\dots,\alpha_k}(R)| = [N_R(<n)\colon N_R'(<n)].$$

□

Remark 5.4.13.

1. *When $R = \mathbb{F}_q$ is a finite field, we have shown in Theorem 5.4.4 (3) that $|St_{\alpha_1,\dots,\alpha_k}(\mathbb{F}_q)| = (q-1)!$. But we will see later that*

$$[N_{\mathbb{F}_q}\colon N_{\mathbb{F}_q}'] = [N_{\mathbb{F}_q}(<2q)\colon N_{\mathbb{F}_q}'(<2q)] = q^q.$$

2. *When $k = 1$, Theorem 5.4.12 is still a generalization of [2, Proposition 7.2].*

Proposition 5.4.14. *Let R be a finite ring which is a direct sum of local rings that are not fields. Then for any fixed $F \in \mathcal{F}(R)$,*

$$|St_{\alpha_1,\dots,\alpha_k}(R)| = |\{([g]_R, [g']_R)\colon g \in R[x] \text{ with } [g]_R = F\}|.$$

Proof. Set

$$A = \{([g]_R, [g']_R)\colon g \in R[x] \text{ with } [g]_R = F\},$$

and fix $g_0 \in R[x]$ with $[g_0]_R = F$. Then $g - g_0$ is a null polynomial on R for any $g \in R[x]$ with $([g]_R, [g']_R) \in A$.

We define a bijection

$$\phi\colon A \longrightarrow \{[f']_R\colon f \in N_R\}, \quad \phi(([g]_R, [g']_R)) = [(g-g_0)']_R.$$

Since $[(g-g_0)']_R = [g']_R - [g_0']_R$, ϕ is well defined. Further, ϕ is injective, because, for two distinct elements of A, $([g_1]_R, [g_1']_R) \neq ([g]_R, [g']_R)$ implies $[g_1']_R \neq [g']_R$ and hence $[(g_1-g_0)']_R \neq [(g-g_0)']_R$.

Now, consider $[f']_R$, where $f \in N_R$. Then $[g_0+f]_R = F$ and, thus, $([g_0+f]_R, [g_0'+f']_R)$ is in A and $\phi([g_0+f]_R, [g_0'+f']_R) = [f']_R$. Therefore ϕ is surjective.

By Theorem 5.4.12 (1),

$$|St_{\alpha_1,\ldots,\alpha_k}(R)| = |\{[h']_R \colon h \in N_R\}| = |A|.$$

□

The following theorem shows that the stabilizer group $St_{\alpha_1,\ldots,\alpha_k}(R)$ does not depend on the number of variables k.

Theorem 5.4.15. *Let R be a finite ring and let k be a positive integer. Then $St_{\alpha_1,\ldots,\alpha_k}(R) \cong St_{\alpha_i}(R)$ for $i = 1, \ldots, k$.*

Proof. Fix $i \in \{1, \ldots, k\}$. Then by the definition of dual numbers (for the case $k = 1$), $R[\alpha_1] \cong R[\alpha_i]$. Let $F \in \mathcal{P}_R(R[\alpha_1, \ldots, \alpha_k])$ and suppose that F is induced by $f \in R[x]$. Define

$$\psi \colon \mathcal{P}_R(R[\alpha_1, \ldots, \alpha_k]) \longrightarrow \mathcal{P}_R(R[\alpha_i]), \quad F \mapsto [f]_{R[\alpha_i]}.$$

The proof of Proposition 5.4.6 shows that ψ is an isomorphism. If ϕ denotes the restriction of ψ to $St_{\alpha_1,\ldots,\alpha_k}(R)$, then $St_{\alpha_1,\ldots,\alpha_k}(R) \cong \phi(St_{\alpha_1,\ldots,\alpha_k}(R))$. Therefore, we need only show that $\phi(St_{\alpha_1,\ldots,\alpha_k}(R)) = St_{\alpha_i}(R)$. Let $G \in St_{\alpha_i}(R)$. Then G is induced by $x + h(x)$ for some $h \in N_R$ by Proposition 5.4.3 (with $k = 1$). By Corollary 5.3.11 and Proposition 5.4.3, $F = [x + h(x)]_{R[\alpha_1,\ldots,\alpha_k]} \in St_{\alpha_1,\ldots,\alpha_k}(R)$. But then $\phi(F) = \psi(F) = [x + h(x)]_{R[\alpha_i]} = G$, hence $G \in \phi(St_{\alpha_1,\ldots,\alpha_k}(R))$. This shows that $St_{\alpha_i}(R) \subseteq \phi(St_{\alpha_1,\ldots,\alpha_k}(R))$. The other inclusion is similar. □

Lemma 5.4.16. *Let R be a finite ring. Then $[R[x] \colon N_R'] = [R[x] \colon N_R][N_R \colon N_R']$.*

Proof. It is clear that $R[x]$ is an additive abelian group with subgroups N_R, N_R' such that $N_R' < N_R$. Then by the Second Isomorphism Theorem of groups,

$$(R[x]/N_R') \,/\, (\, N_R/N_R') \cong (R[x]/N_R),$$

from which the result follows. □

Theorem 5.4.17. *Let R be a finite ring. Then*

$$|\mathcal{F}(R[\alpha_1, \ldots, \alpha_k])| = [N_R \colon N_R']|\mathcal{F}(R)|^{k+1}.$$

Moreover, when R is a direct sum of local rings which are not fields, we have

$$|\mathcal{F}(R[\alpha_1, \ldots, \alpha_k])| = |St_{\alpha_1,\ldots,\alpha_k}(R)| \cdot |\mathcal{F}(R)|^{k+1}.$$

Proof. We have,

$$\begin{aligned}|\mathcal{F}(R[\alpha_1,\ldots,\alpha_k])| &= [R[x]\colon N'_R]|\mathcal{F}(R)|^k \text{ (By Proposition 5.3.7)}\\ &= [N_R\colon N'_R]|\mathcal{F}(R)|^{k+1} \text{ (By Lemma 5.4.16).}\end{aligned}$$

The second part follows from the above and Theorem 5.4.12 (2b). □

We turn now to find explicitly the number of polynomial functions on $\mathbb{F}_q[\alpha_1,\ldots,\alpha_k]$. To do this, we need the following lemma, and we leave its proof to the reader.

Lemma 5.4.18. *Let $\mathbb{F}_q$ be a finite field. Then:*

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

Proposition 5.4.19. *Let $\mathbb{F}_q$ be a finite field. Then $|\mathcal{F}(\mathbb{F}_q[\alpha_1,\ldots,\alpha_k])| = q^{(k+2)q}$.*

Proof. Set

$$\mathcal{A} = \{f\colon f = f_0 + \sum_{i=1}^{k} f_i\,\alpha_i, \text{ where } f_0, f_i \in \mathbb{F}_q[x], \deg f_0 < 2q, \deg f_i < q \text{ for } i = 1,\ldots,k\}.$$

Then it is clear that $|\mathcal{A}| = q^{(k+2)q}$. To complete the proof, we show that if $f, g \in \mathcal{A}$ with $f \neq g$, then $[f] \neq [g]$, or equivalently if $[f] = [g]$, then $f = g$. Suppose that $f, g \in \mathcal{A}$, where $f_0 + \sum_{i=1}^{k} f_i\,\alpha_i$ and $g_0 + \sum_{i=1}^{k} g_i\,\alpha_i$, such that $[f] = [g]$. Thus $[f-g]$ is the zero function on $\mathbb{F}_q[\alpha_1,\ldots,\alpha_k]$. Hence $f - g = (f_0 - g_0) + \sum_{i=1}^{k}(f_i - g_i)\,\alpha_i$ is a null polynomial on $\mathbb{F}_q[\alpha_1,\ldots,\alpha_k]$, whence $f_0 - g_0 \in N'_{\mathbb{F}_q}$ and $f_i - g_i \in N_{\mathbb{F}_q}$ for $i = 1,\ldots,k$ by Theorem 5.3.4. Then, by Lemma 5.4.18, we have $(x^q - x)^2 \mid (f_0 - g_0)$ and $(x^q - x) \mid (f_i - g_i)$ for $i = 1,\ldots,k$. Therefore $f_0 - g_0 = 0$, $f_i - g_i = 0$ for $i = 1,\ldots,k$ since $\deg(f_0 - g_0) < 2q$ and $\deg(f_i - g_i) < q$ for $i = 1,\ldots,k$. Thus $f = g$. □

The following corollary shows that, when $R = \mathbb{F}_q$, $[N_{\mathbb{F}_q}\colon N'_{\mathbb{F}_q}] \neq |St_{\alpha_1,\ldots,\alpha_k}(\mathbb{F}_q)|$(see Theorem 5.4.4 and Theorem 5.4.12).

Corollary 5.4.20. *Let $\mathbb{F}_q$ be a finite field. Then $[N_{\mathbb{F}_q}\colon N'_{\mathbb{F}_q}] = [N_{\mathbb{F}_q}(<2q)\colon N'_{\mathbb{F}_q}(<2q)] = q^q$.*

Proof. By Theorem 5.4.17, $|\mathcal{F}(\mathbb{F}_q[\alpha_1,\ldots,\alpha_k])| = [N_{\mathbb{F}_q}\colon N'_{\mathbb{F}_q}]|\mathcal{F}(\mathbb{F}_q)|^{k+1}$, whence $[N_{\mathbb{F}_q}\colon N'_{\mathbb{F}_q}] = q^q$ by Proposition 5.4.19. On the other hand, Lemma 5.4.18 gives $|N_{\mathbb{F}_q}(<2q)| = q^q$ and $|N'_{\mathbb{F}_q}(<2q)| = 1$. Thus

$$[N_{\mathbb{F}_q}(<2q)\colon N'_{\mathbb{F}_q}(<2q)] = \frac{|N_{\mathbb{F}_q}(<2q)|}{|N'_{\mathbb{F}_q}(<2q)|} = q^q.$$

□

5.5 Necessary and sufficient conditions

In this section, we prove the following theorem that determines whether a given function on $R[\alpha_1, \ldots, \alpha_k]$ is a polynomial function, and give an algorithm to find a polynomial representation of a polynomial function by solving only a linear system of equations over R.

Being motivated by [20, Theorem 5], we prove the following theorem.

Theorem 5.5.1. *Let R be a finite commutative ring with n elements, and let d_1, d_2 be as in Proposition 5.3.8. Let $F\colon R[\alpha_1, \ldots, \alpha_k] \longrightarrow R[\alpha_1, \ldots, \alpha_k]$ be a function and, for $0 \leq i \leq k$, $b_i\colon R^{k+1} \longrightarrow R$ the functions such that*

$$F(r_0 + \sum_{i=1}^{k} r_i\alpha_i) = b_0(r_0, \ldots, r_k) + \sum_{i=1}^{k} b_i(r_0, \ldots, r_k)\alpha_i,$$

for all $(r_0, \ldots, r_k) \in R^{k+1}$. Then the following statements are equivalent:

1. *F is a polynomial function on $R[\alpha_1, \ldots, \alpha_k]$;*

2. *F can be represented by a polynomial of degree $\leq d_1 - 1$;*

3. *F can be represented by a polynomial*

$$f(x) = f_0(x) + \sum_{i=1}^{k} f_i(x)\alpha_i,$$

where $f_0(x) = \sum_{l=0}^{d_1-1} a_{0\,l}x^l$, $f_i(x) = \sum_{m=0}^{d_2-1} a_{i\,m}x^m$ with $a_{0\,l}, a_{i\,m} \in R$ for $l = 0, \ldots, d_1 - 1$, $i = 1, \ldots, k$, $m = 0, \ldots, d_2 - 1$;

4. *The system of linear equations, where r_j varies through all elements of R for $j = 0, 1, \ldots, k$,*

$$\begin{aligned} \sum_{l=0}^{d_1-1} y_{0\,l}r_0^l &= b_0(r_0, \ldots, r_k) \\ \sum_{l=1}^{d_1-1} (l y_{0\,l}r_0^{l-1})r_i + \sum_{m=0}^{d_2-1} y_{i\,m}r_0^m &= b_i(r_0, \ldots, r_k) \text{ for } i = 1, \ldots, k \end{aligned} \tag{5.1}$$

has a solution $y_{0\,l} = a_{0\,l}, y_{i\,m} = a_{i\,m}$ with $a_{0\,l}, a_{i\,m} \in R$ for $l = 0, \ldots, d_1 - 1$; $i = 1, \ldots, k$; $m = 0, \ldots, d_2 - 1$.

Proof. It is clear that (3) $\Rightarrow$ (2) $\Rightarrow$ (1). The implication (1) $\Rightarrow$ (3) follows by Proposition 5.3.8. To prove (3) $\Rightarrow$ (4), suppose that F can be represented by a polynomial $f \in R[\alpha_1, \ldots, \alpha_k][x]$, where $f = f_0 + \sum_{i=1}^{k} f_i\alpha_i$, such that $f_0(x) = \sum_{l=0}^{d_1-1} a_{0\,l}x^l, f_i(x) = \sum_{m=0}^{d_2-1} a_{i\,m}x^m$, where $f_0, f_i \in R[x]$

for $i = 1, \ldots, k$. So, for $r_0, \ldots, r_k \in R$, we have since F is induced by f,

$$\begin{aligned} F(r_0 + \sum_{i=1}^{k} r_i\,\alpha_i) &= f(r_0 + \sum_{i=1}^{k} r_i\,\alpha_i) = f_0(r_0) + \sum_{i=1}^{k}(r_i f_0'(r_0) + f_i(r_0))\,\alpha_i \text{ (by Lemma 5.2.6)} \\ &= \sum_{l=0}^{d_1-1} a_{0\,l} r_0^l + \sum_{i=1}^{k}(\sum_{l=1}^{d_1-1} r_i(l a_{0\,l} r_0^{l-1}) + \sum_{m=0}^{d_2-1} a_{i\,m} r_0^m)\alpha_i \\ &= b_0(r_0, \ldots, r_k) + \sum_{i=1}^{k} b_i(r_0, \ldots, r_k)\,\alpha_i \text{ (by the definition of } F). \end{aligned}$$

Therefore,

$$\begin{aligned} \sum_{l=0}^{d_1-1} a_{0\,l} r_0^l &= b_0(r_0, \ldots, r_k) \\ \sum_{l=1}^{d_1-1} (l a_{0\,l} r_0^{l-1}) r_i + \sum_{m=0}^{d_2-1} a_{i\,m} r_0^m &= b_i(r_0, \ldots, r_k) \text{ for } i = 1, \ldots, k. \end{aligned}$$

Hence, since each r_j varies through all the elements of R, the system of linear equations (5.1) has a solution $y_{0\,l} = a_{0\,l}$, $y_{i\,m} = a_{i\,m}$, for $l = 0, \ldots, d_1 - 1$; $m = 0, \ldots, d_2 - 1$; $i = 1, \ldots, k$.

Finally, we can prove (4) $\Rightarrow$ (3) by reversing the previous steps. □

Remark 5.5.2. *Keep the notation of Theorem 5.5.1.*

1. *For an element $r_0 + \sum_{i=1}^{k} r_i\alpha_i$, there are exactly $k + 1$ equations in the system of linear equations (5.1) corresponding to this element.*

2. *In view of the necessary conditions of Corollary 5.2.7, we expect to get repetitions of equations in the system (5.1). For example, let us consider the elements $r_0 + \sum_{i=1}^{k} r_i\alpha_i$ and $r_0 + \sum_{i=1}^{k} c_i\alpha_i$ of $R[\alpha_1, \ldots, \alpha_k]$ with $c_i \neq r_i$ for some $i \geq 1$. Then, for a polynomial function F, it is necessary that $b_0(r_0, r_1, \ldots, r_k) = b_0(r_0, c_1, \ldots, c_k)$. Because, otherwise, the system (5.1) will contain the following equations*

$$\begin{aligned} \sum_{l=0}^{d_1-1} y_{0\,l} r_0^l &= b_0(r_0, r_1, \ldots, r_k) \\ \sum_{l=0}^{d_1-1} y_{0\,l} r_0^l &= b_0(r_0, c_1, \ldots, c_k), \end{aligned}$$

which implies that the system (5.1) has no solution.

Bibliography

[1] Elsayed Ahmed and Dmytro Savchuk. "Endomorphisms of regular rooted trees induced by the action of polynomials on the ring $\mathbb{Z}_d$ of d-adic integers". In: *J. Algebra Appl.* 19.8 (2020), pp. 2050154, 20. ISSN: 0219-4988. DOI: 10.1142/S0219498820501546. URL: https://doi.org/10.1142/S0219498820501546.

[2] Hasan Al-Ezeh, Amr A. Al-Maktry, and Sophie Frisch. "Polynomial functions on rings of dual numbers over residue class rings of the integers". To appear in Mathematica Slovaca. Arxiv: https://arxiv.org/abs/1910.00238v3. Appears in this thesis as Chapter 2.

[3] Amr A. Al-Maktry. "On a property of the ideals of the polynomial ring $R[x]$". To appear in the International Electronic Journal of Algebra. Appears in this thesis as Chapter 4.

[4] Amr A. Al-Maktry. "On the group of unit-valued polynomial functions". In: *Appl. Algebra Engrg. Comm. Comput.* (2021). Appears in this thesis as Chapter 3. DOI: 10.1007/s00200-021-00510-x. URL: https://doi.org/10.1007/s00200-021-00510-x.

[5] Amr A. Al-Maktry. "Polynomial functions over dual numbers of several variables". Submitted. Arxiv: https://arxiv.org/abs/2002.01304v1. Appears in this thesis as Chapter 5.

[6] Vladimir Anashin. "Ergodic transformations in the space of p-adic integers". In: *p-adic mathematical physics*. Vol. 826. AIP Conf. Proc. Amer. Inst. Phys., Melville, NY, 2006, pp. 3–24. DOI: 10.1063/1.2193107. URL: https://doi.org/10.1063/1.2193107.

[7] Daniel A. Ashlock. "Compositional attractors and enumeration of permutation polynomials over finite fields". In: *J. Pure Appl. Algebra* 81.1 (1992), pp. 1–9. ISSN: 0022-4049. DOI: 10.1016/0022-4049(92)90130-8. URL: https://doi.org/10.1016/0022-4049(92)90130-8.

[8] Daniel A. Ashlock. “Permutation polynomials of abelian group rings over finite fields”. In: *J. Pure Appl. Algebra* 86.1 (1993), pp. 1–5. ISSN: 0022-4049. DOI: 10.1016/0022-4049(93)90148-M. URL: https://doi.org/10.1016/0022-4049(93)90148-M.

[9] Ayman Badawi. “On Φ-pseudo-valuation rings. II”. In: *Houston J. Math.* 26.3 (2000), pp. 473–480. ISSN: 0362-1588.

[10] Neal Brand. “Isomorphisms of cyclic combinatorial objects”. In: *Discrete Math.* 78.1-2 (1989), pp. 73–81. ISSN: 0012-365X. DOI: 10.1016/0012-365X(89)90162-3. URL: https://doi.org/10.1016/0012-365X(89)90162-3.

[11] Neal Brand. “Polynomial isomorphisms of combinatorial objects”. In: *Graphs Combin.* 7.1 (1991), pp. 7–14. ISSN: 0911-0119. DOI: 10.1007/BF01789458. URL: https://doi.org/10.1007/BF01789458.

[12] Joel V. Brawley. “A note on polynomial matrix functions over a finite field”. In: *Linear Algebra Appl.* 28 (1979), pp. 35–38. ISSN: 0024-3795. DOI: 10.1016/0024-3795(79)90115-0. URL: https://doi.org/10.1016/0024-3795(79)90115-0.

[13] Joel V. Brawley. “The number of polynomial functions which permute the matrices over a finite field”. In: *J. Combinatorial Theory Ser. A* 21.2 (1976), pp. 147–154. ISSN: 0097-3165. DOI: 10.1016/0097-3165(76)90059-5. URL: https://doi.org/10.1016/0097-3165(76)90059-5.

[14] Joel V. Brawley, Leonard Carlitz, and Jack Levine. “Scalar polynomial functions on the *timesn* matrices over a finite field”. In: *Linear Algebra Appl.* 10 (1975), pp. 199–217. ISSN: 0024-3795. DOI: 10.1016/0024-3795(75)90069-5. URL: https://doi.org/10.1016/0024-3795(75)90069-5.

[15] Joel V. Brawley and Gary L. Mullen. “Functions and polynomials over Galois rings”. In: *J. Number Theory* 41.2 (1992), pp. 156–166. ISSN: 0022-314X. DOI: 10.1016/0022-314X(92)90116-7. URL: http://dx.doi.org/10.1016/0022-314X(92)90116-7.

[16] Balázs Bulyovszky and Gábor Horváth. “Polynomial functions over finite commutative rings”. In: *Theoret. Comput. Sci.* 703 (2017), pp. 76–86. ISSN: 0304-3975. DOI: 10.1016/j.tcs.2017.09.002. URL: https://doi.org/10.1016/j.tcs.2017.09.002.

[17] Leonard Carlitz. “Functions and polynomials (mod p^n)”. In: *Acta Arith.* 9 (1964), pp. 67–78. ISSN: 0065-1036. DOI: 10.4064/aa-9-1-67-78. URL: https://doi.org/10.4064/aa-9-1-67-78.

[18] Leonard Carlitz. "Some theorems on permutation polynomials". In: *Bull. Amer. Math. Soc.* 68 (1962), pp. 120–122. ISSN: 0002-9904. DOI: 10.1090/S0002-9904-1962-10750-2. URL: https://doi.org/10.1090/S0002-9904-1962-10750-2.

[19] Yasemin Cengellenmis, Abdullah Dertli, and Nuh Ayd'ı n. "Some constacyclic codes over $\mathbb{Z}_4[u]/\langle u^2\rangle$, new Gray maps, and new quaternary codes". In: *Algebra Colloq.* 25.3 (2018), pp. 369–376. ISSN: 1005-3867. DOI: 10.1142/S1005386718000263. URL: https://doi.org/10.1142/S1005386718000263.

[20] Zhibo Chen. "On polynomial functions from Z_n to Z_m". In: *Discrete Math.* 137.1-3 (1995), pp. 137–145. ISSN: 0012-365X. DOI: 10.1016/0012-365X(93)E0162-W. URL: http://dx.doi.org/10.1016/0012-365X(93)E0162-W.

[21] Zhibo Chen. "On polynomial functions from $Z_{n_1} \times Z_{n_2} \times \cdots \times Z_{n_r}$ to Z_m". In: *Discrete Math.* 162.1-3 (1996), pp. 67–76. ISSN: 0012-365X. DOI: 10.1016/0012-365X(95)00305-G. URL: https://doi.org/10.1016/0012-365X(95)00305-G.

[22] Leonard E. Dickson. *Introduction to the theory of Numbers*. The University of Chicago Press, 1929.

[23] Jian Ding and Hong-ju Li. "The Gray images of $(1 + u)$ constacyclic codes over $F_{2^m}[u]/\langle u^k\rangle$". In: *J. Appl. Math. Comput.* 49.1-2 (2015), pp. 433–445. ISSN: 1598-5865. DOI: 10.1007/s12190-014-0847-5. URL: https://doi.org/10.1007/s12190-014-0847-5.

[24] David E. Dobbs. "Every commutative ring has a minimal ring extension". In: *Comm. Algebra* 34.10 (2006), pp. 3875–3881. ISSN: 0092-7872. DOI: 10.1080/00927870600862706. URL: https://doi.org/10.1080/00927870600862706.

[25] Günther Eigenthaler. "On direct products of algebras of polynomials and polynomial functions". In: *Contributions to general algebra (Proc. Klagenfurt Conf., Klagenfurt, 1978)*. Heyn, Klagenfurt, 1979, pp. 83–96.

[26] Günther Eigenthaler and Harald Woracek. "Permutable polynomials and related topics". In: *Contributions to general algebra, 9 (Linz, 1994)*. Hölder-Pichler-Tempsky, Vienna, 1995, pp. 163–182.

[27] Aihua Fan and Lingmin Liao. "On minimal decomposition of p-adic polynomial dynamical systems". In: *Adv. Math.* 228.4 (2011), pp. 2116–2144. ISSN: 0001-8708. DOI: 10.1016/j.aim.2011.06.032. URL: https://doi.org/10.1016/j.aim.2011.06.032.

[28] Sophie Frisch. "Integrally closed domains, minimal polynomials, and null ideals of matrices". In: *Comm. Algebra* 32.5 (2004), pp. 2015–2017. ISSN: 0092-7872. DOI: 10.1081/AGB-120029919. URL: https://doi.org/10.1081/AGB-120029919.

[29] Sophie Frisch. “Polynomial functions on finite commutative rings”. In: *Advances in Commutative Ring Theory (Fez, 1997)*. Vol. 205. Lecture Notes in Pure and Appl. Math. Dekker, New York, 1999, pp. 323–336.

[30] Sophie Frisch. “Polynomial separation of points in algebras”. In: *Arithmetical properties of commutative rings and monoids*. Vol. 241. Lect. Notes Pure Appl. Math. Chapman & Hall/CRC, Boca Raton, FL, 2005, pp. 253–259. DOI: 10.1201/9781420028249.ch15. URL: https://doi.org/10.1201/9781420028249.ch15.

[31] Sophie Frisch. “When are weak permutation polynomials strong?” In: *Finite Fields Appl.* 1.4 (1995), pp. 437–439. ISSN: 1071-5797. DOI: 10.1006/ffta.1995.1034. URL: https://doi.org/10.1006/ffta.1995.1034.

[32] Sophie Frisch. “When are weak permutation polynomials strong?” In: *Finite Fields Appl.* 1.4 (1995), pp. 437–439. ISSN: 1071-5797. DOI: 10.1006/ffta.1995.1034. URL: https://doi.org/10.1006/ffta.1995.1034.

[33] Sophie Frisch and Daniel Krenn. “Sylow p-groups of polynomial permutations on the integers $\bmod p^n$”. In: *J. Number Theory* 133.12 (2013), pp. 4188–4199. ISSN: 0022-314X. DOI: 10.1016/j.jnt.2013.06.002. URL: http://dx.doi.org/10.1016/j.jnt.2013.06.002.

[34] Robert Gilmer. “R-automorphisms of $R[X]$”. In: *Proc. London Math. Soc. (3)* 18 (1968), pp. 328–336. ISSN: 0024-6115. DOI: 10.1112/plms/s3-18.2.328. URL: https://doi.org/10.1112/plms/s3-18.2.328.

[35] Robert Gilmer. “The ideal of polynomials vanishing on a commutative ring”. In: *Proc. Amer. Math. Soc.* 127.5 (1999), pp. 1265–1267. ISSN: 0002-9939. DOI: 10.1090/S0002-9939-99-04634-1. URL: https://doi.org/10.1090/S0002-9939-99-04634-1.

[36] Dalma Görcsös, Gábor Horváth, and Anett Mészáros. “Permutation polynomials over finite rings”. In: *Finite Fields Appl.* 49 (2018), pp. 198–211. ISSN: 1071-5797. DOI: 10.1016/j.ffa.2017.10.004. URL: https://doi.org/10.1016/j.ffa.2017.10.004.

[37] Ashwin Guha and Ambedkar Dukkipati. “A faster algorithm for testing polynomial representability of functions over finite integer rings”. In: *Theoret. Comput. Sci.* 579 (2015), pp. 88–99. ISSN: 0304-3975. DOI: 10.1016/j.tcs.2015.02.013. URL: https://doi.org/10.1016/j.tcs.2015.02.013.

[38] Jebrel M. Habeb, Mowaffaq Hajja, and William J. Heinzer. "Conjugacy classes and invariant subrings of R-automorphisms of $R[x]$". In: *Comm. Algebra* 40.4 (2012), pp. 1496–1524. ISSN: 0092-7872. DOI: 10.1080/00927872.2011.552082. URL: https://doi.org/10.1080/00927872.2011.552082.

[39] Godfrey H. Hardy and Edward M. Wright. *An introduction to the theory of numbers*. 3rd ed. Oxford, at the Clarendon Press, 1954, pp. xvi+419.

[40] Jian J. Jiang. "A note on polynomial functions over finite commutative rings". In: *Adv. Math. (China)* 39.5 (2010), pp. 555–560. ISSN: 1000-0917.

[41] Gordon Keller and Frank R. Olson. "Counting polynomial functions (mod p^n)". In: *Duke Math. J.* 35 (1968), pp. 835–838. ISSN: 0012-7094. URL: http://projecteuclid.org/euclid.dmj/1077377970.

[42] Aubrey J. Kempner. "Miscellanea". In: *Amer. Math. Monthly* 25.5 (1918), pp. 201–210. ISSN: 0002-9890. DOI: 10.2307/2972639. URL: https://doi.org/10.2307/2972639.

[43] Aubrey J. Kempner. "Polynomials and their residue systems". In: *Trans. Amer. Math. Soc.* 22.2 (1921), pp. 240–266, 267–288. ISSN: 0002-9947. DOI: 10.2307/1989020. URL: http://dx.doi.org/10.2307/1989020.

[44] Gerhard Kowol. "Polynomial functions over groups: from algebraically closed groups to endomorphism near-rings". In: *Contributions to general algebra. 15*. Heyn, Klagenfurt, 2004, pp. 45–62.

[45] Gerhard Kowol and Heinz Mitsch. "Polynomial functions over commutative semigroups". In: *Semigroup Forum* 12.2 (1976), pp. 109–118. ISSN: 0037-1912. DOI: 10.1007/BF02195915. URL: http://dx.doi.org/10.1007/BF02195915.

[46] Hans Kurzweil and Bernd Stellmacher. *The theory of finite groups*. Universitext. An introduction, Translated from the 1998 German original. Springer-Verlag, New York, 2004, pp. xii+387. ISBN: 0-387-40510-0. DOI: 10.1007/b97433. URL: https://doi.org/10.1007/b97433.

[47] Hans Lausch and Wilfried Nöbauer. *Algebra of polynomials*. North-Holland Mathematical Library, Vol. 5. North-Holland Publishing Co., Amsterdam-London; American Elsevier Publishing Co., Inc., New York, 1973, pp. xi+322.

[48] Francis. C. Leary. "Rings with invertible regular elements". In: *Amer. Math. Monthly* 96.10 (1989), pp. 924–926. ISSN: 0002-9890. DOI: 10.2307/2324590. URL: https://doi.org/10.2307/2324590.

[49] Kangquan Li, Longjiang Qu, and Xi Chen. "New classes of permutation binomials and permutation trinomials over finite fields". In: *Finite Fields Appl.* 43 (2017), pp. 69–85. ISSN: 1071-5797. DOI: 10.1016/j.ffa.2016.09.002. URL: https://doi.org/10.1016/j.ffa.2016.09.002.

[50] Rudolf Lidl and Harald Niederreiter. *Finite fields*. Second. Vol. 20. Encyclopedia of Mathematics and its Applications. With a foreword by P. M. Cohn. Cambridge University Press, Cambridge, 1997, pp. xiv+755. ISBN: 0-521-39231-4.

[51] Nian Ping Liu and Jian Jun Jiang. "Polynomial functions in n variables over a finite commutative ring". In: *Sichuan Daxue Xuebao* 46.1 (2009), pp. 44–46. ISSN: 0490-6756.

[52] Clas Löfwall. "The global homological dimensions of trivial extensions of rings". In: *J. Algebra* 39.1 (1976), pp. 287–307. ISSN: 0021-8693. DOI: 10.1016/0021-8693(76)90078-8. URL: https://doi.org/10.1016/0021-8693(76)90078-8.

[53] Alan K. Loper. "A note on Dedekind non-D-rings". In: *Rocky Mountain J. Math.* 23.2 (1993), pp. 671–681. ISSN: 0035-7596. DOI: 10.1216/rmjm/1181072584. URL: https://doi.org/10.1216/rmjm/1181072584.

[54] Alan K. Loper. "On Prüfer non-D-rings". In: *J. Pure Appl. Algebra* 96.3 (1994), pp. 271–278. ISSN: 0022-4049. DOI: 10.1016/0022-4049(94)90103-1. URL: https://doi.org/10.1016/0022-4049(94)90103-1.

[55] Alan K. Loper. "On rings without a certain divisibility property". In: *J. Number Theory* 28.2 (1988), pp. 132–144. ISSN: 0022-314X. DOI: 10.1016/0022-314X(88)90060-1. URL: https://doi.org/10.1016/0022-314X(88)90060-1.

[56] Carlton J. Maxson and Andries B. van der Merwe. "Functions and polynomials over finite commutative rings". In: *Aequationes Math.* 62.1-2 (2001), pp. 30–38. ISSN: 0001-9054. DOI: 10.1007/PL00000141. URL: https://doi.org/10.1007/PL00000141.

[57] Bernard R. McDonald. *Finite rings with identity*. Pure and Applied Mathematics, Vol. 28. Marcel Dekker, Inc., New York, 1974, pp. ix+429.

[58] Abdeslam Mimouni. "Note on non-D-rings". In: *Quaest. Math.* 42.6 (2019), pp. 823–830. ISSN: 1607-3606. DOI: 10.2989/16073606.2018.1498406. URL: https://doi.org/10.2989/16073606.2018.1498406.

[59] Heinz Mitsch. "Über Polynome und Polynomfunktionen auf Verbänden". In: *Monatsh. Math.* 74 (1970), pp. 239–243. ISSN: 0026-9255. DOI: 10.1007/BF01303443. URL: https://doi.org/10.1007/BF01303443.

[60] Gary L. Mullen, ed. *Handbook of finite fields*. Discrete Mathematics and its Applications (Boca Raton). CRC Press, Boca Raton, FL, 2013, pp. xxxvi+1033. ISBN: 978-1-4398-7378-6. DOI: 10.1201/b15006. URL: https://doi.org/10.1201/b15006.

[61] Gary L. Mullen and Harald Niederreiter. "The structure of a group of permutation polynomials". In: *J. Austral. Math. Soc. Ser. A* 38.2 (1985), pp. 164–170. ISSN: 0263-6115.

[62] Gary L. Mullen and Harlan Stevens. "Polynomial functions (mod m)". In: *Acta Math. Hungar.* 44.3-4 (1984), pp. 237–241. ISSN: 0236-5294. DOI: 10.1007/BF01950276. URL: http://dx.doi.org/10.1007/BF01950276.

[63] Alexander A. Nechaev. "Polynomial transformations of finite commutative local rings of principal ideals". In: *Math. Notes* 27 (1980). transl. from Mat. Zametki 27 (1980) 885-897, pp. 425–432.

[64] Wilfried Nöbauer. *Die Operation des Einsetzens bei Polynomen in mehreren Unbestimmten*. J. Reine Angew. Math., 1959, pp. 207–220.

[65] Wilfried Nöbauer. "Gruppen von Restpolynomidealrestklassen nach Primzahlpotenzen". In: *Monatsh. Math.* 59 (1955), pp. 194–202. DOI: 10.1007/BF01303794. URL: http://dx.doi.org/10.1007/BF01303794.

[66] Wilfried Nöbauer. "Gruppen von Restpolynomidealrestklassen nach Primzahlpotenzen". In: *Monatsh. Math.* 59 (1955), pp. 194–202. DOI: 10.1007/BF01303794. URL: http://dx.doi.org/10.1007/BF01303794.

[67] Wilfried Nöbauer. "Polynomfunktionen auf primen Restklassen". In: *Arch. Math. (Basel)* 39.5 (1982), pp. 431–435. ISSN: 0003-889X. DOI: 10.1007/BF01899544. URL: https://doi.org/10.1007/BF01899544.

[68] Wilfried Nöbauer. "Über die Ableitungen der Vollideale". In: *Math. Z* 75 (1960/1961), pp. 14–21. ISSN: 0025-5874. DOI: 10.1007/BF01211006. URL: https://doi.org/10.1007/BF01211006.

[69] Wilfried Nöbauer. "Über Gruppen von Restklassen nach Restpolynomidealen". In: *Österreich. Akad. Wiss. Math.-Nat. Kl. S.-B. IIa* 162 (1953), pp. 207–233. ISSN: 0029-8816.

[70] Wilfried Nöbauer. "Zur Theorie der Polynomtransformationen und Permutationspolynome". In: *Math. Ann.* 157 (1964), pp. 332–342. ISSN: 0025-5831. DOI: 10.1007/BF01360874. URL: https://doi.org/10.1007/BF01360874.

[71] Wilfried Nöbauer. "Zur Theorie der Vollideale". In: *Monatsh. Math.* 64 (1960), pp. 176–183. ISSN: 0026-9255. DOI: 10.1007/BF01890540. URL: https://doi.org/10.1007/BF01890540.

[72] Wilfried Nöbauer. "Zur Theorie der Vollideale. II". In: *Monatsh. Math.* 64 (1960), pp. 335–348. ISSN: 0026-9255. DOI: 10.1007/BF01498611. URL: https://doi.org/10.1007/BF01498611.

[73] Giulio Peruginelli and Nicholas J. Werner. "Non-triviality conditions for integer-valued polynomial rings on algebras". In: *Monatsh. Math.* 183.1 (2017), pp. 177–189. ISSN: 0026-9255. DOI: 10.1007/s00605-016-0951-8. URL: https://doi.org/10.1007/s00605-016-0951-8.

[74] Giulio Peruginelli and Nicholas J. Werner. "Properly integral polynomials over the ring of integer-valued polynomials on a matrix ring". In: *J. Algebra* 460 (2016), pp. 320–339. ISSN: 0021-8693. DOI: 10.1016/j.jalgebra.2016.04.016. URL: https://doi.org/10.1016/j.jalgebra.2016.04.016.

[75] László Rédei and Tibor Szele. "Algebraischzahlentheoretische Betrachtungen über Ringe. I". In: *Acta Math.* 79 (1947), pp. 291–320. ISSN: 0001-5962. DOI: 10.1007/BF02404701. URL: https://doi.org/10.1007/BF02404701.

[76] Roswitha Rissner. "Null ideals of matrices over residue class rings of principal ideal domains". In: *Linear Algebra Appl.* 494 (2016), pp. 44–69. ISSN: 0024-3795. DOI: 10.1016/j.laa.2016.01.004. URL: https://doi.org/10.1016/j.laa.2016.01.004.

[77] Ronald L. Rivest. "Permutation polynomials modulo 2^w". In: *Finite Fields Appl.* 7.2 (2001), pp. 287–292. ISSN: 1071-5797. DOI: 10.1006/ffta.2000.0282. URL: https://doi.org/10.1006/ffta.2000.0282.

[78] Mark W. Rogers and Cameron Wickham. "Polynomials inducing the zero function on local rings". In: *Int. Electron. J. Algebra* 22 (2017), pp. 170–186. DOI: 10.24330/ieja.325942. URL: https://doi.org/10.24330/ieja.325942.

[79] Javad Sedighi Hafshejani and Ali R. Naghipour. "Integer-valued Polynomials Over Matrix Rings of Number Fields". In: *Bull. Iran. Math. Soc.* (2020). DOI: 0.1007/s41980-020-00484-5. URL: https://doi.org/10.1007/s41980-020-00484-5.

[80] David Singmaster. "A maximal generalization of Fermat's theorem". In: *Math. Mag.* 39 (1966), pp. 103–107. ISSN: 0025-570X. DOI: 10.2307/2688723. URL: https://doi.org/10.2307/2688723.

[81] David Singmaster. "On polynomial functions (mod m)". In: *J. Number Theory* 6 (1974), pp. 345–352. ISSN: 0022-314X. DOI: 10.1016/0022-314X(74)90031-6. URL: http://dx.doi.org/10.1016/0022-314X(74)90031-6.

[82] Roxana Smarandache and Pascal O. Vontobel. "Quasi-cyclic LDPC codes: influence of proto- and Tanner-graph structure on minimum Hamming distance upper bounds". In: *IEEE Trans. Inform. Theory* 58.2 (2012), pp. 585–607. ISSN: 0018-9448. DOI: 10.1109/TIT.2011.2173244. URL: https://doi.org/10.1109/TIT.2011.2173244.

[83] Jing Sun and Oscar Y. Takeshita. "Interleavers for turbo codes using permutation polynomials over integer rings". In: *IEEE Trans. Inform. Theory* 51.1 (2005), pp. 101–119. ISSN: 0018-9448. DOI: 10.1109/TIT.2004.839478. URL: https://doi.org/10.1109/TIT.2004.839478.

[84] John A. Suvak. "Full ideals and ring groups in $Z_n[x]$". In: *Canad. Math. Bull.* 19.3 (1976), pp. 329–335. ISSN: 0008-4395. DOI: 10.4153/CMB-1976-050-6. URL: https://doi.org/10.4153/CMB-1976-050-6.

[85] Oscar Y. Takeshita. "Permutation polynomial interleavers: an algebraic-geometric perspective". In: *IEEE Trans. Inform. Theory* 53.6 (2007), pp. 2116–2132. ISSN: 0018-9448. DOI: 10.1109/TIT.2007.896870. URL: https://doi.org/10.1109/TIT.2007.896870.

[86] Robert F. Tichy. "Polynomial functions over monoids". In: *Semigroup Forum* 18.4 (1979), pp. 371–380. ISSN: 0037-1912. DOI: 10.1007/BF02574201. URL: http://dx.doi.org/10.1007/BF02574201.

[87] Da Qing Wan and Rudolf Lidl. "Permutation polynomials of the form $x^r f(x^{(q-1)/d})$ and their group structure". In: *Monatsh. Math.* 112.2 (1991), pp. 149–163. ISSN: 0026-9255. DOI: 10.1007/BF01525801. URL: https://doi.org/10.1007/BF01525801.

[88] Qi Jiao Wei and Qifan Zhang. "On permutation polynomials in two variables over $\mathbb{Z}/p^2\mathbb{Z}$". In: *Acta Math. Sin. (Engl. Ser.)* 25.7 (2009), pp. 1191–1200. ISSN: 1439-8516. DOI: 10.1007/s10114-009-6526-z. URL: https://doi.org/10.1007/s10114-009-6526-z.

[89] Qijiao Wei and Qifan Zhang. "On strong orthogonal systems and weak permutation polynomials over finite commutative rings". In: *Finite Fields Appl.* 13.1 (2007), pp. 113–120. ISSN: 1071-5797. DOI: 10.1016/j.ffa.2005.08.005. URL: https://doi.org/10.1016/j.ffa.2005.08.005.

[90] Johann Wiesenbauer. "On polynomial functions over residue class rings of **Z**". In: *Contributions to general algebra, 2 (Klagenfurt, 1982)*. Hölder-Pichler-Tempsky, Vienna, 1983, pp. 395–398.

[91] Qifan Zhang. “Polynomial functions and permutation polynomials over some finite commutative rings”. In: *J. Number Theory* 105.1 (2004), pp. 192–202. ISSN: 0022-314X. DOI: 10.1016/j.jnt.2003.09.009. URL: https://doi.org/10.1016/j.jnt.2003.09.009.