Applicable Algebra in Engineering, Communication and Computing (2023) 34:521–537
https://doi.org/10.1007/s00200-021-00510-x

ORIGINAL PAPER

On the group of unit-valued polynomial functions

Amr Ali Al-Maktry[1]

Received: 9 July 2020 / Revised: 16 January 2021 / Accepted: 10 April 2021 /
Published online: 29 May 2021

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

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 $F : R \longrightarrow R$ 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.

✉ Amr Ali Al-Maktry
almaktry@math.tugraz.at

[1] Institute of Analysis and Number Theory (5010), Technische Universität Graz, Kopernikusgasse 24/II, 8010 Graz, Austria

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 permutations 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.

2 Preliminaries

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

Definition 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 [6] 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 1 [7, 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 1 Recall that, in a finite commutative ring R with unity, every element is either a unit or a zero divisor, according to whether multiplication by the element is a bijection of R or not (see for example [5]).

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

Fact 2 *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;*

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

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 1. 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 1. $\square$

Remark 2 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 1 Let $R = \{\frac{a}{b} : a, b \in \mathbb{Z} \text{ and } 2 \nmid b\}$, 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 2 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 $R[\alpha] = \{a + b\alpha : a, b \in R, \alpha^2 = 0\}$, where α denotes the element $x + (x^2)$.

Remark 3 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 *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 4 *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 (1),

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

$\square$

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 Let $\mathcal{P}_R(R[\alpha]) = \{F \in \mathcal{P}(R[\alpha]) : F = [f]_{R[\alpha]}$ 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 4 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 5 *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, $F_1 \circ F_2 \in \mathcal{P}_R(R[\alpha])$. □

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

1. *the map $\theta_G : \mathcal{F}(R)^\times \longrightarrow \mathcal{F}(R)^\times$ 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 $\theta : \mathcal{P}(R) \longrightarrow Aut(\mathcal{F}(R)^\times)$ defined by $(G)\theta = \theta_G$ is a homomorphism with respect to composition.*

Proof Ad(1) in view of Lemma 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 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 $\theta : \mathcal{P}(R) \longrightarrow Aut(\mathcal{F}(R)^\times)$ 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. □

Notation and Remark 1 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 1 *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 $\theta : \mathcal{P}(R) \longrightarrow Aut(\mathcal{F}(R)^\times)$ be the homomorphism of Lemma 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 1 depends essentially on Lemma 2, and is just the justifications of the semidirect product properties (see for example [4]).

Remark 5 Consider the following subsets of $\mathcal{P}(R) \ltimes_\theta \mathcal{F}(R)^\times$:

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

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. For completeness' sake, we prove the following lemma, which is a special case of [1, Theorem 4.1].

Lemma 3 *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 (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 zero divisor of R. Now, if $0 \neq b \in R$ such that $bg'(a) = 0$, then by Fact 3 (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 (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. $\square$

Recall from Definition 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 6 Let $F \in \mathcal{P}_R(R[\alpha])$. Then there exists $f \in R[x]$ such that $F = [f]_{R[\alpha]}$ by Definition 3. Further, by Lemma 3, $([f]_R, [f']_R) \in \mathcal{P}(R) \ltimes_\theta \mathcal{F}(R)^\times$. Now define a map

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

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 (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 and Fact 2 the definitions of the groups $(\mathcal{P}_R(R[\alpha]), \circ)$ and $(\mathcal{F}(R)^\times, \cdot)$, namely

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

and

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

Proposition 2 *Let R be a finite commutative ring, and θ the homomorphism defined in Lemma 2. Then the map*

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

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 6, 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 4 and Proposition 1,

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

□

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 4). 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 [1].

Definition 4 Let $St_\alpha(R) = \{F \in \mathcal{P}(R[\alpha]) : F(r) = r \text{ for every } r \in R\}$.

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 [1]. We include a proof for the readers' convenience.

Proposition 3 [1, *Proposition* 4.6] *Let R be a finite commutative ring. Then*

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

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

Proof Obviously,

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

Now if $F \in St_\alpha(R)$, then by Definition 4, $F \in \mathcal{P}(R[\alpha])$ 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), $r = F(r) = h_0(r) + h_1(r)\alpha$ 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 4. 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 7 Let $\mathbb{F}_q = \{a_0, \dots, a_{q-1}\}$ be the finite field of q elements. If $F : \mathbb{F}_q \longrightarrow \mathbb{F}_q$, 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 $\mathbb{F}_q^\times = \mathbb{F}_q \setminus \{0\}$. 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 4 *For each pair of functions (G, F) with*

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

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 7. 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 1 *Let R be a finite commutative ring. Then the map*

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

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. Further, $[f]_R = id_R = [x]_R$ by Definition 4. 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 6. By Lemma 3, $[f']_R \in \mathcal{F}(R)^\times$. 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. 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 4, $[g]_R = id_R$, 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 6 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 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 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 4, and hence $\psi([f]_{\mathbb{F}_q[\alpha]}) = [f']_{\mathbb{F}_q} = F$. Therefore ψ is surjective. □

Notation 1 Let $S_\alpha(R)$ denote the subgroup $\psi(St_\alpha(R))$ of $\mathcal{F}(R)^\times$, where ψ is the embedding of Theorem 1. 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 8 From Remark 5, we know that

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

and, so, by the embedding ψ of Theorem 1, we have, with respect to Notation 1, the isomorphisms

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

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 2 to $St_\alpha(R)$, we have, by the definitions of ϕ and $S_\alpha(R)$,

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

This shows that the embedding of $St_\alpha(R)$ in $\mathcal{P}(R) \ltimes_\theta \mathcal{F}(R)^\times$ via Proposition 2 is identical to the embedding using Theorem 1 and Remark 5. In other words the following diagram commutes:

$$\begin{tikzcd}
\mathcal{P}_R(R[\alpha]) \arrow[r, "\phi(F)=([f]_R,[f']_R)"] & \mathcal{P}(R) \ltimes_\theta \mathcal{F}(R)^\times \\
St_\alpha(R) \arrow[u, "inclusion\ (Proposition\ 3)"] \arrow[r, "\psi(F)=[f']_R"] & \mathcal{F}(R)^\times \arrow[u, "embedding\ (Remark\ 5)"']
\end{tikzcd}$$

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

Notation 2 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 8. That is, $\overline{S_\alpha(R)} = \{(id_R, F) : F \in S_\alpha(R)\}$.

Lemma 5 *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 4. On the other hand, when R is a finite local ring that is not a field, the result follows from Fact 1. $\square$

Remark 9

1. Define a map

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

   Then, by Remark 6 and Lemma 5, 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 [1]).
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 2. Then, by (1) and Remark 8, $\overline{S_\alpha(R)} \lhd \phi(\mathcal{P}_R(R[\alpha]))$.

Lemma 6 *Let $S_\alpha(R)$ be as in Notation 1, 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 5, 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. Thus, by Proposition 2, $([f]_R, [f']_R) = (G, F_1) \in \phi(\mathcal{P}_R(R[\alpha]))$, where ϕ is the homomorphism of Proposition 2 (see also, Remark 9 (2)). We now use the fact that $\overline{S_\alpha(R)} = \{(id_R, F) : F \in S_\alpha(R)\}$ is a normal subgroup of $\phi(\mathcal{P}_R(R[\alpha]))$, by Proposition 1 and the fact that $\mathcal{F}(R)^\times$ is Abelian, we have

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

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

Theorem 2 *Let R be a finite commutative ring, $\mathcal{P}(R) \ltimes_\theta \mathcal{F}(R)^\times$ the semidirect product constructed in Proposition 1 and $St_\alpha(R)$ the stabilizer group defined in Definition 4*. Then the map

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

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 2 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 8 and Notation 2,

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

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 1, we have, just as in the proof of Lemma 6, 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 6. □

Recall from Notation 1 that $S_\alpha(R)$ denotes a subgroup of $\mathcal{F}(R)^\times$, which is isomorphic to $St_\alpha(R)$.

Remark 10 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 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 6, $F \circ G \in S_\alpha(R)$ for every $F \in S_\alpha(R)$. Thus the restriction of θ_G to $S_\alpha(R)$ is an automorphism, that is, the map $\tilde{\theta}_G : S_\alpha(R) \longrightarrow S_\alpha(R)$ 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 $\theta : \mathcal{P}(R) \longrightarrow Aut(\mathcal{F}(R)^\times)$ of Lemma 2, we have the map $\tilde{\theta} : \mathcal{P}(R) \longrightarrow Aut(S_\alpha(R))$ 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 4 *Let R be a finite commutative ring. Let θ and $\tilde{\theta}$ be the homomorphisms of Remark 10. 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 1. Again, by Theorem 1, $St_\alpha(R) \cong S_\alpha(R) = \mathcal{F}(R)^\times$. $\square$

In Proposition 2 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 *Let $\mathbb{F}_q$ be the finite field of q elements. Let θ and $\tilde{\theta}$ be the homomorphisms of Remark 10, 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 2, Proposition 4 and Theorem 1 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 7, 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

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

It is obvious that the total number of different pairs of this form is $q!(q-1)^q$. Moreover, by Lemma 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. Then, by Remark 6, every two different pairs of functions satisfying the conditions of Lemma 4 determine two different elements of $\mathcal{P}_{\mathbb{F}_q}(\mathbb{F}_q[\alpha])$. Therefore $|\mathcal{P}_{\mathbb{F}_q}(\mathbb{F}_q[\alpha])| \geq q!(q-1)^q$. $\square$

Remark 11 When $q = p$ (where p is a prime number), Frisch and Krenn [2] 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 $n \geq 2$.

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, [3, 8]). In this section we apply the results of [3] 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 12

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

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

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 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 [3] gives the cardinality of $\ker \phi_n$ of the epimorphism ϕ_n mentioned in Remark 12.

Lemma 7 [3, *Theorem* 2] *Let $n > 1$ and let ϕ_n be the epimorphism of Remark* 12.

Then $|\ker \phi_n| = p^{\beta(n)}$.

Lemma 8 *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 12 (2). Then $\phi_n^{-1}(\mathcal{F}(\mathbb{Z}_{p^{n-1}})^\times) = \mathcal{F}(\mathbb{Z}_{p^n})^\times$ by Remark 12 (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 12, $|\phi_n^{-1}(F)| = |\ker \phi_n|$. 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 7. $\square$

Keep the notations of Notation 3. We now state our counting formula for the order of $\mathcal{F}(\mathbb{Z}_{p^{n-1}})^{\times}$.

Theorem 4 *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 8 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 7. □

We need the following fact from [3].

Lemma 9 [3, *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 $i = 0, \dots, \beta(n) - 1$.*

It follows that, $|\mathcal{F}(\mathbb{Z}_{p^n})| = p^{\sum_{i=1}^{n} \beta(i)}$.

Keep the notations of Notation 3. 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 7).

Theorem 5 *Let $l_1, \dots, l_{(p-1)^p}$ 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*

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

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 $s = 1, \dots, (p-1)^p$.

Proof Let A denote the set of all polynomials in $\mathbb{Z}[x]$ that satisfy the conditions of equation (1). By Remark 12 (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

$$\sum_{i=0}^{\beta(n)-1} a_i (x)_i, \text{ where } 0 \le a_i < p^{n-v_p(i!)} \text{ for } 0 \le i < \beta(n) \text{ with } p \mid a_i \text{ for } i < p. \tag{2}$$

Clearly,

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

In the light of Equation (2) and Lemma 9,

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

Therefore, by Theorem 4,

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

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 $s_1, s_2 \in \{1, \dots, (p-1)^p\}$. 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 9, 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 1 Let $R = \mathbb{Z}_4 = \{0, 1, 2, 3\}$. In this case, $\mathbb{Z}_4[\alpha] = \{a + b\alpha : a, b \in \mathbb{Z}_4\}$. 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

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

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 $1 + f_1', \dots, 1 + f_4'$ 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 4. Furthermore, by Remark 9 (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 2 and Theorem 1 need not be isomorphisms.

Acknowledgements This work is supported by the Austrian Science Fund (FWF): P 27816-N26 and P 30934-N35. I would like to thank my supervisor Sophie Frisch for her valuable suggestions on earlier version of the manuscript.

Funding Open access funding provided by Graz University of Technology.

References

1. Al-Ezeh, H., Al-Maktry, A.A., Frisch, S.: Polynomial functions on rings of dual numbers over residue class of the integers. To appear in Mathematica Slovaca, https://arxiv.org/abs/1910.00238
2. Frisch, S., Krenn, D.: Sylow p-groups of polynomial permutations on the integers mod p^n. J. Number Theory **133**(12), 4188–4199 (2013)
3. Keller, G., Olson, F.R.: Counting polynomial functions $(\bmod\, p^n)$. Duke Math. J. **35**, 835–838 (1968)
4. Kurzweil, H., Stellmacher, B.: The theory of finite groups. Universitext, Springer-Verlag, New York, (2004), An introduction, Translated from the 1998 German original
5. Leary, F.C.: Rings with invertible regular elements. Am. Math. Monthly **96**(10), 924–926 (1989)
6. Loper, A.: On rings without a certain divisibility property. J. Number Theory **28**(2), 132–144 (1988)
7. Nechaev, A.A.: Polynomial transformations of finite commutative local rings of principal ideals, Math. Notes, 27, 425-432 (1980), transl. from Mat. Zametki, 27, 885-897 (1980)
8. Singmaster, D.: On polynomial functions (mod m). J. Number Theory **6**, 345–352 (1974)