Journal of Number Theory 133 (2013) 4188–4199

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Sylow p-groups of polynomial permutations on the integers mod p^n

Sophie Frisch[a,*,1], Daniel Krenn[b,2]

[a] *Institut für Mathematik A, Technische Universität Graz, Steyrergasse 30, A-8010 Graz, Austria*
[b] *Institut für Mathematik B, Technische Universität Graz, Steyrergasse 30, A-8010 Graz, Austria*

ARTICLE INFO

Article history:
Received 9 July 2012
Accepted 23 June 2013
Available online 4 September 2013
Communicated by D. Wan

MSC:
primary 20D20
secondary 11T06, 13M10, 11C08, 13F20, 20E18

Keywords:
Polynomial permutations
Polynomial functions
Polynomial mappings
p-Groups
Pro-p-groups
Sylow p-groups
Finite rings

ABSTRACT

We enumerate and describe the Sylow p-groups of the groups of polynomial permutations of the integers mod p^n for $n \geqslant 1$ and of the pro-finite group which is the projective limit of these groups.

© 2013 The Authors. Published by Elsevier Inc.
Open access under CC BY license.

* Corresponding author.
E-mail addresses: frisch@tugraz.at (S. Frisch), krenn@math.tugraz.at (D. Krenn).
[1] Sophie Frisch is supported by the Austrian Science Fund (FWF), grant P23245-N18.
[2] Daniel Krenn is supported by the Austrian Science Fund (FWF), project W1230 doctoral program "Discrete Mathematics".

0022-314X © 2013 The Authors. Published by Elsevier Inc. Open access under CC BY license.
http://dx.doi.org/10.1016/j.jnt.2013.06.002

1. Introduction

Fix a prime p and let $n \in \mathbb{N}$. Every polynomial $f \in \mathbb{Z}[x]$ defines a function from $\mathbb{Z}_{p^n} = \mathbb{Z}/p^n\mathbb{Z}$ to itself. If this function happens to be bijective, it is called a *polynomial permutation* of $\mathbb{Z}_{p^n}$. The polynomial permutations of $\mathbb{Z}_{p^n}$ form a group $(G_n, \circ)$ with respect to composition. The order of this group has been known since at least 1921 (Kempner [10]) to be

$$|G_2| = p!(p-1)^p p^p \quad \text{and} \quad |G_n| = p!(p-1)^p p^p p^{\sum_{k=3}^{n} \beta(k)} \quad \text{for } n \geqslant 3,$$

where $\beta(k)$ is the least n such that p^k divides $n!$, but the structure of $(G_n, \circ)$ is elusive. (See, however, Nöbauer [15] for some partial results.) Since the order of G_n is divisible by a high power of $(p-1)$ for large p, even the number of Sylow p-groups is not obvious.

We will show that there are $(p-1)!(p-1)^{p-2}$ Sylow p-groups of G_n and describe these Sylow p-groups, see Theorem 5.1 and Corollary 5.2.

Some notation: p is a fixed prime throughout. A function $g: \mathbb{Z}_{p^n} \to \mathbb{Z}_{p^n}$ arising from a polynomial in $\mathbb{Z}_{p^n}[x]$ or, equivalently, from a polynomial in $\mathbb{Z}[x]$, is called a *polynomial function* on $\mathbb{Z}_{p^n}$. We denote by $(F_n, \circ)$ the monoid with respect to composition of polynomial functions on $\mathbb{Z}_{p^n}$. By monoid, we mean semigroup with an identity element. Let $(G_n, \circ)$ be the group of units of $(F_n, \circ)$, which is the group of polynomial permutations of $\mathbb{Z}_{p^n}$.

Since every function induced by a polynomial preserves congruences modulo ideals, there is a natural epimorphism mapping polynomial functions on $\mathbb{Z}_{p^{n+1}}$ onto polynomial functions on $\mathbb{Z}_{p^n}$, and we write it as $\pi_n: F_{n+1} \to F_n$. If f is a polynomial in $\mathbb{Z}[x]$ (or in $\mathbb{Z}_{p^m}[x]$ for $m \geqslant n$) we denote the polynomial function on $\mathbb{Z}_{p^n}[x]$ induced by f by $[f]_{p^n}$.

The order of F_n and that of G_n have been determined by Kempner [10] in a rather complicated manner. His results were cast into a simpler form by Nöbauer [14] and Keller and Olson [9] among others. Since then there have been many generalizations of the order formulas to more general finite rings [16,13,2,6,1,8,7]. Also, polynomial permutations in several variables (permutations of $(\mathbb{Z}_{p^n})^k$ defined by k-tuples of polynomials in k variables) have been looked into [5,4,19,17,18,11].

2. Polynomial functions and permutations

To put things in context, we recall some well-known facts, to be found, among other places, in [10,14,3,9]. The reader familiar with polynomial functions on finite rings is encouraged to skip to Section 3. Note that we do not claim anything in Section 2 as new.

Definition. For p prime and $n \in \mathbb{N}$, let

$$\alpha_p(n) = \sum_{k=1}^{\infty} \left[\frac{n}{p^k}\right] \quad \text{and} \quad \beta_p(n) = \min\{m \mid \alpha_p(m) \geqslant n\}.$$

If p is fixed, we just write $\alpha(n)$ and $\beta(n)$.

Notation. For $k \in \mathbb{N}$, let $(x)_k = x(x-1)\dots(x-k+1)$ and $(x)_0 = 1$. We denote p-adic valuation by v_p.

2.1 Fact.

(1) $\alpha_p(n) = v_p(n!)$.
(2) For $1 \leqslant n \leqslant p$, $\beta_p(n) = np$ and for $n > p$, $\beta_p(n) < np$.
(3) For all $n \in \mathbb{Z}$, $v_p((n)_k) \geqslant \alpha_p(k)$; and $v_p((k)_k) = v_p(k!) = \alpha_p(k)$.

Proof. Easy. □

Remark. The sequence $(\beta_p(n))_{n=1}^{\infty}$ is obtained by going through the natural numbers in increasing order and repeating each $k \in \mathbb{N}$ $v_p(k)$ times. For instance, $\beta_2(n)$ for $n \geqslant 1$ is: $2, 4, 4, 6, 8, 8, 8, 10, 12, 12, 14, 16, 16, 16, 16, 18, 20, 20, \dots$.

The falling factorials $(x)_0 = 1$, $(x)_k = x(x-1)\dots(x-k+1)$, $k > 0$, form a basis of the free $\mathbb{Z}$-module $\mathbb{Z}[x]$, and representation with respect to this basis gives a convenient canonical form for a polynomial representing a given polynomial function on $\mathbb{Z}_{p^n}$.

2.2 Fact. (Cf. Keller and Olson [9].) A polynomial $f \in \mathbb{Z}[x]$, $f = \sum_k a_k (x)_k$, induces the zero-function mod p^n if and only if $a_k \equiv 0 \bmod p^{n-\alpha(k)}$ for all k (or, equivalently, for all $k < \beta(n)$).

Proof. Induction on k using the facts that $(m)_k = 0$ for $m < k$, that $v_p((n)_k) \geqslant \alpha_p(k)$ for all $n \in \mathbb{Z}$, and that $v_p((k)_k) = v_p(k!) = \alpha_p(k)$. □

2.3 Corollary. *(Cf. Keller and Olson [9].) Every polynomial function on $\mathbb{Z}_{p^n}$ is represented by a unique $f \in \mathbb{Z}[x]$ of the form $f = \sum_{k=0}^{\beta(n)-1} a_k (x)_k$, with $0 \leqslant a_k < p^{n-\alpha(k)}$ for all k.*

Comparing the canonical forms of polynomial functions mod p^n with those mod p^{n-1} we see that every polynomial function mod p^{n-1} gives rise to $p^{\beta(n)}$ different polynomial functions mod p^n:

2.4 Corollary. *(See cf. Keller and Olson [9].) Let $(F_n, \circ)$ be the monoid of polynomial functions on $\mathbb{Z}_{p^n}$ with respect to composition and $\pi_n \colon F_{n+1} \to F_n$ the canonical projection.*

(1) *For all $n \geqslant 1$ and for each $f \in F_n$ we have $|\pi_n^{-1}(f)| = p^{\beta(n+1)}$.*
(2) *For all $n \geqslant 1$, the number of polynomial functions on $\mathbb{Z}_{p^n}$ is*

$$|F_n| = p^{\sum_{k=1}^{n} \beta(k)}.$$

Notation. We write $[f]_{p^n}$ for the function defined by $f \in \mathbb{Z}[x]$ on $\mathbb{Z}_{p^n}$.

2.5 Lemma. *Every polynomial $f \in \mathbb{Z}[x]$ is uniquely representable as*

$$f(x) = f_0(x) + f_1(x)\big(x^p - x\big) + f_2(x)\big(x^p - x\big)^2 + \cdots + f_m(x)\big(x^p - x\big)^m + \cdots$$

with $f_m \in \mathbb{Z}[x]$, $\deg f_m < p$, for all $m \geqslant 0$. Now let $f, g \in \mathbb{Z}[x]$.

(1) *If $n \leqslant p$, then $[f]_{p^n} = [g]_{p^n}$ is equivalent to: $f_k = g_k \bmod p^{n-k}\mathbb{Z}[x]$ for $0 \leqslant k < n$.*
(2) *$[f]_{p^2} = [g]_{p^2}$ is equivalent to: $f_0 = g_0 \bmod p^2\mathbb{Z}[x]$ and $f_1 = g_1 \bmod p\mathbb{Z}[x]$.*
(3) *$[f]_p = [g]_p$ and $[f']_p = [g']_p$ is equivalent to: $f_0 = g_0 \bmod p\mathbb{Z}[x]$ and $f_1 = g_1 \bmod p\mathbb{Z}[x]$.*

Proof. The canonical representation is obtained by repeated division with remainder by $(x^p - x)$, and uniqueness follows from uniqueness of quotient and remainder of polynomial division. Note that $[f]_p = [f_0]_p$ and $[f']_p = [f_0' - f_1]_p$. This gives (3).

Denote by $f \sim g$ the equivalence relation $f_k = g_k \bmod p^{n-k}\mathbb{Z}[x]$ for $0 \leqslant k < n$. Then $f \sim g$ implies $[f]_{p^n} = [g]_{p^n}$. There are $p^{p+2p+3p+\cdots+np}$ equivalence classes of $\sim$ and $p^{\beta(1)+\beta(2)+\beta(3)+\cdots+\beta(n)}$ different $[f]_{p^n}$. For $k \leqslant p$, $\beta(k) = kp$. Therefore the equivalence relations $f \sim g$ and $[f]_{p^n} = [g]_{p^n}$ coincide. This gives (1), and (2) is just the special case $n = 2$. □

We can rephrase this in terms of ideals of $\mathbb{Z}[x]$.

2.6 Corollary. *For every $n \in \mathbb{N}$, consider the two ideals of $\mathbb{Z}[x]$*

$$I_n = \big\{f \in \mathbb{Z}[x] \;\big|\; f(\mathbb{Z}) \subseteq p^n\mathbb{Z}\big\} \quad \text{and} \quad J_n = \big(\big\{p^{n-k}\big(x^p - x\big)^k \;\big|\; 0 \leqslant k \leqslant n\big\}\big).$$

Then $[\mathbb{Z}[x]\colon I_n] = p^{\beta(1)+\beta(2)+\beta(3)+\cdots+\beta(n)}$ and $[\mathbb{Z}[x]\colon J_n] = p^{p+2p+3p+\cdots+np}$. Therefore, $J_n = I_n$ for $n \leqslant p$, whereas for $n > p$, J_n is properly contained in I_n.

Proof. $J_n \subseteq I_n$. The index of J_n in $\mathbb{Z}[x]$ is $p^{p+2p+3p+\cdots+np}$, because $f \in J_n$ if and only if $f_k = 0 \bmod p^{n-k}\mathbb{Z}[x]$ for $0 \leqslant k < n$ in the canonical representation of Lemma 2.5. The index of I_n in $\mathbb{Z}[x]$ is $p^{\beta(1)+\beta(2)+\beta(3)+\cdots+\beta(n)}$ by Corollary 2.4(2) and $[\mathbb{Z}[x]\colon I_n] < [\mathbb{Z}[x]\colon J_n]$ if and only if $n > p$ by Fact 2.1(2). □

2.7 Fact. (Cf. McDonald [12].) Let $n \geqslant 2$. The function on $\mathbb{Z}_{p^n}$ induced by a polynomial $f \in \mathbb{Z}[x]$ is a permutation if and only if

(1) f induces a permutation of $\mathbb{Z}_p$, and
(2) the derivative f' has no zero mod p.

2.8 Lemma. *Let $[f]_{p^n}$ and $[f]_p$ be the functions defined by $f \in \mathbb{Z}[x]$ on $\mathbb{Z}_{p^n}$ and $\mathbb{Z}_p$, respectively, and $[f']_p$ the function defined by the formal derivative of f on $\mathbb{Z}_p$. Then*

(1) $[f]_{p^2}$ *determines not just* $[f]_p$, *but also* $[f']_p$.
(2) *Let* $n \geqslant 2$. *Then* $[f]_{p^n}$ *is a permutation if and only if* $[f]_{p^2}$ *is a permutation.*
(3) *For every pair of functions* (α, β), $\alpha: \mathbb{Z}_p \to \mathbb{Z}_p$, $\beta: \mathbb{Z}_p \to \mathbb{Z}_p$, *there are exactly* p^p *polynomial functions* $[f]_{p^2}$ *on* $\mathbb{Z}_{p^2}$ *with* $[f]_p = \alpha$ *and* $[f']_p = \beta$.
(4) *For every pair of functions* (α, β), $\alpha: \mathbb{Z}_p \to \mathbb{Z}_p$ *bijective*, $\beta: \mathbb{Z}_p \to \mathbb{Z}_p \setminus \{0\}$, *there are exactly* p^p *polynomial permutations* $[f]_{p^2}$ *on* $\mathbb{Z}_{p^2}$ *with* $[f]_p = \alpha$ *and* $[f']_p = \beta$.

Proof. (1) and (3) follow immediately from Lemma 2.5 for $n = 2$ and (2) and (4) then follow from Fact 2.7. □

2.9 Remark. Fact 2.7 and Lemma 2.8(2) imply that

(1) for all $n \geqslant 1$, the image of G_{n+1} under $\pi_n: F_{n+1} \to F_n$ is contained in G_n, and
(2) for all $n \geqslant 2$, the inverse image of G_n under $\pi_n: F_{n+1} \to F_n$ is G_{n+1}.

We denote by $\pi_n: G_{n+1} \to G_n$ the restriction of π_n to G_n. This is the canonical epimorphism from the group of polynomial permutations on $\mathbb{Z}_{p^{n+1}}$ onto the group of polynomial permutations on $\mathbb{Z}_{p^n}$.

The above remark allows us to draw conclusions on the projective system of groups G_n from the information in Corollary 2.4 concerning the projective system of monoids F_n.

2.10 Corollary. *Let* $n \geqslant 2$, *and* $\pi_n: G_{n+1} \to G_n$ *the canonical epimorphism from the group of polynomial permutations on* $\mathbb{Z}_{p^{n+1}}$ *onto the group of polynomial permutations on* $\mathbb{Z}_{p^n}$. *Then*

$$\left|\ker(\pi_n)\right| = p^{\beta(n+1)}.$$

2.11 Corollary. *(See cf. Kempner [10] and Keller and Olson [9].) The number of polynomial permutations on* $\mathbb{Z}_{p^2}$ *is*

$$|G_2| = p!(p-1)^p p^p,$$

and for $n \geqslant 3$ *the number of polynomial permutations on* $\mathbb{Z}_{p^2}$ *is*

$$|G_n| = p!(p-1)^p p^p p^{\sum_{k=3}^{n} \beta(k)}.$$

Proof. In the canonical representation of $f \in \mathbb{Z}[x]$ in Lemma 2.5, there are $p!(p-1)^p$ choices of coefficients mod p for f_0 and f_1 such that the criteria of Fact 2.7 for a polynomial permutation on $\mathbb{Z}_{p^2}$ are satisfied. And for each such choice there are p^p possibilities for the coefficients of f_0 mod p^2. The coefficients of f_0 mod p^2 and those of f_1 mod p then determine the polynomial function mod p^2. So $|G_2| = p!(p-1)^p p^p$. The formula for $|G_n|$ then follows from Corollary 2.10. □

This concludes our review of polynomial functions and polynomial permutations on $\mathbb{Z}_{p^n}$. We will now introduce a homomorphic image of G_2 whose Sylow p-groups bijectively correspond to the Sylow p-groups of G_n for any $n \geqslant 2$.

3. A group between G_1 and G_2

Into the projective system of monoids $(F_n, \circ)$ we insert an extra monoid E between F_1 and F_2 by means of monoid-epimorphisms $\theta: F_2 \to E$ and $\psi: E \to F_1$ with $\psi\theta = \pi_1$,

$$F_1 \xleftarrow{\psi} E \xleftarrow{\theta} F_2 \xleftarrow{\pi_2} F_3 \xleftarrow{\pi_3} \cdots.$$

The restrictions of θ to G_2 and of ψ to the group of units H of E will be group-epimorphisms, so that we also insert an extra group H between G_1 and G_2 into the projective system of the G_i,

$$G_1 \xleftarrow{\psi} H \xleftarrow{\theta} G_2 \xleftarrow{\pi_2} G_3 \xleftarrow{\pi_3} \cdots.$$

In the following definition of E and H, f and f' are just two different names for functions. The connection with polynomials and their formal derivatives suggested by the notation will appear when we define θ and ψ.

Definition. We define the semigroup $(E, \circ)$ by

$$E = \{(f, f') \mid f: \mathbb{Z}_p \to \mathbb{Z}_p f' : \mathbb{Z}_p \to \mathbb{Z}_p\}$$

(where f and f' are just symbols) with law of composition

$$(f, f') \circ (g, g') = (f \circ g, (f' \circ g) \cdot g').$$

Here $(f \circ g)(x) = f(g(x))$ and $((f' \circ g) \cdot g')(x) = f'(g(x)) \cdot g'(x)$.

We denote by $(H, \circ)$ the group of units of E.

The following facts are easy to verify:

3.1 Lemma.

(1) *The identity element of E is $(\iota, 1)$, with ι denoting the identity function on $\mathbb{Z}_p$ and 1 the constant function 1.*
(2) *The group of units of E has the form*

$$H = \{(f, f') \mid f: \mathbb{Z}_p \to \mathbb{Z}_p \text{ bijective},\ f': \mathbb{Z}_p \to \mathbb{Z}_p \setminus \{0\}\}.$$

(3) *The inverse of* $(g, g') \in H$ *is*

$$(g, g')^{-1} = \left(g^{-1}, \frac{1}{g' \circ g^{-1}}\right),$$

where g^{-1} *is the inverse permutation of the permutation* g *and* $1/a$ *stands for the multiplicative inverse of a non-zero element* $a \in \mathbb{Z}_p$*, such that*

$$\left(\frac{1}{g' \circ g^{-1}}\right)(x) = \frac{1}{g'(g^{-1}(x))}$$

means the multiplicative inverse in $\mathbb{Z}_p \setminus \{0\}$ *of* $g'(g^{-1}(x))$.

Note that H is a semidirect product of (as the normal subgroup) a direct sum of p copies of the cyclic group of order $p - 1$ and (as the complement acting on it) the symmetric group on p letters, S_p, acting on the direct sum by permuting its components. In combinatorics, one would call this a wreath product (designed to act on the left) of the abstract group C_{p-1} by the permutation group S_p with its standard action on p letters. (Group theorists, however, have a narrower definition of wreath product, which is not applicable here.)

Now for the homomorphisms θ and ψ.

Definition. We define $\psi: E \longrightarrow F_1$ by $\psi(f, f') = f$. As for $\theta: F_2 \to E$, given an element $[g]_{p^2} \in F_2$, set $\theta([g]_{p^2}) = ([g]_p, [g']_p)$. θ is well defined by Lemma 2.8(1).

3.2 Lemma.

(i) $\theta: F_2 \to E$ *is a monoid-epimorphism.*
(ii) *The inverse image of* H *under* $\theta: F_2 \to E$ *is* G_2.
(iii) *The restriction of* θ *to* G_2 *is a group-epimorphism* $\theta: G_2 \to H$ *with* $|\ker(\theta)| = p^p$.
(iv) $\psi: E \to F_1$ *is a monoid-epimorphism and* ψ *restricted to* H *is a group-epimorphism* $\psi: H \to G_1$.

Proof. (i) follows from Lemma 2.8(3) and (ii) from Fact 2.7. (iii) follows from Lemma 2.8(4). Finally, (iv) holds because every function on $\mathbb{Z}_p$ is a polynomial function and every permutation of $\mathbb{Z}_p$ is a polynomial permutation. □

4. Sylow subgroups of *H*

We will first determine the Sylow p-groups of H. The Sylow p-groups of G_n for $n \geqslant 2$ are obtained in the next section as the inverse images of the Sylow p-groups of H under the epimorphism $G_n \to H$.

4.1 Lemma. *Let C_0 be the subgroup of S_p generated by the p-cycle $(0\ 1\ 2 \dots p-1)$. Then one Sylow p-subgroup of H is*

$$S = \{(f, f') \in H \mid f \in C_0,\ f' = 1\},$$

where $f' = 1$ means the constant function 1. The normalizer of S in H is

$$N_H(S) = \{(g, g') \mid g \in N_{S_p}(C_0),\ g' \text{ a non-zero constant}\}.$$

Proof. As $|H| = p!(p-1)^p$, and S is a subgroup of H of order p, S is a Sylow p-group of H. Conjugation of $(f, f') \in S$ by $(g, g') \in H$ (using the fact that $f' = 1$) gives

$$(g, g')^{-1}(f, f')(g, g') = \left(g^{-1}, \frac{1}{g' \circ g^{-1}}\right)(f \circ g, g') = \left(g^{-1} \circ f \circ g, \frac{g'}{g' \circ g^{-1} \circ f \circ g}\right).$$

The first coordinate of $(g, g')^{-1}(f, f')(g, g')$ being in C_0 for all $(f, f') \in S$ is equivalent to $g \in N_{S_p}(C_0)$. The second coordinate of $(g, g')^{-1}(f, f')(g, g')$ being the constant function 1 for all $(f, f') \in S$ is equivalent to

$$\forall x \in \mathbb{Z}_p, \quad g'(x) = g'\left(g^{-1}\left(f\left(g(x)\right)\right)\right),$$

which is equivalent to g' being constant on every cycle of $g^{-1} f g$, which is equivalent to g' being constant on $\mathbb{Z}_p$, since f can be chosen to be a p-cycle. □

4.2 Lemma. *Another way of describing the normalizer of S in H is*

$$N_H(S) = \{(g, g') \in H \mid \exists k \neq 0\ \forall a, b,\ g(a) - g(b) = k(a-b);\ g' \text{ a non-zero constant}\}.$$

Therefore, $|N_H(S)| = p(p-1)^2$ and $[H : N_H(S)] = (p-1)!(p-1)^{p-2}$.

Proof. Let $\sigma = (0\ 1\ 2 \dots p-1)$ and $g \in S_p$ then

$$g \sigma g^{-1} = \left(g(0)\ g(1)\ g(2) \dots g(p-1)\right).$$

Now $g \in N_{S_p}(C_0)$ if and only if, for some $1 \leqslant k < p$, $g \sigma g^{-1} = \sigma^k$, i.e.,

$$\left(g(0)\ g(1)\ g(2) \dots g(p-1)\right) = \left(0\ k\ 2k \dots (p-1)k\right),$$

all numbers taken mod p. This is equivalent to $g(x+1) = g(x) + k$ or

$$g(x+1) - g(x) = k$$

and further equivalent to $g(a) - g(b) = k(a-b)$. Thus k and $g(0)$ determine $g \in N_{S_p}(C_0)$, and there are $(p-1)$ choices for k and p choices for $g(0)$. Together with the $(p-1)$ choices for the non-zero constant g' this makes $p(p-1)^2$ elements of $N_H(S)$. □

4.3 Corollary. *There are $(p-1)!(p-1)^{p-2}$ Sylow p-subgroups of H.*

4.4 Theorem. *The Sylow p-subgroups of H are in bijective correspondence with pairs $(C,\bar{\varphi})$, where C is a cyclic subgroup of order p of S_p, $\varphi\colon \mathbb{Z}_p \to \mathbb{Z}_p \setminus \{0\}$ is a function and $\bar{\varphi}$ is the class of φ with respect to the equivalence relation of multiplication by a non-zero constant. The subgroup corresponding to $(C,\bar{\varphi})$ is*

$$S_{(C,\bar{\varphi})} = \left\{ (f,f') \in H \;\middle|\; f \in C,\ f'(x) = \frac{\varphi(f(x))}{\varphi(x)} \right\}.$$

Proof. Observe that each $S_{(C,\bar{\varphi})}$ is a subgroup of order p of H. Different pairs $(C,\bar{\varphi})$ give rise to different groups: Suppose $S_{(C,\bar{\varphi})} = S_{(D,\bar{\psi})}$. Then $C = D$ and for all $x \in \mathbb{Z}_p$ and for all $f \in C$ we get

$$\frac{\varphi(f(x))}{\varphi(x)} = \frac{\psi(f(x))}{\psi(x)}.$$

As C is transitive on $\mathbb{Z}_p$ the latter condition is equivalent to

$$\forall x,y \in \mathbb{Z}_p \quad \frac{\psi(x)}{\varphi(x)} = \frac{\psi(y)}{\varphi(y)},$$

which means that $\varphi = k\psi$ for a non-zero $k \in \mathbb{Z}_p$.

There are $(p-2)!$ cyclic subgroups of order p of S_p, and $(p-1)^{p-1}$ equivalence classes $\bar{\varphi}$ of functions $\varphi\colon \mathbb{Z}_p \to \mathbb{Z}_p \setminus \{0\}$. So the number of pairs $(C,\bar{\varphi})$ equals $(p-1)!(p-1)^{p-2}$, which is the number of Sylow p-groups of H, by the preceding corollary. □

4.5 Proposition. *If p is an odd prime then the intersection of all Sylow p-subgroups of H is trivial, i.e.,*

$$\bigcap_{(C,\overline{\varphi})} S_{(C,\overline{\varphi})} = \{(\iota,1)\}.$$

If $p = 2$ then $|H| = 2$ and the intersection of all Sylow 2-subgroups of H is H itself.

Proof. Let p be an odd prime, and let $(f,f') \in \bigcap_{(C,\overline{\varphi})} S_{(C,\overline{\varphi})}$. Suppose f is not the identity function and let $k \in \mathbb{Z}_p$ such that $f(k) \neq k$.

Note that φ in $(C,\overline{\varphi})$ is arbitrary, apart from the fact that 0 is not in the image. Therefore, and because $p \geqslant 3$, among the various φ there occur functions ϑ and η with $\vartheta(k) = \eta(k)$ and $\vartheta(f(k)) \neq \eta(f(k))$. Now $(f,f') \in S_{(D,\bar{\vartheta})} \cap S_{(E,\bar{\eta})}$ for any cyclic subgroups D and E of S_p of order p.

Therefore

$$\frac{\vartheta(f(k))}{\vartheta(k)} = f'(k) = \frac{\eta(f(k))}{\eta(k)},$$

and hence $\vartheta(f(k)) = \eta(f(k))$, a contradiction. Thus f is the identity and therefore $f' = 1$.

If $p = 2$ then $|H| = 2$ and therefore the one and only Sylow 2-subgroup of H is H. $\square$

In the case $p \geqslant 5$, the lemma above can be proved in a simpler way: There is more than one cyclic group of order p, so for $(f, f') \in \bigcap_{(C,\overline{\varphi})} S_{(C,\overline{\varphi})}$, there are distinct cyclic groups D and E of order p with $f \in D \cap E$. Therefore f has to be the identity.

5. Sylow subgroups of G_n and of the projective limit

Again we consider the projective system of finite groups

$$G_1 \xleftarrow{\psi} H \xleftarrow{\theta} G_2 \xleftarrow{\pi_2} \cdots \xleftarrow{\pi_{n-1}} G_n \xleftarrow{\pi_n}$$

where $(G_n, \circ)$ is the group of polynomial permutations on $\mathbb{Z}_{p^n}$ (with respect to composition of functions) and H is the group defined in section 3. Let $G = \varprojlim G_n$ be the projective limit of this system. Recall that a Sylow p-group of a pro-finite group is defined as a maximal group consisting of elements whose order in each of the finite groups in the projective system is a power of p.

5.1 Theorem.

(i) *Let $(G_n, \circ)$ be the group of polynomial permutations on $\mathbb{Z}_{p^n}$ with respect to composition. If $n \geqslant 2$ there are $(p-1)!(p-1)^{p-2}$ Sylow p-groups of G_n. They are the inverse images of the Sylow p-groups of H (described in Theorem 4.4) under the canonical projection $\pi: G_n \to H$, with $\pi = \theta\pi_2 \ldots \pi_{n-1}$.*

(ii) *Let $G = \varprojlim G_n$. There are $(p-1)!(p-1)^{p-2}$ Sylow p-groups of G, which are the inverse images of the Sylow p-groups of H (described in Theorem 4.4) under the canonical projection $\pi: G \to H$.*

Proof. In the projective system $G_1 \xleftarrow{\psi} H \xleftarrow{\theta} G_2 \xleftarrow{\pi_2} \cdots \xleftarrow{\pi_{n-1}} G_n$ the kernel of the group-epimorphism $G_n \to H$ is a finite p-group for every $n \geqslant 2$, because for $n \geqslant 2$ the kernel of $\pi_n: G_{n+1} \to G_n$ is of order $p^{\beta(n+1)}$ by Corollary 2.10 $\theta: G_2 \to H$ is of order p^p by Lemma 3.2(iii). So the Sylow p-groups of G_n for $n \geqslant 2$ are just the inverse images of the Sylow p-groups of H and, likewise, the Sylow p-groups of the projective limit G are just the inverse images of the Sylow p-groups of H, whose number was determined in Corollary 4.3. $\square$

If we combine this information with the description of the Sylow p-groups of H in Theorem 4.4 we get the following explicit description of the Sylow p-groups of G_n. Recall that $[f]_{p^n}$ denotes the function induced on $\mathbb{Z}_{p^n}$ by the polynomial f in $\mathbb{Z}[x]$ (or in $\mathbb{Z}_{p^m}[x]$ for some $m \geqslant n$).

5.2 Corollary. *Let $n \geqslant 2$. Let G_n be the group (with respect to composition) of polynomial permutations on $\mathbb{Z}_{p^n}$. The Sylow p-groups of G_n are in bijective correspondence with pairs $(C, \bar{\varphi})$, where C is a cyclic subgroup of order p of S_p, $\varphi: \mathbb{Z}_p \to \mathbb{Z}_p \setminus \{0\}$ is a function and $\bar{\varphi}$ its class with respect to the equivalence relation of multiplication by a non-zero constant. The subgroup corresponding to $(C, \bar{\varphi})$ is*

$$S_{(C,\bar{\varphi})} = \left\{ [f]_{p^n} \in G_n \;\middle|\; [f]_p \in C,\ \left[f'\right]_p(x) = \frac{\varphi([f]_p(x))}{\varphi(x)} \right\}.$$

Example. A particularly easy to describe Sylow p-group of G_n is the one corresponding to (C, φ) where φ is a constant function and C the subgroup of S_p generated by $(0\ 1\ 2 \ldots p-1)$. It is the inverse image of S defined in Lemma 4.1 and it consists of the functions on $\mathbb{Z}_{p^n}$ induced by polynomials f such that the formal derivative f' induces the constant function 1 on $\mathbb{Z}_p$ and the function induced by f itself on $\mathbb{Z}_p$ is a power of $(0\ 1\ 2 \ldots p-1)$.

Combining Theorem 5.1 with Proposition 4.5 we obtain the following description of the intersection of all Sylow p-groups of G_n for odd p.

5.3 Corollary. *Let p be an odd prime.*

(i) *For $n \geqslant 2$ the intersection of all Sylow p-groups of G_n is the kernel of the projection $\pi: G \to H$.*
(ii) *Likewise, the intersection of all Sylow p-groups of G is the kernel of the canonical epimorphism of G onto H.*
(iii) *The intersection of all Sylow p-groups of G_n $(n \geqslant 2)$ can also be described as the normal subgroup*

$$N = \left\{ [f]_{p^n} \in G_n \;\middle|\; [f]_p = \iota,\ \left[f'\right]_p = 1 \right\},$$

where ι denotes the identity function on $\mathbb{Z}_p$. Its order is $p^p p^{\sum_{k=3}^{n} \beta(k)}$ and its index in G_n (for $n \geqslant 2$) is

$$[G_n : N] = p!(p-1)^p.$$

(iv) *Likewise, the index of the intersection of all Sylow p-subgroups of G in G is $p!(p-1)^p$.*

Proof. (i) and (ii) follow immediately from Theorem 5.1 and Proposition 4.5. To see (iii), let π be the projection from G_n to H (that is $\pi = \theta\pi_2 \ldots \pi_{n-1}$). Then N is the inverse image of $\{(\iota, 1)\}$, the identity element of H, under π, and is therefore the intersection of the Sylow p-groups of G_n by (i). As the kernel of a group homomorphism, N is a normal subgroup.

The order of N is the order of the kernel of π, which is the product of p^p (the order of the kernel of θ) and $p^{\beta(k)}$ (the order of the kernel of π_{k-1}) for $3 \leqslant k \leqslant n$. Finally, the index of the kernel of the homomorphism of G_n or G onto H is the order of H which is $p!(p-1)^p$. $\square$

Acknowledgments

The authors wish to thank W. Herfort for stimulating discussions.

References

[1] M. Bhargava, *P*-orderings and polynomial functions on arbitrary subsets of Dedekind rings, J. Reine Angew. Math. 490 (1997) 101–127.
[2] J.V. Brawley, G.L. Mullen, Functions and polynomials over Galois rings, J. Number Theory 41 (1992) 156–166.
[3] L. Carlitz, Functions and polynomials (mod p^n), Acta Arith. 9 (1964) 67–78.
[4] Z. Chen, On polynomial functions from $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_r}$ to $\mathbb{Z}_m$, Discrete Math. 162 (1996) 67–76.
[5] S. Frisch, When are weak permutation polynomials strong?, Finite Fields Appl. 1 (1995) 437–439.
[6] S. Frisch, Polynomial functions on finite commutative rings, in: D.E. Dobbs, et al. (Eds.), Advances in Commutative Ring Theory, in: Lect. Notes Pure Appl. Math., vol. 205, Dekker, New York, 1999, pp. 323–336.
[7] J. Jiang, A note on polynomial functions over finite commutative rings, Adv. Math. (China) 39 (2010) 555–560.
[8] J.J. Jiang, G.H. Peng, Q. Sun, Q. Zhang, On polynomial functions over finite commutative rings, Acta Math. Sin. (Engl. Ser.) 22 (2006) 1047–1050.
[9] G. Keller, F.R. Olson, Counting polynomial functions (mod p^n), Duke Math. J. 35 (1968) 835–838.
[10] A.J. Kempner, Polynomials and their residue systems, Trans. Amer. Math. Soc. 22 (1921) 240–266, 267–288.
[11] N.P. Liu, J.J. Jiang, Polynomial functions in n variables over a finite commutative ring, Sichuan Daxue Xuebao 46 (2009) 44–46.
[12] B.R. McDonald, Finite Rings with Identity, Dekker, 1974.
[13] A.A. Nechaev, Polynomial transformations of finite commutative local rings of principal ideals, Math. Notes 27 (1980) 425–432, transl. from Mat. Zametki 27 (1980) 885–897, 989.
[14] W. Nöbauer, Gruppen von Restpolynomidealrestklassen nach Primzahlpotenzen, Monatsh. Math. 59 (1955) 194–202.
[15] W. Nöbauer, Polynomfunktionen auf primen Restklassen, Arch. Math. (Basel) 39 (1982) 431–435.
[16] I.G. Rosenberg, Polynomial functions over finite rings, Glasg. Math. 10 (1975) 25–33.
[17] Q. Wei, Q. Zhang, On strong orthogonal systems and weak permutation polynomials over finite commutative rings, Finite Fields Appl. 13 (2007) 113–120.
[18] Q.J. Wei, Q.F. Zhang, On permutation polynomials in two variables over $\mathbb{Z}/p^2\mathbb{Z}$, Acta Math. Sin. (Engl. Ser.) 25 (2009) 1191–1200.
[19] Q. Zhang, Polynomial functions and permutation polynomials over some finite commutative rings, J. Number Theory 105 (2004) 192–202.