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

Sophie Frisch and Daniel Krenn

**Abstract.** We enumerate and describe the Sylow $p$-groups of the groups of polynomial permutations of the integers mod $p^n$ for $n \geq 1$ and of the pro-finite group which is the projective limit of these groups. MSC 2000: primary 20D20, secondary 11T06, 13M10, 11C08, 13F20, 20E18.

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

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

and

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

for $n \geq 3$,

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 $g: \mathbb{Z}_{p^n} \rightarrow \mathbb{Z}_{p^n}$ 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 $\mathbb{Z}_{p^n}$.

Sophie Frisch is supported by the Austrian Science Fund (FWF), grant P23245-N18.

Daniel Krenn is supported by the Austrian Science Fund (FWF), project W1230 doctoral program “Discrete Mathematics”.
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 $m \geq n$) 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

$$\alpha_p(n) = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor$$

and

$$\beta_p(n) = \min\{m \mid \alpha_p(m) \geq n\}.$$

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

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

**2.1 Fact.**

1. $\alpha_p(n) = v_p(n!)$.
2. For $1 \leq k \leq p$, $\beta_p(k) = kp$ and for $k > p$, $\beta_p(k) < kp$.
3. For all $n \in \mathbb{Z}$, $v_p((n)_k) \geq \alpha_p(k)$; 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 $n \geq 1$ is: 2, 4, 4, 6, 8, 8, 8, 10, 12, 12, 14, 16, 16, 16, 18, 20, 20, ...
The falling factorials \((x)_0 = 1, (x)_k = x(x-1)\ldots(x-k+1), k > 0,\) 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 \(a_k \equiv 0 \mod p^n - \alpha(k)\) 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 \(v_p((n)_k) \geq \alpha_p(k)\) 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 \(0 \leq a_k < p^{n-\alpha(k)}\) 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.** (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 \(\pi_n : F_{n+1} \rightarrow F_n\) the canonical projection.

1. For all \(n \geq 1\) and for each \(f \in F_n\) we have \(|\pi_n^{-1}(f)| = p^{\beta(n+1)}\).
2. For all \(n \geq 1,\) 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

\[
f(x) = f_0(x) + f_1(x)(x^p - x) + f_2(x)(x^p - x)^2 + \ldots + f_m(x)(x^p - x)^m + \ldots
\]

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

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

**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 \(f_k = g_k \mod p^{n-k}Z[x]\) for \(0 \leq k < n\). Then \(f \sim g\) implies \([f]_p^n = [g]_p^n\). There are \(p^{n+2p+3p+...+np}\) equivalence classes of \(\sim\) and \(p^{\beta(1)+\beta(2)+\beta(3)+...+\beta(n)}\) different \([f]_p^n\). For \(k \leq p\), \(\beta(k) = kp\). 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 \(Z[x]\).

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

\[ I_n = \{ f \in Z[x] \mid f(Z) \subseteq p^nZ \} \quad \text{and} \quad J_n = \{ (p^{n-k}(x^p - x)^k \mid 0 \leq k \leq n) \}. \]

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

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

2.7 Fact. (cf. McDonald [12]) Let \(n \geq 2\). The function on \(Z_p^n\) induced by a polynomial \(f \in Z[x]\) is a permutation if and only if

1. \(f\) induces a permutation of \(Z_p\) 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 \(f \in Z[x]\) on \(Z_p^n\) and \(Z_p\), respectively, and \([f']_p\) the function defined by the formal derivative of \(f\) on \(Z_p\). Then

1. \([f]_p^2\) determines not just \([f]_p\), but also \([f']_p\).
2. Let \(n \geq 2\). Then \([f]_p^n\) is a permutation if and only if \([f]_p^2\) is a permutation.
3. For every pair of functions \((\alpha, \beta)\), \(\alpha : Z_p \to Z_p\), \(\beta : Z_p \to Z_p\), there are exactly \(p^p\) polynomial functions \([f]_p^2\) on \(Z_p^2\) with \([f]_p = \alpha\) and \([f']_p = \beta\).
4. For every pair of functions \((\alpha, \beta)\), \(\alpha : Z_p \to Z_p\) bijective, \(\beta : Z_p \to Z_p \setminus \{0\}\), there are exactly \(p^p\) polynomial permutations \([f]_p^2\) on \(Z_p^2\) 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 \( n \geq 1 \), the image of \( G_{n+1} \) under \( \pi_n : F_{n+1} \to F_n \) is contained in \( G_n \) and
(2) for all \( n \geq 2 \), 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 \( \pi_n \) 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 \( n \geq 2 \), 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

\[
|\ker(\pi_n)| = p^{\beta(n+1)}.
\]

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

\[
|G_2| = p!(p-1)^pp^p,
\]

and for \( n \geq 3 \) the number of polynomial permutations on \( \mathbb{Z}_{p^2} \) is

\[
|G_n| = p!(p-1)^pp^p\sum_{k=3}^{n}e^k
\]

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 \( |G_2| = p!(p-1)^pp^p \). 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 \( n \geq 2 \).

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 \( \psi \theta = \pi_1 \).
The restrictions of $\theta$ to $G_2$ and of $\psi$ 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 $G_i$.

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 $\theta$ and $\psi$.

**Definition.** We define the semi-group $(E, \circ)$ 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 $\iota$ denoting the identity function on $\mathbb{Z}_p$ and 1 the constant function 1.

(2) The group of units of $E$ has the form

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

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

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

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 $\theta$ and $\psi$.

**Definition.** We define $\psi : E \to F_1$ by $\psi(f, f') = f$. As for $\theta : F_2 \to E$, given an element $[g]_{p^2} \in F_2$, set $\theta([g]_{p^2}) = ([g], [g']_{p^2})$. $\theta$ 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 $\theta$ 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 $\psi$ 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 $n \geq 2$ 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 $(0 1 2 \ldots p-1)$. 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

$$N_H(S) = \{(g, g') \mid g \in N_{S_p}(C_0), \; g' \text{ a non-zero constant }\}.$$
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 $[H : N_H(S)] = (p - 1)!p^{p-2}$.

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

$$g\sigma g^{-1} = (g(0) \; g(1) \; g(2) \ldots g(p - 1))$$

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

$$(g(0) \; g(1) \; g(2) \ldots g(p - 1)) = (0 \; k \; 2k \ldots (p - 1)k),$$

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 $(p - 1)!p^{p-2}$ 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 $S_p$, $\varphi : \mathbb{Z}_p \rightarrow \mathbb{Z}_p \setminus \{0\}$.
is a function and $\bar{\varphi}$ is the class of $\varphi$ with respect to the equivalence relation of multiplication by a non-zero constant. The subgroup corresponding to $(C, \bar{\varphi})$ is

$$S_{(C, \varphi)} = \{ (f, f') \in H \mid f \in C, f'(x) = \frac{\varphi(f(x))}{\varphi(x)} \}.$$ 

Proof. Observe that each $S_{(C, \varphi)}$ is a subgroup of order $p$ of $H$. Different pairs $(C, \bar{\varphi})$ give rise to different groups: Suppose $S_{(C, \varphi)} = S_{(D, \bar{\psi})}$. 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 nonzero $k \in \mathbb{Z}_p$.

There are $(p-2)!$ cyclic subgroups of order $p$ of $S_p$, and $(p-1)^{p-1}$ equivalence classes $\bar{\varphi}$ of functions $\varphi : \mathbb{Z}_p \to \mathbb{Z}_p \setminus \{0\}$. 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. \(\square\)

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

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

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 $(f, f') \in \bigcap_{(C, \varphi)} S_{(C, \bar{\varphi})}$. Suppose $f$ is not the identity function and let $k \in \mathbb{Z}_p$ such that $f(k) \neq k$.

Note that $\varphi$ in $(C, \bar{\varphi})$ is arbitrary, apart from the fact that $0$ is not in the image. Therefore, and because $p \geq 3$, among the various $\varphi$ there occur functions $\vartheta$ and $\eta$ 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 $p \geq 5$, the lemma above can be proved in a simpler way: There is more than one cyclic group of order $p$, so for $(f, f') \in \bigcap_{(C, \varphi)} S_{(C, \varphi)}$, 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 $G$

Again we consider the projective system of finite groups

$$G_1 \leftarrow H \leftarrow G_2 \leftarrow \cdots \leftarrow G_n \leftarrow H$$

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 $n \geq 2$ 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 $\pi : G_n \rightarrow H$, with $\pi = \theta \pi_2 \cdots \pi_{n-1}$.

(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 $\pi : G \rightarrow H$.

Proof. In the projective system $G_1 \leftarrow H \leftarrow G_2 \leftarrow \cdots \leftarrow G_n$, the kernel of the group epimorphism $G_n \rightarrow H$ is a finite $p$-group for every $n \geq 2$, because for $n \geq 2$ the kernel of $\pi_n : G_{n+1} \rightarrow G_n$ is of order $p^{\beta(n+1)}$ by Corollary 2.10, and the kernel of $\theta : G_2 \rightarrow H$ is of order $p^\beta$ by Lemma 3.2 (iii). So the Sylow $p$-groups of $G_n$ for $n \geq 2$ 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. □

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 $m \geq n$).
5.2 Corollary. Let \( n \geq 2 \). 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 \((C, \varphi)\), 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
\[
S_{(C, \bar{\varphi})} = \{ [f]_{p^n} \in G_n \mid [f]_p \in C, [f']_p(x) = \frac{\varphi([f]_p(x))}{\varphi(x)} \}.
\]

Example. A particularly easy to describe Sylow \( p \)-group of \( G_n \) is the one corresponding to \((C, \varphi)\) where \( \psi \) 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 \( n \geq 2 \) 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 \( G_n \) \((n \geq 2)\) can also be described as the normal subgroup
\[
N = \{ [f]_{p^n} \in G_n \mid [f]_p = \iota, [f']_p = 1 \},
\]
where \( \iota \) denotes the identity function on \( \mathbb{Z}_p \). Its order is \( p^np^{\sum_{k=3}^{n} \beta(k)} \) and its index in \( G_n \) \((\text{for } n \geq 2)\) 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 \( \pi \) be the projection from \( G_n \) to \( H \) \((\text{that is } \pi = \theta \pi_2 \ldots \pi_{n-1})\). Then \( N \) is the inverse image of \( \{(\iota, 1)\} \), the identity element of \( H \), under \( \pi \), 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 \( \pi \), which is the product of \( p^\alpha \) (the order of the kernel of \( \theta \)) and \( p^\beta(k) \) (the order of the kernel of \( \pi_{k-1} \)) for \( 3 \leq k \leq n \). Finally, the index of the kernel of the homomorphism of \( G_n \) or \( G \) onto \( H \) is the order of \( H \) which is \( p!(p-1)^p \). \( \square \)

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

References


[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), pp. 67–76.


S. F.
Institut für Mathematik A
Technische Universität Graz
Steyrergasse 30
A-8010 Graz, Austria
frisch@tugraz.at

D. K.
Institut für Mathematik B
Technische Universität Graz
Steyrergasse 30
A-8010 Graz, Austria
krenn@math.tugraz.at