Honam Mathematical J. **34** (2012), No. 4, pp. 483–494
http://dx.doi.org/10.5831/HMJ.2012.34.4.483

GROUP OF POLYNOMIAL PERMUTATIONS OF $\mathbb{Z}_{p^r}$

Kwankyu Lee and Heisook Lee

Abstract. The set of all polynomial permutations of $\mathbb{Z}_{p^r}$ forms a group. We investigate the structure of the group and some related groups, and completely determine the structure of the group of all polynomial permutations of $\mathbb{Z}_{p^2}$.

1. Introduction

Let p^r be a prime power. If a polynomial over the Galois ring $\mathbb{Z}_{p^r}$ induces a permutation of $\mathbb{Z}_{p^r}$, then it is called a *permutation polynomial.* For $r = 1$, it is well-known that every permutation of the field $\mathbb{Z}_p$ is induced by a polynomial [4]. On the other hand, for $r > 1$, not every permutation of $\mathbb{Z}_{p^r}$ is induced by a polynomial. Hence the notion of a *polynomial permutation*, that is, permutation induced by a polynomial is meaningful in this case.

It is easy to see that the set of all polynomial permutations of $\mathbb{Z}_{p^r}$ is a group. Indeed the set of all polynomial permutations of $\mathbb{Z}_{p^r}$ is clearly closed under composition and is a finite subset of the symmetric group of $\mathbb{Z}_{p^r}$, and hence forms a subgroup. We investigate the structure of this group and related groups. In particular, we completely determine the structure of the group of all polynomial permutations of $\mathbb{Z}_{p^2}$. Along the way, we review some known results about polynomial permutations and in general polynomial functions of $\mathbb{Z}_{p^r}$, giving simpler proofs than in literature.

Let us consider the set $\mathcal{P}_{p^r}$ of all permutation polynomials in $\mathbb{Z}_{p^r}[x]$ and the set V_{p^r} of all polynomials in $\mathbb{Z}_{p^r}[x]$ inducing the zero function on $\mathbb{Z}_{p^r}$. Let

$$P_{p^r} = \{\overline{f(x)} \mid f(x) \in \mathcal{P}_{p^r}\},$$

Received July 23, 2012. Accepted September 5, 2012.
2010 Mathematics Subject Classification. Primary 05A05, 20B35, 11T06.
Key words and phrases. polynomial permutation, Galois ring, permutation group.

where $\overline{f(x)} = f(x) + V_{p^r}$. Then P_{p^r} is a monoid under polynomial composition, naturally isomorphic to the group of all polynomial permutations of $\mathbb{Z}_{p^r}$. Thus our object of study is P_{p^r}. We write $f(x) \approx g(x)$ when two polynomials induce the same function on the base ring.

2. Preliminaries

Let m be a positive integer. Several authors [3, 5, 8] presented somewhat complicated proofs for the following result.

Theorem 2.1. *Let m be a positive integer. Let $f(x) \in \mathbb{Z}_m[x]$. Then $f(x)$ induces the zero function on $\mathbb{Z}_m$ if and only if it can be written in the form*

$$f(x) = \sum_{n=0}^{\infty} \frac{a_n m}{\gcd(n!, m)} x^{\underline{n}}, \qquad 0 \le a_n < \gcd(n!, m),$$

where $x^{\underline{n}}$ denotes the falling power $x(x-1)\cdots(x-n+1)$.

Proof. Note that a polynomial can be expressed uniquely as $f(x) = \sum_{n=0}^{\infty} b_n x^{\underline{n}}$ with $b_n \in \mathbb{Z}_m$. So $f(x)$ induces the zero function on $\mathbb{Z}_m$ if and only if

$$f(k) = \sum_{n=0}^{k} b_n k^{\underline{n}} = 0 \quad \text{for all } k \ge 0. \tag{1}$$

Note that $b_k k!$ divides $b_k n^{\underline{k}}$ as the binomial coefficient $\binom{n}{k} = n^{\underline{k}}/k!$ is an integer. Thus a condition equivalent to (1) is for the coefficients b_k to satisfy $b_k k! = 0$ in $\mathbb{Z}_m$ for all $k \ge 0$. Since all solutions of the last equation are

$$b_k = \frac{am}{\gcd(k!, m)}, \quad 0 \le a < \gcd(k!, m),$$

we obtain the result. □

Corollary 2.2. *Every polynomial function on $\mathbb{Z}_m$ has a unique polynomial representation of the form*

$$f(x) = \sum_{n=0}^{m-1} b_n x^n, \qquad 0 \le b_n < \frac{m}{\gcd(n!, m)}.$$

Carlitz [1] gave several characterizations of polynomial functions on $\mathbb{Z}_{p^r}$. In particular, his Theorem 3 gives a characterization most interesting to us, but it is proved in an indirect way. We give a constructive proof of the result in a slightly modified form.

Theorem 2.3. *A function χ on $\mathbb{Z}_{p^r}$ is induced by a polynomial over $\mathbb{Z}_{p^r}$ if and only if there are some functions $\chi_i : \mathbb{Z}_p \to \mathbb{Z}_{p^r}$, $0 \le i \le r-1$ such that*

$$\chi(c+kp) = \sum_{i=0}^{r-1} (kp)^i \chi_i(c) \tag{2}$$

for all $0 \le c < p$, $0 \le k < p^{r-1}$. If a polynomial $f(x)$ induces χ, then $f(c) = \chi_0(c)$ and $f'(c) \equiv \chi_1(c) \pmod p$ for $0 \le c < p$.

Proof. Let $0 \le c < p$, $0 \le k < p^{r-1}$ throughout. Suppose χ is induced by a polynomial $f(x)$. Then

$$\chi(c+kp) = f(c+kp) = \sum_{i=0}^{r-1} (kp)^i \frac{f^{(i)}(c)}{i!} \tag{3}$$

for each $k \ge 0$. It is easy to see that $\frac{f^{(i)}(x)}{i!}$ is in fact a polynomial over $\mathbb{Z}$. Therefore we can take χ_i defined by $\chi_i(c) = f^{(i)}(c)/i!$ for $0 \le c < p$ and $0 \le i \le r-1$.

To prove the converse, let χ be a function on $\mathbb{Z}_{p^r}$ satisfying (2). Carlitz's interpolation formula [1] says that for $0 \le c < p$, the polynomial $L_c(x) = (1-(x-c)^{p-1})^{p^{r-1}}$ over $\mathbb{Z}_{p^r}$ satisfies

$$L_c(a) = \begin{cases} 1 & \text{if } a \equiv c \pmod p, \\ 0 & \text{if } a \not\equiv c \pmod p. \end{cases}$$

for $a \in \mathbb{Z}_{p^r}$. Now let $f_i(x) = \sum_{e=0}^{p-1} \chi_i(e) L_e(x)$ for $0 \le i \le r-1$. Note that $f_i(c+kp) = \chi_i(c)$. Let $g(x) = x - \sum_{e=0}^{p-1} eL_e(x)$. Note that $g(c+kp) = kp$. Finally we define a polynomial $f(x) = \sum_{i=0}^{r-1} g(x)^i f_i(x)$. The polynomial $f(x)$ indeed induces χ on $\mathbb{Z}_{p^r}$ since

$$f(c+kp) = \sum_{i=0}^{r-1} g(c+kp)^i f_i(c+kp) = \sum_{i=0}^{r-1} (kp)^i \chi_i(c) = \chi(c+kp).$$

Finally suppose a polynomial $f(x)$ induces χ. We have $f(c) = \chi(c) = \chi_0(c)$, and $f(c+p) \equiv \chi_0(c) + p\chi_1(c) \pmod{p^2}$. Hence

$$f(c+p) - f(c) \equiv p\chi_1(c) \pmod{p^2}$$

On the other hand by (3),

$$f(c+p) - f(c) \equiv f(c) + pf'(c) - f(c) = pf'(c) \pmod{p^2}.$$

Therefore $pf'(c) \equiv p\chi_1(c) \pmod{p^2}$, and hence $f'(c) \equiv \chi_1(c) \pmod p$. $\square$

For $f(x) \in \mathbb{Z}_{p^r}[x]$, let $\bar{f}(x)$ denote the polynomial in $\mathbb{Z}_p[x]$ obtained from $f(x)$ by reducing the coefficients modulo p. Keller and Olson [3] observed that the following theorem is a direct consequence of Theorem 123 in [2].

Theorem 2.4. *Let $f(x)$ be a polynomial in $\mathbb{Z}_{p^r}[x]$. Then $f(x)$ induces a permutation of $\mathbb{Z}_{p^r}$ if and only if $\bar{f}(x)$ induces a permutation of $\mathbb{Z}_p$ and $\bar{f}'(c) \neq 0$ for every c in $\mathbb{Z}_p$.*

A characterization of permutation polynomials over $\mathbb{Z}_{2^r}$ by Rivest [7] is a consequence of the above theorem. Using the same result, Keller and Olson [3] and Mullen and Stevens [5] counted the number of polynomial permutations of $\mathbb{Z}_{p^r}$. See Theorem 2.7.

Lemma 2.5. *For $r \geq 2p$, $(x^{\underline{r}})' \approx 0$ over $\mathbb{Z}_p$. For $p \leq r < 2p$, $(x^{\underline{r}})' \approx -x^{\underline{r-p}}$ over $\mathbb{Z}_p$.*

Proof. Note that $(x^{\underline{r}})' = \sum_{i=0}^{r-1} x^{\underline{i}}(x-i-1)^{\underline{r-1-i}}$. If $r \geq 2p$, then $i \geq p$ or $r-1-i \geq p$ so that $(x^{\underline{r}})' \approx 0$. Note that $x^{\underline{p}} - (x^p - x) = 0$ in $\mathbb{Z}_p[x]$ because the left side is a polynomial of degree $< p$ vanishing on $\mathbb{Z}_p$. Therefore if $p \leq r < 2p$, then

$$\begin{aligned}(x^{\underline{r}})' &= (x^{\underline{p}}(x-p)^{\underline{r-p}})' = ((x^p - x)x^{\underline{r-p}})' \\ &= -x^{\underline{r-p}} + (x^p - x)(x^{\underline{r-p}})' \approx -x^{\underline{r-p}}.\end{aligned}$$

□

Lemma 2.6. *Let $s \geq 2p$. There are $p!(p-1)^p p^{s-2p}$ number of polynomials $f(x) \in \mathbb{Z}_p[x]$ of degree $< s$ inducing a permutation of $\mathbb{Z}_p$ and $f'(c) \neq 0$ for every $c \in \mathbb{Z}_p$.*

Proof. Let $f(x) = a_0 + a_1 x^{\underline{1}} + a_2 x^{\underline{2}} + \cdots + a_{s-1} x^{\underline{s-1}} \in \mathbb{Z}_p[x]$. Then

$$\begin{aligned}f(x) &\approx a_0 + a_1 x^{\underline{1}} + a_2 x^{\underline{2}} + \cdots + a_{p-1} x^{\underline{p-1}}, \\ f'(x) &\approx a_1 + a_2 (x^{\underline{2}})' + \cdots + a_{p-1}(x^{\underline{p-1}})' \\ &\quad - a_p - a_{p+1} x - a_{p+2} x^{\underline{2}} - \cdots - a_{2p-1} x^{\underline{p-1}}.\end{aligned}$$

Hence

$$\begin{aligned}
f'(0) &= (a_1 + \cdots + a_{p-1}(x^{\underline{p-1}})')_{|x=0} - a_p,\\
f'(1) &= (a_1 + \cdots + a_{p-1}(x^{\underline{p-1}})')_{|x=1} - a_p - a_{p+1},\\
f'(2) &= (a_1 + \cdots + a_{p-1}(x^{\underline{p-1}})')_{|x=2} - a_p - a_{p+1}2 - a_{p+2}2!,\\
&\vdots\\
f'(p-1) &= (a_1 + \cdots + a_{p-1}(x^{\underline{p-1}})')_{|x=p-1} - a_p - \cdots - a_{2p-1}(p-1)!.
\end{aligned}$$

Because there are $p!$ polynomial permutations of $\mathbb{Z}_p$, there are $p!$ choices of the coefficients $a_0, a_1, \ldots, a_{p-1}$ for $f(x)$ to induce a permutation of $\mathbb{Z}_p$. For $f'(x)$ not to vanish on $\mathbb{Z}_p$, there are $p-1$ choices for each coefficient $a_p, a_{p+1}, \ldots, a_{2p-1}$. And the coefficient a_r for $r \geq 2p$ can be chosen arbitrarily in $\mathbb{Z}_p$. Thus we get the number. □

Theorem 2.7. *Let $r \geq 2$. The number of polynomial permutations of $\mathbb{Z}_{p^r}$ is*

$$\frac{p!(p-1)^p p^{rp^r-2p}}{\prod_{n=0}^{p^r-1} \gcd(n!, p^r)}. \tag{4}$$

Proof. Every polynomial permutation of $\mathbb{Z}_{p^r}$ is induced by a polynomial of degree $< p^r$. A polynomial $f(x)$ of degree $< p^r$ induces a permutation of $\mathbb{Z}_{p^r}$ if and only if $\bar{f}(x)$ is one of the $p!(p-1)^p p^{p^r-2p}$ number of polynomials satisfying the condition in Theorem 2.4. It follows that there are $p!(p-1)^p p^{p^r-2p} \times p^{(r-1)p^r}$ number of polynomials $f(x)$ of degree $< p^r$ inducing a permutation of $\mathbb{Z}_{p^r}$. But theses polynomials are divided into classes such that $\prod_{n=0}^{p^r-1} \gcd(n!, p^r)$ number of polynomials in the same class induce the same function on $\mathbb{Z}_{p^r}$ by Theorem 2.1. □

3. The group of basic permutation polynomials

In view of Theorem 2.4, we define a *basic permutation polynomial* $f(x)$ in $\mathbb{Z}_p[x]$ as a permutation polynomial over $\mathbb{Z}_p$ such that its derivative $f'(x)$ never vanishes on $\mathbb{Z}_p$. We denote by $\mathcal{B}_p$ the set of all basic permutation polynomials.

Lemma 3.1. *Let $f(x)$ be a polynomial in $\mathbb{Z}_p[x]$. Both of $f(x)$ and $f'(x)$ induce the zero function on $\mathbb{Z}_p$ if and only if $f(x) = h(x)(x^p - x)^2$ with some $h(x)$ in $\mathbb{Z}_p[x]$.*

Proof. If $f(x) = h(x)(x^p - x)^2$, then $f'(x) = h'(x)(x^p - x)^2 - 2h(x)(x^p - x)$, and hence $f(x) \approx 0$ and $f'(x) \approx 0$ on $\mathbb{Z}_p$.

Let us suppose conversely, and write $f(x) = \sum_{n\geq 0} a_n x^{\underline{n}}$. Then

$$f(x) \approx a_0 + a_1 x + a_2 x^{\underline{2}} + \cdots + a_{p-1} x^{\underline{p-1}}.$$

As $f(x) \approx 0$, it follows that $a_0 = a_1 = \cdots = a_{p-1} = 0$. Now by Lemma 2.5,

$$f'(x) = \sum_{n\geq p} a_n (x^{\underline{n}})' \approx -a_p - a_{p+1} x - a_{p+2} x^{\underline{2}} - \cdots - a_{2p-1} x^{\underline{p-1}}.$$

As $f'(x) \approx 0$, we also have $a_p = a_{p+1} = \cdots = a_{2p-1} = 0$. Hence

$$f(x) = \sum_{n\geq 2p} x^{\underline{n}} = \sum_{n\geq 2p} x^{\underline{p}} (x-p)^{\underline{p}} (x-2p) x^{\underline{n-2p}} = (x^p - x)^2 \sum_{n\geq 2p} x^{\underline{n-2p}}.$$

$\square$

Lemma 3.2. *Let $r \geq 2$. If $f(x) \in \mathbb{Z}_{p^r}[x]$ induces the zero function on $\mathbb{Z}_{p^r}$, then $\bar{f}(x) = h(x)(x^p - x)^2$ for some $h(x)$ in $\mathbb{Z}_p[x]$.*

Proof. Suppose $f(x) \approx 0$ on $\mathbb{Z}_{p^r}$. Then by Theorem 2.1, we can write

$$f(x) = a_p p^{r-1} x^{\underline{p}} + a_{p+1} p^{r-1} x^{\underline{p+1}} + \cdots + a_{2p-1} p^{r-1} x^{\underline{2p-1}} + \sum_{n\geq 2p} a_n x^{\underline{n}}.$$

Therefore $\bar{f}(x) = \sum_{n\geq 2p} a_n x^{\underline{n}} = (x^p - x)^2 \sum_{n\geq 2p} a_n x^{\underline{n-2p}}$. $\square$

We define

$$B_p = \{\overline{f(x)} \mid f(x) \in \mathcal{B}_p\}$$

where $\overline{f(x)}$ denotes the set $\{f(x) + h(x)(x^p - x)^2 \mid h(x) \in \mathbb{Z}_p[x]\}$. By Lemma 3.1, note that $\overline{f(x)} = \overline{g(x)}$ if and only if $f(x)$ and $g(x)$ are basic permutation polynomials inducing the same permutation of $\mathbb{Z}_p$ and their derivatives also induce the same nonvanishing function on $\mathbb{Z}_p$.

Lemma 3.3. *B_p is a group under polynomial composition. Let $r \geq 2$. We have a surjective group homomorphism*

$$\varphi : P_{p^r} \to B_p$$

defined by reduction modulo p, that is $\overline{f(x)} \mapsto \overline{\bar{f}(x)}$.

Proof. We first show that polynomial composition gives a well-defined operation on B_p. Let $\overline{f_1(x)} = \overline{g_1(x)}$ and $\overline{f_2(x)} = \overline{g_2(x)}$ so that

$$f_1(x) = g_1(x) + h_1(x)(x^p - x)^2,$$
$$f_2(x) = g_2(x) + h_2(x)(x^p - x)^2$$

for some $h_1(x)$ and $h_2(x)$ in $\mathbb{Z}_p[x]$. Note that $f_2 \circ f_1(x)$ is in $\mathcal{B}_p$ since $f_2 \circ f_1(x)$ induces a permutation of $\mathbb{Z}_p$ and

$$(f_2 \circ f_1)'(x) = f_2'(f_1(x))f_1'(x)$$

does not vanish on $\mathbb{Z}_p$. Similarly $g_2 \circ g_1(x)$ is in $\mathcal{B}_p$. Note that $f_2(f_1(x))$ and $g_2(g_1(x))$ induce the same function on $\mathbb{Z}_p$, and so do their derivatives $f_2'(f_1(x))f_1'(x)$ and $g_2'(g_1(x))g_1'(x)$. Therefore by Lemma 3.1, there is a polynomial $h(x)$ such that

$$f_2 \circ f_1(x) - g_2 \circ g_1(x) = h(x)(x^p - x)^2.$$

This verifies that polynomial composition gives a well-defined operation on B_p. Hence B_p is a monoid with identity $\overline{x}$.

By Theorem 2.4 and Lemma 3.2, the natural map

$$\varphi : P_{p^r} \to B_p$$

is well-defined and a surjective monoid homomorphism from a group to a monoid. It follows that B_p is in fact a group, and φ is a group homomorphism. $\square$

Through the following series of lemmas, we reveal the structure of the group B_p completely. See Theorem 3.7.

Lemma 3.4. *We have a surjective group homomorphism*

$$\psi : B_p \to P_p$$

defined by $\overline{f(x)} \mapsto \overline{f(x)}$.

Proof. It is clear that ψ is a well-defined group homomorphism. To see ψ is surjective, observe that if

$$f(x) = a_0 + a_1 x^{\underline{1}} + \cdots + a_{p-1} x^{\underline{p-1}}$$

is a permutation polynomial over $\mathbb{Z}_p$, then we can find $a_p, a_{p+1}, \ldots, a_{2p-1}$ in $\mathbb{Z}_p$ such that the polynomial

$$g(x) = a_0 + a_1 x^{\underline{1}} + \cdots + a_{p-1} x^{\underline{p-1}} + a_p x^{\underline{p}} + \cdots + a_{2p-1} x^{\underline{2p-1}}$$

is a basic permutation polynomial. Indeed $a_p, a_{p+1}, \dots, a_{2p-1}$ are chosen successively to satisfy

$$\begin{aligned}
g'(0) &= (a_1 + \cdots + a_{p-1}(x^{\underline{p-1}})')_{|x=0} - a_p \neq 0,\\
g'(1) &= (a_1 + \cdots + a_{p-1}(x^{\underline{p-1}})')_{|x=1} - a_p - a_{p+1} \neq 0,\\
g'(2) &= (a_1 + \cdots + a_{p-1}(x^{\underline{p-1}})')_{|x=2} - a_p - a_{p+1}2 - a_{p+2}2! \neq 0,\\
&\vdots\\
g'(p-1) &= (a_1 + \cdots + a_{p-1}(x^{\underline{p-1}})')_{|x=p-1} - a_p - \cdots - a_{2p-1}(p-1)! \neq 0.
\end{aligned}$$

Then $g(x) \approx f(x)$, and $\psi(\overline{g(x)}) = \overline{f(x)}$. $\square$

Let us define

$$M_p = \text{group of all functions from } \mathbb{Z}_p \to \mathbb{Z}_p^\times$$

under usual pointwise multiplication operation. Note that M_p is isomorphic to $(\mathbb{Z}_p^\times)^p$, p-times direct product of the cyclic group $\mathbb{Z}_p^\times$.

Lemma 3.5. *The kernel of ψ is isomorphic to M_p.*

Proof. Define $\lambda : \ker\psi \to M_p$ by mapping $\overline{f(x)}$ to the function τ on $\mathbb{Z}_p$ induced by $f'(x)$. It is clearly well-defined. To see λ is a group homomorphism, observe that for $\overline{f(x)}, \overline{g(x)}$ in $\ker\psi$,

$$(f \circ g)'(x) = f'(g(x))g'(x) \approx f'(x)g'(x)$$

because $g(x)$ induces the identity permutation on $\mathbb{Z}_p$, and hence $\lambda(\overline{f \circ g(x)}) = \lambda(\overline{f(x)})\lambda(\overline{g(x)})$. Injectivity is clear. Finally to show that λ is surjective, let τ be a function in M_p. Let $f(x) = x + h(x)(x^p - x)$ where $h(x)$ is a polynomial of degree $< p$ we now determine. Since $f'(x) \approx 1 - h(x)$, we need to have $h(c) = 1 - \tau(c)$ for every $c \in \mathbb{Z}_p$. There is a unique polynomial $h(x)$ of degree $< p$ satisfying this condition. With this $h(x)$, we have $\overline{f(x)} \mapsto \tau$. $\square$

Lemma 3.6. *The exact sequence*

$$1 \longrightarrow \ker\psi \longrightarrow B_p \xrightarrow{\psi} P_p \longrightarrow 1$$

splits. Hence B_p is the semidirect product of P_p and $\ker\psi$.

Proof. We now define a homomorphism $\rho : P_p \to B_p$ such that $\psi \circ \rho$ is the identity on P_p. Let $\overline{g(x)} \in P_p$. Let $f(x) = g(x) + (g'(x) - 1)(x^p - x)$. Then $f(x) \approx g(x)$ and $f'(x) = 1 + g''(x)(x^p - x) \approx 1$. Therefore $f(x)$ is a basic permutation polynomial. Thus we define $\rho : P_p \to B_p$ by $\overline{g(x)} \mapsto \overline{f(x)}$. Then $\rho : P_p \to B_p$ is a well-defined group homomorphism.

Suppose $\rho(\overline{g(x)}) = \overline{f(x)}$ with $\overline{g(x)} \in P_p$. Then by the definition of ρ, $f(x)$ and $g(x)$ induce the same function on $\mathbb{Z}_p$. Therefore $\psi(\overline{f(x)}) = \overline{g(x)}$. Hence $\psi \circ \rho$ is the identity on P_p. □

In Lemma 3.5, we saw $\ker \psi$ is isomorphic to M_p that is $(\mathbb{Z}_p^\times)^p$. Recall that P_p is isomorphic to

$$S_p = \text{symmetric group of } p \text{ letters},$$

because every permutation of $\mathbb{Z}_p$ is induced by a polynomial. Thus we obtain the following theorem that determines the structure of the group B_p.

Theorem 3.7. *B_p is isomorphic to the semidirect product $M_p \rtimes_\alpha S_p$ where $\alpha : S_p \to \mathrm{Aut}(M_p)$ is described by $\alpha(\sigma)(\tau) = \tau \circ \sigma$ for each $\sigma \in S_p$, $\tau \in M_p$.*

4. Group of polynomial permutations of $\mathbb{Z}_{p^r}$

From now on, we will regard the elements of P_{p^r} as functions on $\mathbb{Z}_{p^r}$ rather than equivalence classes of polynomials.

Let $r \geq 2$. We now show that there is a natural copy of B_p inside of P_{p^r}. Let $\overline{f(x)} \in B_p$. Let σ be the permutation of $\mathbb{Z}_p$ that $f(x)$ induces. Let τ be the nonvanishing function on $\mathbb{Z}_p$ that $f'(x)$ induces. We then define a permutation χ_f on $\mathbb{Z}_{p^r}$ by

$$\chi_f(a) = \sigma(c) + kp\tau(c) \tag{5}$$

for $a = c + kp$ in $\mathbb{Z}_{p^r}$. It is easy to see that χ_f is a permutation of $\mathbb{Z}_{p^r}$. By Theorem 2.3, it is then indeed a polynomial permutation. Define the map $\xi : B_p \to P_{p^r}$ by $\overline{f(x)} \mapsto \chi_f$.

Lemma 4.1. *The map $\xi : B_p \to P_{p^r}$ is an injective group homomorphism.*

Proof. Let $\overline{f_1(x)}$, $\overline{f_2(x)}$ be in B_p. Suppose $f_1(x)$, $f_1'(x)$ induce σ_1, τ_1 on $\mathbb{Z}_p$, respectively and $f_2(x)$, $f_2'(x)$ induce σ_2, τ_2 on $\mathbb{Z}_p$, respectively. Then $f_1 \circ f_2(x)$ induces $\sigma_1 \circ \sigma_2$ on $\mathbb{Z}_p$. and $(f_1 \circ f_2)'(x) = f_1'(f_2(x))f_2'(x)$ induces $(\tau_1 \circ \sigma_2)\tau_2$. Observe that for every $a = c + kp$ in $\mathbb{Z}_{p^r}$,

$$\begin{aligned}
\chi_{f_1} \circ \chi_{f_2}(a) &= \chi_{f_1}(\sigma_2(c) + kp\tau_2(c)) \\
&= \sigma_1(\sigma_2(c)) + kp\tau_2(c)\tau_1(\sigma_2(c)) \\
&= \sigma_1 \circ \sigma_2(c) + kp(\tau_1 \circ \sigma_2)(c)\tau_2(c) \\
&= \chi_{f_1 \circ f_2}(a).
\end{aligned}$$

Hence ξ is a group homomorphism. If χ_f is the identity permutation of $\mathbb{Z}_{p^r}$, then $\sigma(c) = c$ and $\tau(c) = 1$ for $0 \leq c < p$, so $\overline{f(x)}$ is the identity of B_p. Hence ξ is injective. $\square$

Lemma 4.2. *The exact sequence*

$$1 \longrightarrow \ker\varphi \longrightarrow P_{p^r} \xrightarrow{\varphi} B_p \longrightarrow 1$$

splits. Hence P_{p^r} is the semidirect product of B_p and $\ker\varphi$.

Proof. Let us show that the composition $\varphi \circ \xi$ is the identity on B_p. Let $\overline{f(x)}$ be in B_p. Let χ_f be the permutation of $\mathbb{Z}_{p^r}$ defined by (5). Suppose a polynomial $g(x)$ in $\mathbb{Z}_{p^r}[x]$ induces χ_f. Then by Theorem 2.3, $\bar{g}(x)$ and $\bar{g}'(x)$ induce σ and τ on $\mathbb{Z}_p$. Hence $\varphi(\chi_f) = \overline{f(x)}$. $\square$

The following theorem characterizes the polynomial permutations in $\ker\varphi$. Let ι denote the identity permutation of $\mathbb{Z}_{p^r}$.

Lemma 4.3. *A permutation χ of $\mathbb{Z}_{p^r}$ is in $\ker\varphi$ if and only if $\chi = \iota + \mu$ where μ is a polynomial function on $\mathbb{Z}_{p^r}$ satisfying $\mu(c) \equiv 0 \pmod p$ and $\mu(c+p) \equiv \mu(c) \pmod{p^2}$ for $0 \leq c < p$. The condition for μ is equivalent to that μ is induced by a polynomial $f(x)$ satisfying $f(c) \equiv f'(c) \equiv 0 \pmod p$ for $0 \leq c < p$.*

Proof. Let $0 \leq c < p$ and $0 \leq k < p^{r-1}$ throughout. Suppose $\chi \in \ker\varphi$. Then χ is induced by a polynomial $f(x)$ satisfying $f(c) \equiv c \pmod p$ and $f'(c) \equiv 1 \pmod p$. Since χ is a polynomial function, by Theorem 2.3, there exist $\chi_i : \mathbb{Z}_p \to \mathbb{Z}_{p^r}$ such that

$$\chi(c + kp) = \sum_{i=0}^{r-1} (kp)^i \chi_i(c),$$

and $f(c) = \chi_0(c)$ and $f'(c) \equiv \chi_1(c) \pmod p$. It follows that $\chi_0(c) \equiv c \pmod p$ and $\chi_1(c) \equiv 1 \pmod p$. So we can write $\chi_0(c) = c + p\tilde{\chi}_0(c)$ and $\chi_1(c) = 1 + p\tilde{\chi}_1(c)$. Then

$$\chi(c + kp) = c + p\tilde{\chi}_0(c) + kp(1 + p\tilde{\chi}_1(c)) + \sum_{i=2}^{r-1} (kp)^i \chi_i(c)$$

If we define μ by

$$\mu(c + kp) = \tilde{\chi}_0(c)p + (kp)\tilde{\chi}_1(c)p + \sum_{i=2}^{r-1} (kp)^i \chi_i(c),$$

then $\chi = \iota + \mu$ and μ is a polynomial function by Theorem 2.3 satisfying $\mu(c) \equiv 0 \pmod p$ and $\mu(c + p) \equiv \tilde{\chi}_0(c)p = \mu(c) \pmod{p^2}$.

The converse is proved by reversing the above argument. The equivalent condition for μ follows by Theorem 2.3. $\square$

Let $r = 2$. In this case, the structure of $\ker\varphi$ is particularly simple. Let

$$T_p = \text{group of all functions } \gamma : \mathbb{Z}_p \to \mathbb{Z}_p$$

with usual pointwise addition operation. Note that T_p is isomorphic to $(\mathbb{Z}_p)^p$, p-times direct product of the additive cyclic group $\mathbb{Z}_p$.

Lemma 4.4. *The subgroup* $\ker\varphi$ *of* P_{p^2} *is isomorphic to* T_p.

Proof. Let $0 \le c, k < p$ throughout. By Lemma 4.3, $\chi \in \ker\varphi$ if and only if $\chi = \iota + \mu$ where μ satisfies $\mu(c + kp) = \tilde{\mu}_0(c)p$ with an arbitrary function $\tilde{\mu}_0$ from $\mathbb{Z}_p$ to $\mathbb{Z}_p$. In other words, $\chi \in \ker\varphi$ if and only if $\chi(c + kp) = c + kp + p\gamma(c)$ with an an arbitrary function γ from $\mathbb{Z}_p$ to $\mathbb{Z}_p$. If $\chi_1(c + kp) = c + kp + p\gamma_1(c)$ and $\chi_2(c) = c + kp + p\gamma_2(c)$, then $\chi_2 \circ \chi_1(c + kp) = \chi_2(c + kp + p\gamma_1(c)) = c + kp + p\gamma_1(c) + p\gamma_2(c) = c + kp + p(\gamma_1(c) + \gamma_2(c))$. This shows that $\ker\varphi$ is isomorphic to the additive group T_p. $\square$

Theorem 4.5. *The group of polynomial permutations of* $\mathbb{Z}_{p^2}$ *is isomorphic to*

$$T_p \rtimes_\beta (M_p \rtimes_\alpha S_p),$$

where $\beta : M_p \rtimes_\alpha S_p \to \mathrm{Aut}(T_p)$ *is given by* $\beta(\tau, \sigma)(\gamma) = (\gamma\tau) \circ \sigma^{-1}$.

It follows that the order of the group P_{p^2} is $p^p(p-1)^p p!$, which is verified by Theorem 2.7. Moreover from Theorem 4.5, we see that a Sylow p-subgroup of P_{p^2} of order p^{p+1} is the same with that of the Sylow p-subgroup of the symmetric group S_{p^2}, namely the wreath product of the additive group $\mathbb{Z}_p$ with itself.

5. Remarks

We could determine the structure of P_{p^2} because of the simple structure of $\ker\varphi$ in the case $r = 2$. However for $r > 2$ cases, the structure of $\ker\varphi$ seems to be more complicated, and we could not resolve it yet. This remains as a future work.

Starting with [6], Nöbauer had studied polynomial permutations of $\mathbb{Z}_m$, from the same point of view with ours. However, it seems that there is no duplication among his and our works.

The first author was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education, Science and Technology(2009-0064770) and also by research fund from Chosun University, 2008. The second author was supported by Insitute of Mathematical Sciences at Ewha Womans University(2010).

Finally, the authors thank the reviewers for their valuable suggestions.

References

[1] L. Carlitz, *Functions and polynomials (mod p^n)*, Acta Arith. **9** (1964), 67–78.

[2] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers, fourth edition*, Oxford, 1960.

[3] G. Keller and F. R. Olson, *Counting polynomial functions* (mod p^n), Duke Math. Journal **35** (1968), 835–838.

[4] R. Lidl and H. Niederreiter, *Finite fields*, Addison-Wesley, 1983.

[5] G. Mullen and H. Stevens, *Polynomial functions* (mod m), Acta Math. Hung. **44** (1984), no. 3–4, 237–241.

[6] W. Nöbauer, *Über gruppen von restklassen nach restpolynomidealen*, Österreich. Akad. Wiss. Math.-Nat. Kl. S.-B. IIa. **162** (1953), 207–233.

[7] R. L. Rivest, *Permutation polynomials modulo* 2^w, Finite Fields Appl. **7** (2001), 287–292.

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

Kwankyu Lee
Department of Mathematics, Chosun University,
Gwangju 501-759, Korea.
E-mail: kwankyu@chosun.ac.kr

Heisook Lee
Department of Mathematics, Ewha Womans University,
Seoul 120-750, Korea.
E-mail: hsllee@ewha.ac.kr