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

HEISOOK LEE, HYUNJOO CHOI, AND KWANKYU 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. This study provides a group-theoretic perspective on some known results about polynomial permutations of $\mathbb{Z}_{p^r}$.

1. Introduction

Let p^r be a prime power. If a polynomial over $\mathbb{Z}_{p^r}$ induces a permutation of $\mathbb{Z}_{p^r}$, then it is called a *permutation polynomial* [4]. If $r = 1$, then it is well-known that every permutation of $\mathbb{Z}_p$ is induced by a polynomial. If $r > 1$, then not every permutation of $\mathbb{Z}_{p^r}$ is induced by a polynomial. Hence the concept of polynomial permutation becomes meaningful for $r > 1$ cases.

It is easily shown that the set of all polynomial permutations of $\mathbb{Z}_{p^r}$ forms a group, a subgroup of the group of all permutations of $\mathbb{Z}_{p^r}$. We investigate the structure of this group. Along the way, we review some known results about polynomial permutations and in general polynomial functions of $\mathbb{Z}_{p^r}$, and give simplified proofs for some of them.

2. Polynomial functions on $\mathbb{Z}_{p^r}$

Let m be a positive integer. Several authors [3, 5, 8] presented somewhat complicated proofs for the following result. So it seems worth while to repeat the result here with a short proof.

Theorem 2.1. *Let m be a positive integer. Let $f(x)$ be a polynomial 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*

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

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

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

2000 *Mathematics Subject Classification.* Primary 11T06.

Third author was supported by the Seoam Scholarship Foundation and by grant No. R01-2002-000-00083-0(2003) from the Basic Research Program of the Korea Science and Engineering Foundation.

if

$$\begin{aligned}
f(0) &= b_0 = 0,\\
f(1) &= 1!b_1 = 0,\\
f(2) &= 2b_1 + 2!b_2 = 0,\\
f(3) &= 3b_1 + 2\cdot 3b_2 + 3!b_3 = 0,\\
&\vdots\\
f(k) &= kb_1 + (k-1)kb_2 + (k-2)(k-1)kb_3 + \cdots + k!b_k = 0,\\
&\vdots
\end{aligned}$$

Note that for every positive integer k, $k!$ divides every product of k consecutive positive integers, as you see by noting that the binomial coefficient $x^{\underline{k}}/k!$ is an integer for integer x. Thus an equivalent condition is for the coefficients $b_0, b_1, \ldots$ to satisfy

$$\begin{aligned}
b_0 &= 0,\\
1!b_1 &= 0,\\
2!b_2 &= 0,\\
3!b_3 &= 0,\\
&\vdots\\
k!b_k &= 0,\\
&\vdots
\end{aligned}$$

in $\mathbb{Z}_m$. Solving these linear congruences modulo m, we obtain the result. □

Corollary 2.2. *There are* $\prod_{n=0}^{s-1}(n!, m)$ *number of polynomials of* $\deg f(x) < s$ *in* $\mathbb{Z}_m[x]$ *inducing the zero function on* $\mathbb{Z}_m$.

Proof. Count the number of possible choices of the s coefficients. □

Corollary 2.3. *Every polynomial function on* $\mathbb{Z}_m$ *has a unique polynomial representation*

$$f(x) = \sum_{n\geq 0} b_n x^n, \qquad 0 \leq b_n < \frac{m}{(n!, m)}.$$

Proof. We can repeatedly subtract from the given polynomial the polynomials inducing the zero function on $\mathbb{Z}_m$, to get the unique representation. □

Note that for a prime p, in particular, every (polynomial) function on $\mathbb{Z}_p$ is induced by a unique polynomial of degree $< p$.

Corollary 2.4. *There are* $\prod_{n=0}^{m-1} \frac{m}{(n!,m)}$ *distinct polynomial functions on* $\mathbb{Z}_m$.

Proof. This follows from the corollary above, noting that every polynomial function on $\mathbb{Z}_m$ is induced by a polynomial of degree $< m$. □

Carlitz gave several characterizations of polynomial functions on $\mathbb{Z}_{p^r}$ in [1]. In particular, his Theorem 3 gives a characterization most interesting to us, but he proved it in an indirect way. Fully using his Lagrange interpolation formula (see below), we give a direct and constructive proof of the result in a slightly modified form. First we recall two propositions.

Proposition 2.5. *Let $f(x) = \sum_{n\geq 0} a_n x^n$ be a polynomial over $\mathbb{Z}$. Then for $k = 0, 1, 2, \ldots,$*

$$\frac{f^{(k)}(x)}{k!} = \sum_{n\geq 0} a_{n+k}\binom{n+k}{k}x^n.$$

In particular, $\frac{f^{(k)}(x)}{k!}$ is a polynomial over $\mathbb{Z}$ for each $k \geq 0$.

Proof. Observe

$$f'(x) = \sum_{n\geq 1} a_n n x^{n-1} = \sum_{n\geq 0} a_{n+1}(n+1)x^n,$$

and

$$f''(x) = \sum_{n\geq 1} a_{n+1}(n+1)n x^{n-1} = \sum_{n\geq 0} a_{n+2}(n+2)(n+1)x^n.$$

Then we see the result follows by induction. □

Proposition 2.6. *Let $f(x)$ be a polynomial over $\mathbb{Z}$. Let $e \in \mathbb{Z}$. Then*

$$f(x+e) = \sum_{k\geq 0} e^k \frac{f^{(k)}(x)}{k!}.$$

Proof. Let $f(x) = \sum_{n\geq 0} a_n x^n$. Then

$$\begin{aligned} f(x+e) &= \sum_{n\geq 0} a_n (x+e)^n = \sum_{n\geq 0} a_n \sum_{k\geq 0}\binom{n}{k} e^k x^{n-k} \\ &= \sum_{k\geq 0} e^k \sum_{n\geq 0} a_n \binom{n}{k} x^{n-k} = \sum_{k\geq 0} e^k \sum_{n\geq 0} a_{n+k}\binom{n+k}{k}x^n \\ &= \sum_{k\geq 0} e^k \frac{f^{(k)}(x)}{k!}. \end{aligned}$$

□

Now we state and prove the theorem slightly modified from Carlitz's Theorem 3 in [1].

Theorem 2.7. *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 $\chi_i : \mathbb{Z}_p \to \mathbb{Z}_{p^r}$ $(i = 0, \ldots, r-1)$ such that*

$$\chi(c+kp) = \chi_0(c) + kp\chi_1(c) + (kp)^2\chi_2(c) + \cdots + (kp)^{r-1}\chi_{r-1}(c) \tag{2.1}$$

for $0 \leq c < p$, k arbitrary integer.

Proof. Suppose χ is induced by a polynomial $f(x)$. Then by Proposition 2.6,

$$\chi(c+kp) = f(c+kp) = f(c) + kpf'(c) + (kp)^2\frac{f''(c)}{2!} + \cdots + (kp)^{r-1}\frac{f^{(r-1)}(c)}{(r-1)!}$$

Therefore we can take χ_i defined by $\chi_i(c) = f^{(i)}(c)/i!$ for each $i = 0, 1, \ldots, r-1$.

To prove the converse, let χ be a function on $\mathbb{Z}_{p^r}$ satisfying (2.1). We construct a polynomial inducing χ in a way which we may call *Lagrange interpolation formula* on $\mathbb{Z}_{p^r}$ (see [1]). For each $0 \le c < p$, the polynomial $L_c(x) = (1-(x-c)^{p-1})^{p^{(r-1)}}$ satisfies

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

Now for each $i = 0, \ldots, r-1$, let $f_i(x) = \sum_{e=0}^{p-1} \chi_i(e) L_e(x)$. 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

$$f(x) = f_0(x) + g(x)f_1(x) + g(x)^2 f_2(x) + \cdots + g(x)^{r-1} f_{r-1}(x).$$

The polynomial $f(x)$ indeed induces χ on $\mathbb{Z}_{p^r}$ for

$$\begin{aligned} f(c+kp) &= f_0(c+kp) + g(c+kp)f_1(c+kp) + \cdots + g(c+kp)^{r-1} f_{r-1}(c+kp) \\ &= \chi_0(c) + kp\chi_1(c) + \cdots + (kp)^{r-1}\chi_{r-1}(c) \\ &= \chi(c+kp). \end{aligned}$$

This completes the proof. □

The following proposition will be used later.

Proposition 2.8. *Suppose a polynomial function χ on $\mathbb{Z}_{p^r}$ satisfies* (2.1). *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 $0 \le c < p$. We have $f(c) = \chi(c) = \chi_0(c)$. Next we observe

$$\begin{aligned} f(c+p) - f(c) &= \chi(c+p) - \chi(c) \\ &\equiv \chi_0(c) + p\chi_1(c) - \chi_0(c) = p\chi_1(c) \pmod{p^2} \end{aligned}$$

and by Proposition 2.6,

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

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

3. Polynomial permutations of $\mathbb{Z}_{p^r}$

We define some useful notations. For polynomials $f(x)$ and $g(x)$, we denote by $f \circ g(x)$ the composed polynomial of $f(x)$ and $g(x)$. If $f(x)$ is in $\mathbb{Z}_{p^r}[x]$, we denote by $\bar{f}(x)$ the polynomial in $\mathbb{Z}_p[x]$ obtained from $f(x)$ by reducing coefficients modulo p. For polynomials $f(x)$, $g(x)$ in $\mathbb{Z}_{p^r}[x]$, we write

$$f(x) \equiv g(x) \pmod{V}$$

if $f(x)$ and $g(x)$ induce the same function on $\mathbb{Z}_{p^r}$. Later we will define some groups as a set of equivalence classes. Then $\overline{f(x)}$ denotes the equivalence class with representative $f(x)$. These notations will be used throughout the rest of this paper.

As Keller and Olson observed in [3], the following theorem is a direct consequence of Theorem 123 in [2].

Theorem 3.1. *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 an easy result of the theorem above. On the other hand, based on the theorem above, Keller and Olson [3] and Mullen and Stevens [5] counted the number of polynomial permutations of $\mathbb{Z}_{p^r}$. Because their proof is much condensed, and their ideas employed in the proof are important for our own results in Section 4, we repeat the proof here. The essential idea is contained in the following lemma.

Lemma 3.2. *Let $s \geq 2p$. There are $p!(p-1)^p p^{s-2p}$ number of polynomials $f(x)$ in $\mathbb{Z}_p[x]$ inducing a permutation of $\mathbb{Z}_p$ and $f'(c) \neq 0$ for every $c \in \mathbb{Z}_p$.*

Proof. Let

$$f(x) = a_0 + a_1 x^{\underline{1}} + a_2 x^{\underline{2}} + \cdots + a_{s-1} x^{\underline{s-1}}$$

be a polynomial over $\mathbb{Z}_p$. 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 $r-i-1 \geq p$ so that $(x^{\underline{r}})' \equiv 0 \pmod{V}$.

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

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

Thus we see

$$\begin{aligned}
f'(x) \equiv\ & a_1 + a_2 (x^{\underline{2}})' + \cdots + a_{p-1}(x^{\underline{p-1}})' \\
& - a_p - a_{p+1} x - a_{p+2} x^{\underline{2}} - \cdots - a_{2p-1} x^{\underline{p-1}} \pmod{V}.
\end{aligned}$$

Then

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

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 $\mathbb{Z}_p$. With these considerations, the result follows. □

Theorem 3.3. *Let $r > 1$. The number of polynomial permutations of $\mathbb{Z}_{p^r}$ is*

$$\frac{p!(p-1)^p p^{rp^r-2p}}{\prod_{n=0}^{p^r-1}(n!, p^r)}. \tag{3.1}$$

Proof. As a consequence of Theorem 2.1, 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 3.1. 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 groups such that $\prod_{n=0}^{p^r-1}(n!, p^r)$ number of polynomials in the same group induce the same function on $\mathbb{Z}_{p^r}$ (Corollary 2.2). Therefore our conclusion follows. □

As an example, there are $p!(p-1)^p p^p$ number of polynomial permutations of $\mathbb{Z}_{p^2}$.

The following proposition computes the denominator of the formula (3.1). See Theorem 2.2 in [5].

Proposition 3.4. *If N is the smallest integer such that p^r divides $N!$. Then $\log_p \prod_{n=0}^{p^r-1}(n!, p^r)$ equals*

$$N \sum_{t \geq 1} \left\lfloor \frac{N}{p^t} \right\rfloor - \frac{1}{2} \sum_{t \geq 1} p^t \left\lfloor \frac{N}{p^t} \right\rfloor \left(\left\lfloor \frac{N}{p^t} \right\rfloor + 1 \right) + r(p^r - N).$$

Proof. Note that

$$(n!, p^r) = p^{\min\{\sum_{t \geq 1} \lfloor n/p^t \rfloor, r\}}.$$

Therefore

$$\begin{aligned}
\log_p \prod_{n=0}^{p^r-1} (n!, p^r) &= \sum_{n=0}^{p^r-1} \min \left\{ \sum_{t \geq 1} \left\lfloor \frac{n}{p^t} \right\rfloor, r \right\} \\
&= \sum_{n=0}^{N-1} \sum_{t \geq 1} \left\lfloor \frac{n}{p^t} \right\rfloor + \sum_{n=N}^{p^r-1} r \\
&= \sum_{t \geq 1} \sum_{n=0}^{N-1} \left\lfloor \frac{n}{p^t} \right\rfloor + r(p^r - N) \\
&= \sum_{t \geq 1} \left\lfloor \frac{N}{p^t} \right\rfloor \left(N - \frac{p^t}{2} \left(\left\lfloor \frac{N}{p^t} \right\rfloor + 1 \right) \right) + r(p^r - N).
\end{aligned}$$

□

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

We now begin to study the polynomial permutations of $\mathbb{Z}_{p^r}$, in group-theoretic point of view. For this approach, the following result is fundamental although trivially verified.

Theorem 4.1. *The set of all polynomial permutations of $\mathbb{Z}_{p^r}$ forms a group, a subgroup of all permutations of $\mathbb{Z}_{p^r}$.*

Proof. The composition of two polynomial permutations is again a polynomial permutation. Therefore the set of all polynomial permutations of $\mathbb{Z}_{p^r}$ is a finite subset, closed under composition, of the group of all permutations of $\mathbb{Z}_{p^r}$. Such a subset is always a subgroup. □

Let $PP(p^r)$ be the set of all permutation polynomials in $\mathbb{Z}_{p^r}[x]$ and $V(p^r)$ the set of all polynomials in $\mathbb{Z}_{p^r}[x]$ inducing the zero function on $\mathbb{Z}_{p^r}$. Note that two polynomials in $PP(p^r)$ induce the same permutation of $\mathbb{Z}_{p^r}$ if and only if their difference is in $V(p^r)$. We define $P(p^r)$ to be the set of all equivalence classes of $PP(p^r)$ modulo $V(p^r)$. Then

Theorem 4.2. *Under polynomial composition, $P(p^r)$ is a group, isomorphic to the group of all polynomial permutations over $\mathbb{Z}_{p^r}$.*

Proof. Clearly $P(p^r)$ is a monoid under polynomial composition. As monoids, $P(p^r)$ is naturally isomorphic to the group of all polynomial permutations of $\mathbb{Z}_{p^r}$. It follows that $P(p^r)$ itself is a group. □

With this result, we can say that our object of study is the group $P(p^r)$.

In view of Theorem 3.1, it is natural to define the following concept. A *basic permutation polynomial* $f(x)$ in $\mathbb{Z}_p[x]$ is defined to be a permutation polynomial over $\mathbb{Z}_p$ such that its derivative $f'(x)$ never vanishes on $\mathbb{Z}_p$. We denote by $BP(p)$ the set of all basic permutation polynomials.

For our next theorem, we prove two lemmas.

Lemma 4.3. *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 $f(x) = h(x)(x^p - x)^2$ for some polynomial $h(x)$ 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 $f(x)$ and $f'(x)$ both vanish on $\mathbb{Z}_p$.

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

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

and $f(x)$ induces the zero function on $\mathbb{Z}_p$, we see $a_0 = a_1 = \cdots = a_{p-1} = 0$. Then as (see the proof of Lemma 3.2)

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

we also have $a_p = a_{p+1} = \cdots = a_{2p-1} = 0$. Hence

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

This completes the proof. □

Lemma 4.4. *Let $r > 1$. 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 $f(x)$ induces the zero function on $\mathbb{Z}_{p^r}$. Then by Theorem 2.1, we can write

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

Reducing modulo p, we see

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

This proves the lemma. □

We define $B(p)$ to be the set of all equivalence classes of $BP(p)$ modulo $((x^p - x)^2)$. In view of Lemma 4.3, $\overline{f(x)} = \overline{g(x)}$ in $B(p)$ if and only if $f(x)$ and $g(x)$ are basic permutation polynomials inducing the same permutation of $\mathbb{Z}_p$ and their derivatives $f'(x)$ and $g'(x)$ also induce the same nonvanishing function on $\mathbb{Z}_p$. We then have

Theorem 4.5. *$B(p)$ is a group under polynomial composition. And for $r > 1$, we have a surjective group homomorphism*

$$\varphi : P(p^r) \to B(p)$$

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

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 $BP(p)$ because $f_2 \circ f_1(x)$ 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 $\mathbb{Z}_p$. In the same way, $g_2 \circ g_1(x)$ is in $BP(p)$. Observe that $f_2(f_1(x))$ and $g_2(g_1(x))$ induce the same function on $\mathbb{Z}_p$ because so do $f_1(x)$ and $g_1(x)$; and $f_2(x)$ and $g_2(x)$. Similarly their derivatives $f_2'(f_1(x))f_1'(x)$ and $g_2'(g_1(x))g_1'(x)$ induce the same function on $\mathbb{Z}_p$. Therefore by Lemma 4.3 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 $\overline{x}$.

Let $r > 1$. We can define a natural map

$$\varphi : P(p^r) \to B(p)$$

by $\varphi(\overline{f(x)}) = \overline{\bar{f}(x)}$. It is a well-defined surjective monoid homomorphism from a group to a monoid by Theorem 3.1 and Lemma 4.4. It follows that $B(p)$ is in fact a group, and φ is a group homomorphism. □

In the following series of theorems, we reveal the structure of the group $B(p)$ completely. See Theorem 4.9.

First we have another natural group homomorphism.

Theorem 4.6. *We have a surjective group homomorphism*

$$\psi : B(p) \to P(p)$$

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

Proof. To check ψ is well-defined, note that for arbitrary $h(x)$, the polynomial $h(x)(x^p - x)^2$ induces the zero function on $\mathbb{Z}_p$ so that $h(x)(x^p - x)^2$ is in $V(p)$. Then ψ is clearly a 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 we just choose them 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 $\overline{g(x)} \mapsto \overline{f(x)}$. This completes the proof. □

Let us denote by M_p the 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 $\mathbb{Z}_p^\times$.

Theorem 4.7. *The kernel of ψ is isomorphic to M_p.*

Proof. We define a map $\lambda : \ker\psi \to M_p$ by mapping $\overline{f(x)}$ to the function τ on $\mathbb{Z}_p$ induced by $f'(x)$. λ is well-defined because the derivative of any representative of $\overline{f(x)}$ in $B(p)$ induces the same function on $\mathbb{Z}_p$. To see λ is a group homomorphism, observe that for $\overline{f(x)}$, $\overline{g(x)}$ in $\ker\psi$,

$$(f \circ g)'(x) = f'(g(x))g'(x) \equiv f'(x)g'(x) \pmod{V}$$

because $g(x)$ induces the identity function on $\mathbb{Z}_p$, and hence $\lambda(\overline{f \circ g(x)}) = \lambda(\overline{f(x)})\lambda(\overline{g(x)})$.

Injectivity is clear. We 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 $f'(x) \equiv 1 - h(x) \pmod{V}$, we need to have $1 - h(c) = \tau(c)$ or $h(c) = 1 - \tau(c)$ 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 $\overline{f(x)} \mapsto \tau$. □

Let $\overline{g(x)} \in P(p)$. Let $f(x) = g(x) + (g'(x) - 1)(x^p - x)$. Then $f(x) \equiv g(x) \pmod{V}$ and $f'(x) = 1 + g''(x)(x^p - x) \equiv 1 \pmod{V}$. Therefore $f(x)$ is a basic permutation polynomial. Thus we can define a map $\rho : P(p) \to B(p)$ by $\overline{g(x)} \mapsto \overline{f(x)}$.

Theorem 4.8. *The map $\rho : P(p) \to B(p)$ is a well-defined injective group homomorphism.*

Proof. If $\rho(\overline{g(x)}) = \overline{f(x)}$, then $g(x)$ and $f(x)$ induce the same permutation of $\mathbb{Z}_p$. Noting that an element $\overline{f(x)}$ of $B(p)$ is determined by the functions induced by $f(x)$ and $f'(x)$ on $\mathbb{Z}_p$, the assertion is clear. □

Theorem 4.9. *The composition $\psi \circ \rho$ is the identity on $P(p)$ so that 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. Let $\overline{g(x)} \in P(p)$. If $\rho(\overline{g(x)}) = \overline{f(x)}$, then by definition of ρ, $f(x)$ and $g(x)$ induce the same function on $\mathbb{Z}_p$. Therefore $\psi(\overline{f(x)}) = \overline{g(x)}$. □

In Theorem 4.7, we saw $\ker \psi$ is isomorphic to M_p or $(Z_p^\times)^p$. Recall that $P(p)$ is isomorphic to S_p, the symmetric group of p letters, because every permutation of $\mathbb{Z}_p$ is induced by a polynomial. Thus we see $B(p)$ 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 $\sigma \in S_p$, $\tau \in M_p$. This completes the analysis of the group $B(p)$.

We now return to the group $P(p^r)$. 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 $r > 1$. 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

$$\chi_f(a) = \sigma(c) + kp\tau(c) \tag{4.1}$$

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 2.7, it is then indeed a polynomial permutation. Define the map $\xi : B(p) \to P(p^r)$ by $\overline{f(x)} \mapsto \chi_f$.

Theorem 4.10. *The map $\xi : B(p) \to P(p^r)$ is an injective group homomorphism.*

Proof. To see ξ is a homomorphism, let $\overline{f_1(x)}, \overline{f_2(x)}$ be in $B(p)$. And 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 $\mathbb{Z}_{p^r}$,

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

Thus we see that ξ is a group homomorphism.

Injectivity is easy because that χ_f is the identity permutation of $\mathbb{Z}_{p^r}$ clearly implies $\sigma(c) = c$ and $\tau(c) = 1$ for every $0 \leq c < p$. □

Theorem 4.11. *The composition $\varphi \circ \xi$ is the identity on $B(p)$ so that 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 $\overline{f(x)}$ be in $B(p)$. Let $\chi = \chi_f$ be the permutation of $\mathbb{Z}_{p^r}$ defined as (4.1). Our theorem will be proved if we show that if a polynomial $g(x)$ in $\mathbb{Z}_{p^r}[x]$ induces χ, then $\bar{g}(x)$ and $\bar{g}'(x)$ induce σ and τ on $\mathbb{Z}_p$, respectively. But this immediately follows from Proposition 2.8. □

The following theorem characterizes those polynomial permutations belonging to the group $\ker\varphi$.

Theorem 4.12. *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 each $0 \leq c < p$. 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 each $0 \leq c < p$.*

Proof. Let χ be 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,

$$\chi(c+kp) = \chi_0(c) + kp\chi_1(c) + (kp)^2\chi_2(c) + \cdots + (kp)^{r-1}\chi_{r-1}(c).$$

by Theorem 2.7. By Proposition 2.8, we here have $f(c) \equiv \chi_0(c)$ and $f'(c) \equiv \chi_1(c) \pmod p$. It follows that $\chi_0(c) \equiv c \pmod p$ and $\chi_1(c) \equiv 1 \pmod p$. Let us write $\chi_0(c) = c + p\tilde{\chi}_0(c)$ and $\chi_1(c) = 1 + p\tilde{\chi}_1(c)$. Then

$$\begin{aligned}\chi(c+kp) &= c + p\tilde{\chi}_0(c) + kp(1 + p\tilde{\chi}_1(c)) + (kp)^2\chi_2(c) + \cdots + (kp)^{r-1}\chi_{r-1}(c) \\ &= c + kp + p\tilde{\chi}_0(c) + (kp)p\tilde{\chi}_1(c) + (kp)^2\chi_2(c) + \cdots + (kp)^{r-1}\chi_{r-1}(c).\end{aligned}$$

If we define μ by

$$\mu(c+kp) = \tilde{\chi}_0(c)p + (kp)\tilde{\chi}_1(c)p + (kp)^2\chi_2(c) + \cdots + (kp)^{r-1}\chi_{r-1}(c),$$

then $\chi = \iota + \mu$ and μ is a polynomial function (by Theorem 2.7) satisfying $\mu(c) \equiv 0 \pmod p$ and $\mu(c+p) \equiv \tilde{\chi}_0(c)p \equiv \mu(c) \pmod{p^2}$.

The converse is exactly the reversed argument of the above. And the equivalent condition for μ follows by Proposition 2.8. □

The analysis of the structure of $\ker\varphi$ is left for further work. But for $r = 2$ case, the structure of $\ker\varphi$ is particularly simple. Let T_p be the 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 $\mathbb{Z}_p$.

Theorem 4.13. *Let $r = 2$. The subgroup $\ker\varphi$ of $P(p^2)$ is isomorphic to T_p.*

Proof. Theorem 4.12 shows that $\chi = \iota + \mu$ where μ satisfies $\mu(c + kp) = \tilde{\chi}_0(c)p$. Therefore $\ker\varphi$ is the set of χ satisfying $\chi(a) = a + p\gamma(c)$ for $a = c + kp \in \mathbb{Z}_{p^2}$ where γ is an arbitrary function from $\mathbb{Z}_p$ to $\mathbb{Z}_p$. If $\chi_1(a) = a+p\gamma_1(c)$ and $\chi_2(a) = a+p\gamma_2(c)$, then $\chi_2\circ\chi_1(a) = \chi_2(a+p\gamma_1(c)) = a+p\gamma_1(c)+p\gamma_2(c) = a+p(\gamma_1(c)+\gamma_2(c))$. This shows that $\ker\varphi$ is isomorphic to the additive group $\{\gamma \mid \gamma : \mathbb{Z}_p \to \mathbb{Z}_p\}$. □

Hence the group $P(p^2)$ of all 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 $\beta(\tau,\sigma)(\gamma) = (\gamma\tau)\circ\sigma^{-1}$. In particular, the order of the group $P(p^2)$ is $p^p(p-1)^p p!$.

Remark. After our work, we learned that 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.

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.

Department of Mathematics, Ewha Womans University, Seoul 120-750, Korea

E-mail address: hsllee@ewha.ac.kr

Department of Mathematics, Ewha Womans University, Seoul 120-750, Korea

E-mail address: chj2454@ewha.ac.kr

Department of Mathematics, Sogang University, Seoul 121-742, Korea

E-mail address: kwankyu@hotmail.com