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

Kwan Kyu 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 $\mathcal{V}_{p^r}$ of all polynomials in $\mathbb{Z}_{p^r}[x]$ inducing the zero function on $\mathbb{Z}_{p^r}$. Let

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

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 \( f(x) = f(x) + V_p \). Then \( P_p \) is a monoid under polynomial composition, naturally isomorphic to the group of all polynomial permutations of \( Z_p \). Thus our object of study is \( P_p \). 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 \( f(x) \in Z_m[x] \). Then \( f(x) \) induces the zero function on \( Z_m \) if and only if it can be written in the form

\[
f(x) = \sum_{n=0}^\infty \frac{a_n m}{\gcd(n!, m)} x_n^n,
\]

where \( x_n^n \) denotes the falling power \( x(x-1) \cdots (x-n+1) \).

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

\[
f(k) = \sum_{n=0}^k b_n k_n^n = 0 \quad \text{for all } k \geq 0.
\]

Note that \( b_k k! \) divides \( b_k n_k^n \) as the binomial coefficient \( \binom{n}{k} = \frac{n_k^n}{k!} \) is an integer. Thus a condition equivalent to (1) is for the coefficients \( b_k \) to satisfy \( b_k k! = 0 \) in \( Z_m \) for all \( k \geq 0 \). Since all solutions of the last equation are

\[
b_k = \frac{am}{\gcd(k!, m)}, \quad 0 \leq a < \gcd(k!, m),
\]

we obtain the result.

**Corollary 2.2.** Every polynomial function on \( Z_m \) has a unique polynomial representation of the form

\[
f(x) = \sum_{n=0}^{m-1} b_n x_n^n, \quad 0 \leq b_n < \frac{m}{\gcd(n!, m)}.
\]

Carlitz [1] gave several characterizations of polynomial functions on \( Z_p \). 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 \( \chi \) on \( \mathbb{Z}_{p^r} \) is induced by a polynomial over \( \mathbb{Z}_{p^r} \) if and only if there are some functions \( \chi_i : \mathbb{Z}_p \to \mathbb{Z}_{p^r}, \ 0 \leq i \leq r - 1 \) such that

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

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

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

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

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

To prove the converse, let \( \chi \) be a function on \( \mathbb{Z}_{p^r} \) satisfying (2). Carlitz’s interpolation formula [1] says that for \( 0 \leq c < p \), the polynomial \( L_c(x) = (1 - (x - c)^{p^{r-1}}) \) 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 \( f_i(x) = \sum_{c=0}^{p-1} \chi_i(c)L_c(x) \) for \( 0 \leq i \leq r - 1 \). Note that \( f_i(c + kp) = \chi_i(c) \). Let \( g(x) = x - \sum_{c=0}^{p-1} cL_c(x) \). 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 \( \chi \) 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 \( \chi \). 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 \( f'(c) \equiv \chi_1(c) \pmod{p} \).
For \( f(x) \in \mathbb{Z}_p[x] \), 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 \( \mathbb{Z}_p[x] \). Then \( f(x) \) induces a permutation of \( \mathbb{Z}_p \) 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 \( \mathbb{Z}_2 \) 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 \( \mathbb{Z}_p \). See Theorem 2.7.

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

**Proof.** Note that \((x^r)' = \sum_{i=0}^{r-1} x^i(x - 1)^{r-1-i} \). If \( r \geq 2p \), then \( i \geq p \) or \( r - 1 - i \geq p \) so that \((x^r)' \approx 0 \). Note that \( x^p - (x^p - x) = 0 \) 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

\[
(x^r)' = (x^p(x - p)^{r-p})' = (x^p - x)x^{r-p}'
\]

\[
= -x^{r-p} + (x^p - x)(x^{r-p})' \approx -x^{r-p}.
\]

\( \square \)

**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 \( f(x) = a_0 + a_1 x^{\frac{1}{p}} + a_2 x^{\frac{2}{p}} + \cdots + a_{s-1} x^{\frac{s-1}{p}} \in \mathbb{Z}_p[x] \). Then

\[
f(x) \approx a_0 + a_1 x^{\frac{1}{p}} + a_2 x^{\frac{2}{p}} + \cdots + a_{p-1} x^{\frac{p-1}{p}},
\]

\[
f'(x) \approx a_1 + a_2 (x^{\frac{1}{p}})' + \cdots + a_{p-1} (x^{\frac{p-1}{p}})' - a_p - a_{p+1} x - a_{p+2} x^2 - \cdots - a_{2p-1} x^{p-1}.
\]
Group of Polynomial Permutations of $\mathbb{Z}_{p^r}$

Hence
\[ f'(0) = (a_1 + \cdots + a_{p-1} (x^{p-1})')|_{x=0} - a_p, \]
\[ f'(1) = (a_1 + \cdots + a_{p-1} (x^{p-1})')|_{x=1} - a_p - a_{p+1}, \]
\[ f'(2) = (a_1 + \cdots + a_{p-1} (x^{p-1})')|_{x=2} - a_p - a_{p+1}^2 - a_{p+2} 2!, \]
\[ \vdots \]
\[ f'(p-1) = (a_1 + \cdots + a_{p-1} (x^{p-1})')|_{x=p-1} - a_p - \cdots - a_{2p-1} (p-1)!. \]

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

\[ \frac{p!(p-1)^r p^{r^2 - 2p}}{\prod_{n=0}^{p-1} \gcd(n!, p^r)}. \]

**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 $p! (p-1)^r p^{r^2 - 2p}$ number of polynomials satisfying the condition in Theorem 2.4. It follows that there are $p! (p-1)^r p^{r^2 - 2p} \times p^{(r-1)p}$ number of polynomials $f(x)$ of degree $< p^r$ inducing a permutation of $\mathbb{Z}_{p^r}$. But these polynomials are divided into classes such that $\prod_{n=0}^{p-1} \gcd(n!, p^r)$ number of polynomials in the same class induce the same function on $\mathbb{Z}_{p^r}$ by Theorem 2.1. \hfill $\Box$

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 \( f(x) = h(x)(x^p - 2)^2 \), 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 \( f(x) = \sum_{n \geq 0} a_n x^{n-2} \). Then
\[
    f(x) \approx a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1} x^{n-2}.
\]
As \( f(x) \approx 0 \), it follows that \( a_0 = a_1 = \cdots = a_{n-1} = 0 \). Now by Lemma 2.5,
\[
f'(x) = \sum_{n \geq p} a_n (x^2)^n = -a_p - a_{p+1} x - a_{p+2} x^2 - \cdots - a_{2p-1} x^{2p-2}.
\]
As \( f'(x) \approx 0 \), we also have \( a_p = a_{p+1} = \cdots = a_{2p-1} = 0 \). Hence
\[
f(x) = \sum_{n \geq 2p} x^{n-2} = \sum_{n \geq 2p} x^p(x+2p)x^{n-2p} = (x^p - x)^2 \sum_{n \geq 2p} x^{n-2p}.
\]

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 \( f(x) = h(x)(x^p - x)^2 \) 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
\[
f(x) = a_p p^{r-1} x^p + a_{p+1} p^{r-1} x^{2p+1} + \cdots + a_{2p-1} p^{r-1} x^{2p-1} + \sum_{n \geq 2p} a_n x^n.
\]
Therefore \( \tilde{f}(x) = \sum_{n \geq 2p} a_n x^n = (x^p - x)^2 \sum_{n \geq 2p} a_n x^{n-2p} \).

We define
\[
    B_p = \{ \overline{f(x)} \mid f(x) \in B_p \}
\]
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 \( \overline{f(x)} = g(x) \) 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 \( \overline{f(x)} \mapsto \overline{f(x)} \).

Proof. We first show that polynomial composition gives a well-defined operation on \( B_p \). Let \( \overline{f_1(x)} = g_1(x) \) and \( \overline{f_2(x)} = g_2(x) \) 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 $\mathcal{B}_p$. Hence $\mathcal{B}_p$ is a monoid with identity $\overline{x}$.

By Theorem 2.4 and Lemma 3.2, the natural map

$$\varphi : \mathcal{P}_p \to \mathcal{B}_p$$

is well-defined and a surjective monoid homomorphism from a group to a monoid. It follows that $\mathcal{B}_p$ is in fact a group, and $\varphi$ is a group homomorphism.

Through the following series of lemmas, we reveal the structure of the group $\mathcal{B}_p$ completely. See Theorem 3.7.

**Lemma 3.4.** We have a surjective group homomorphism

$$\psi : \mathcal{B}_p \to \mathcal{P}_p$$

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

**Proof.** It is clear that $\psi$ is a well-defined group homomorphism. To see $\psi$ is surjective, observe that if

$$f(x) = a_0 + a_1x + \cdots + a_{p-1}x^{p-1}$$

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

$$g(x) = a_0 + a_1x + \cdots + a_{p-1}x^{p-1} + a_p x^p + \cdots + a_{2p-1}x^{2p-1}$$

is also a permutation polynomial over $\mathbb{Z}_p$. Therefore, $\psi$ is surjective.

Hence $\mathcal{B}_p$ is a group, and $\varphi$ is a group homomorphism.
is a basic permutation polynomial. Indeed \( a_p, a_{p+1}, \ldots, a_{2p-1} \) are chosen successively to satisfy
\[
\begin{align*}
g'(0) &= (a_1 + \cdots + a_{p-1}(x^{p-1})')_{x=0} - a_p \neq 0, \\
g'(1) &= (a_1 + \cdots + a_{p-1}(x^{p-1})')_{x=1} - a_p - a_{p+1} \neq 0, \\
g'(2) &= (a_1 + \cdots + a_{p-1}(x^{p-1})')_{x=2} - a_p - a_{p+1}2 - a_{p+2}2! \neq 0, \\
&\vdots \\
g'(p-1) &= (a_1 + \cdots + a_{p-1}(x^{p-1})')_{x=p-1} - a_p - \cdots - a_{2p-1}(p-1)! \neq 0.
\end{align*}
\]
Then \( g(x) \approx f(x) \), and \( \psi(g(x)) = \overline{f(x)} \).

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 \( \psi \) is isomorphic to \( M_p \).

Proof. Define \( \lambda : \ker \psi \to M_p \) by mapping \( \overline{f(x)} \) to the function \( \tau \) on \( \mathbb{Z}_p \) induced by \( f'(x) \). It is clearly well-defined. To see \( \lambda \) 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 \( \lambda(f \circ g(x)) = \lambda(f(x))\lambda(g(x)) \). Injectivity is clear. Finally to show that \( \lambda \) is surjective, let \( \tau \) 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 \( f(x) \approx \tau \).

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 $\rho(g(x)) = \overline{f(x)}$ with $g(x) \in P_p$ Then by the definition of $\rho, f(x)$ and $g(x)$ induce the same function on $\mathbb{Z}_p$. Therefore $\psi(\overline{f(x)}) = g(x)$. 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 $S_p$ = symmetric group of $p$ 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 $\alpha : S_p \rightarrow \text{Aut}(M_p)$ 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 $f(x) \in B_p$. Let $\sigma$ be the permutation of $\mathbb{Z}_p$ that $f(x)$ induces. Let $\tau$ be the nonvanishing function on $\mathbb{Z}_p$ that $f'(x)$ induces. We then define a permutation $\chi_f$ on $\mathbb{Z}_{p^r}$ by

$$\chi_f(a) = \sigma(c) + k\tau(c)$$

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

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

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

$$\chi_{f_1 \circ f_2}(a) = \chi_{f_1}(\sigma_2(c) + k\tau_2(c))$$

$$= \sigma_1(\sigma_2(c)) + k\tau_1(\sigma_2(c))$$

$$= \sigma_1 \circ \sigma_2(c) + k\tau_1 \circ \sigma_2(c)\tau_2(c)$$

$$= \chi_{f_1 \circ f_2}(a).$$
Hence $\xi$ is a group homomorphism. If $\chi_f$ 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 $\xi$ is injective.

**Lemma 4.2.** The exact sequence

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

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 $\chi_f$ be the permutation of $\mathbb{Z}_{p^r}$ defined by (5). Suppose a polynomial $g(x)$ in $\mathbb{Z}_{p^r}[x]$ induces $\chi_f$. Then by Theorem 2.3, $g(x)$ and $\tilde{g}(x)$ induce $\sigma$ and $\tau$ on $\mathbb{Z}_p$. Hence $\varphi(\chi_f) = \overline{f}(x)$.

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

**Lemma 4.3.** A permutation $\chi$ of $\mathbb{Z}_{p^r}$ is in $\ker \varphi$ if and only if $\chi = \iota + \mu$ where $\mu$ is a polynomial function on $\mathbb{Z}_{p^r}$ satisfying $\mu(c) \equiv 0 \pmod{p}$ and $\mu(c + kp) \equiv \mu(c) \pmod{p^2}$ for $0 \leq c < p$. The condition for $\mu$ is equivalent to that $\mu$ 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 $\chi$ is induced by a polynomial $f(x)$ satisfying $f(c) \equiv c \pmod{p}$ and $f'(c) \equiv 1 \pmod{p}$. Since $\chi$ is a polynomial function, by Theorem 2.3, there exist $\chi_i : \mathbb{Z}_p \rightarrow \mathbb{Z}_{p^r}$ 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 $\mu$ 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 $\mu$ 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 \( \mu \) follows by Theorem 2.3.

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

\[
T_p = \text{group of all functions } \gamma : \mathbb{Z}_p \rightarrow \mathbb{Z}_p
\]

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 \( 0 \leq c, k < p \) throughout. By Lemma 4.3, \( \chi \in \ker \varphi \) if and only if \( \chi = \iota + \mu \) where \( \mu \) 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 \( \gamma \) 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 \( T_p \).

**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 \( \beta : M_p \rtimes_\alpha S_p \rightarrow \text{Aut}(T_p) \) 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


Kwanky 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