Algebra and Discrete Mathematics RESEARCH ARTICLE
Number 4. **(2009).** pp. 167 – 184

Minimal generating sets and Cayley graphs of Sylow p-subgroups of finite symmetric groups

Anna J. Slupik and Vitaly I. Sushchansky

Dedicated to L. A. Kurdachenko on the occasion of his 60th birthday

Abstract. Minimal generating sets of a Sylow p-subgroup P_n of the symmetric group S_{p^n} are characterized. The number of ordered minimal generating sets of P_n is calculated. The notion of the type of a generating set of P_n is introduced and it is proved that P_n contains minimal generating sets of all possible type. The isomorphism problem of Cayley graphs of P_n with respect to their minimal generating sets is discussed.

1. Introduction

For any finite p-group (p is a prime) all minimal (in the sense of an inclusion) generating sets have the same size. If X is a minimal generating set of a finite p-group G, then for every automorphism $\alpha \in Aut(G)$ image X^α is also a minimal generating set of G. Hence $Aut(G)$ acts on the set Σ_G of all minimal generating sets of G. The investigation of orbits of $Aut(G)$ on the set Σ_G is interesting from the point of view of the isomorphism problem for Cayley graphs of the group G [1, 2, 9]. Namely, if generating sets X, Y belong to the same orbit of $Aut(G)$ on Σ_G, then Cayley graphs $Cay(G, X)$ and $Cay(G, Y)$ are isomorphic. For many p-groups G the inverse statement is also true, i.e. if $Cay(G, X)$ is isomorphic to $Cay(G, Y)$ then X, Y belong to the same orbit of $Aut(G)$ on Σ_G. We call p-groups with such property MCI-groups. For MCI-group G the isomorphism problem of connected Cayley graphs of minimal branch degree is equivalent to characterization of orbits of the group $Aut(G)$ on Σ_G. If G is not the MCI-group then some orbits $Aut(G)$

2000 Mathematics Subject Classification: *20B35, 05C25, 05C12, 20F65.*
Key words and phrases: *Cayley graph, Sylow p-subgroup, Frattini subgroup.*

on Σ_G can join together into one equivalence class of the Cayley graphs isomorphism relation. Hence, in both cases, the investigation of different types of minimal sets of generators and the action of automorphism group on that sets can be use to solve the isomorphism problem of Cayley graphs in the natural way .

In this paper we investigate minimal sets of generators of the Sylow p-subgroup P_n of symmetric group S_{p^n} of the degree p^n ($n \in \mathbb{N}$), using special polynomial representation of this group proposed by L. Kaloujnine in [4, 5]. The outline of this paper is as follows. In the section 2 we remind basic definitions and facts about Sylow p-subgroups P_n and characterize some calculation techniques connected with the polynomial representation of those groups. In the section 3 the theorem about the number of minimal ordered generating sets of P_n is proved and the characterization of all those sets for $n = 2$ is presented. In the section 4 we focus on investigation of triangular and diagonal generating sets. We give a short description of the decomposition algorithm for elements from P_n into the product of generators from a diagonal generating set. In the section 5 we introduce the notion of the type of generating set and we give a complete description of the set of types for all minimal generating sets of P_n. In the section 6 we discuse sufficient condition for the group P_n to be a MCI-group and we construct examples of generating sets with isomorphic or non-isomorphic Cayley graphs.

2. Preliminaries

Let S_m be the symmetric group of the degree m and $m = a_0+a_1p+a_2p^2+ ... + a_kp^k$, where p is a prime. By P_n we denote the Sylow p-subgroup of the symmetric group S_{p^n} $(n = 1, 2, \ldots)$. Then a Sylow p-subgroup of S_m is isomorphic (see [3]) to the direct product

$$P_1^{a_1} \times P_2^{a_2} \times \ldots \times P_k^{a_k}.$$

So the investigation of the structure of Sylow p-subgroups of the symmetric group S_m can be reduced to analysis of Sylow p-subgroups of the symmetric group S_{p^n} $(n = 1, 2, \ldots, k)$. It is easy to verify that the order of the group P_n is equal to:

$$|P_n| = p^{1+p+p^2+\ldots+p^{n-1}}.$$

It is well known that P_n is isomorphic to the wreath product of n regular cyclic groups of order p (see, for example [3]):

$$P_n \cong \underbrace{C_p \wr C_p \wr \cdots \wr C_p}_{n}.$$

For our considerations we can use very convenient presentation of P_n introduced by L. Kaloujnine (see [4],[5]).

Let $\mathbb{Z}_p$ be the field of residues modulo p. Every function f of n variables over $\mathbb{Z}_p$ can be represented by a polynomial of n variables over $\mathbb{Z}_p$. Let I be an ideal of the ring $\mathbb{Z}_p[x_1,\dots,x_m]$ generated by polynomials $x_1^p - x_1,\dots,x_m^p - x_m$. Polynomials $g,\ h \in \mathbb{Z}_p[x_1,\dots,x_m]$ define the same function if and only if $g \equiv h \pmod I$. Any residue class of $\mathbb{Z}_p[x_1,\dots,x_m]/I$ contains an unique polynomial such that degrees of all its variables $x_1,\dots,x_m$ are equal at most $p-1$. This polynomial is called a reduced polynomial modulo ideal I.
The sequence of the type:

$$u = [f_1, f_2(x_1), f_3(x_1,x_2),\dots,f_n(x_1,\dots,x_{n-1})] \tag{1}$$

where $f_1 \in \mathbb{Z}_p$ and f_i is a reduced polynomial for $i = 2,3,...,n$ is called a tableau of the length n over $\mathbb{Z}_p$ (see, [5]).
Every tableau of the form (1) acts on the set $\mathbb{Z}_p^n$ in the following way:

$$(x_1,x_2,\dots,x_n)^u = (x_1+f_1, x_2+f_2(x_1),\dots,x_n+f_n(x_1,\dots,x_{n-1})) \tag{2}$$

for any $(x_1,x_2,\dots,x_n) \in \mathbb{Z}_p^n$.

Lemma 1. *For any tableau u the action (2) defines some permutation on $\mathbb{Z}_p^n$.*

Proof. Simply checking. □

The set of all tableaux forms a group according to the following operation: If

$$u = [f_1, f_2(x_1),\dots,f_n(x_1,\dots,x_{n-1})]$$

and

$$v = [g_1, g_2(x_1),\dots,g_n(x_1,\dots,x_{n-1})]$$

then:

$$\begin{aligned} uv = [&f_1+g_1, f_2(x_1)+g_2(x_1+f_1),\dots,\\ &f_n(x_1,\dots,x_{n-1})+g_n(x_1+f_1,\dots,x_{n-1}+f_{n-1}(x_1,\dots,x_{n-2}))]\ . \end{aligned} \tag{3}$$

The tableau $e = [0,\dots,0]$ is the neutral element for this operation. The inverse element for u is equal:

$$\begin{aligned} u^{-1} = [&-f_1, -f_2(x_1-f_1), -f_3(x_1-f_1, x_2-f_2(x_1-f_1)),\dots\\ &\dots,-f_n(x_1-f_1,\dots,x_{n-1}-f_{n-1}(...))]\ . \end{aligned} \tag{4}$$

The order of this group is equal to $p^{1+p+p^2+\dots+p^{n-1}}$ and hence it is isomorphic to Sylow p-subgroup of symmetric group S_{p^n}. Thus every element of the Sylow p-subgroup P_n may be represented by a tableau (1). We call this representation as a polynomial or Kaloujnine representation of P_n.

It is convenient to use the following notation. The sequence of variables $x_1, x_2, \ldots, x_i$ we denote by X_i. Let us take any tableau

$$u = [f_1, f_2(X_1), \ldots, f_n(X_{n-1})] .$$

By the symbol $u_{(i)}$ we denote the beginnig of the tableau u of the length i. For any reduced polynomial $g(X_i)$ we denote by $g(X_i^u) = g(X_i^{u_{(i)}})$ the following polynomial

$$g(x_1 + f_1, x_2 + f_2(X_1), \ldots, x_i + f_i(X_{i-1})) .$$

According to our notation, the product of tableaux $u_{(i)} = [u_{(i-1)}, a(X_i)]$ and $v_{(i)} = [v_{(i-1)}, b(X_i)]$ has the form

$$[u_{(i-1)}v_{(i-1)}, a(X_{i-1}) + b(X_{i-1}^{u_{(i-1)}})] .$$

Let us denote by $[u]_i$ the i-th coordinate of the tableau u. The tableau u has the depth k if $[u]_1 = \ldots = [u]_k = 0$ and $[u]_{k+1} \neq 0$.

Technique of calculations using the Kaloujnine representation is based on the following simple facts:

Fact 1. *We have the following equalities:*
1. $[(u,v)]_i = [\ uvu^{-1}v^{-1}]_i =$
$$= a(X_{i-1}) - a(X_{i-1}^{u_{(i-1)}v_{(i-1)}}) + b(X_{i-1}^{u_{(i-1)}}) - b(X_{i-1}^{u_{(i-1)}v_{(i-1)}u_{(i-1)}^{-1}}) ,$$
2. $[uvu^{-1}]_{i+1} = a(X_i^{v_{(i)}}) + b(X_i) - a(X_i^{u_{(i)}v_{(i)}u_{(i)}^{-1}})$,
3. $[u^k]_i = \sum\limits_{j=0}^{k-1} a(X_{i-1}^{u^j_{(i-1)}})$.

For every polynomial of k-variables we can define the height of a polynomial.

Definition 1. *The height of the nonzero monomial* $x_1^{\alpha_1}x_2^{\alpha_2} \cdot \ldots \cdot x_k^{\alpha_k}$ *is called the number:*

$$h(x_1^{\alpha_1}x_2^{\alpha_2} \cdot \ldots \cdot x_k^{\alpha_k}) = 1 + \alpha_1 + \alpha_2 p + \ldots + \alpha_k p^{k-1}.$$

We assume that $h(0) = 0$. *The height of the reduced polynomial* f *of* k *variables is equal to the maximum height of its monomials.*

Fact 2. *1. For any reduced polynomial $f(X_k)$ and a tableau $u \in P_n$ the following equality holds*

$$h(f(X_k^u)) = h(f(X_k)) \ .$$

2. For any reduced polynomial $f(X_k)$ and a tableau $u \in P_n$ the following inequality holds

$$h(f(X_k) - f(X_k^u)) \leq \max\{h(f(X_k)) - 1, 0\} \ .$$

3. For any reduced polynomial $f(X_k)$ there exists a tableau $u \in P_n$ such that

$$h(f(X_k) - f(X_k^u)) = \max\{h(f(X_k)) - 1, 0\} \ .$$

4. For any reduced polynomial $f(X_k)$ and a tableau $u \in P_n$ of depth $s \leq k$ the following inequality holds

$$h(f(X_k) - f(X_k^u)) \leq p^k - p^s \ .$$

5. For every tableau $u \in P_n$ of depth $s \leq k$ there exists a reduced polynomial $f(X_k)$ such that

$$h(f(X_k) - f(X_k^u)) = p^k - p^s \ .$$

6. For every tableaux $u, v \in P_n$ the following inequalities hold:

$$h([v^u]_k) \leq \max\{h([v]_k), h([u]_k) - 1\} \ ,$$

$$h([(u,v)]_k) \leq \max\{h([u]_k) - 1, h([v]_k) - 1, 0\} \ .$$

Moreover, for every tableau $u \in P_n$ and $k \geq 1$ there exists a tableau $v \in P_n$ such that

$$h([(u,v)]_k) \leq \max\{h([u]_k) - 1, 0\} \ .$$

By $pc(f(x_1, ..., x_k))$ we denote the coefficient of the monomial of f which has the maximal height.

Lemma 2. *The commutator subgroup of P_n is equal to:*

$$P_n' = \{[0, f_2(X_1), f_3(X_2), ..., f_n(X_{n-1})];\ h(f_i) < p^{i-1},\ i = 2, ..., n\} \ .$$

The quotient group P_n/P_n' is elementary abelian group of the order p^n.

Proof. See [5]. □

3. Bases of Sylow p-subgroups of symmetric groups

An element $g \in G$ is called a non-generating element of G if it can be deleted from any generating set of G. All non-generating elements of G form a subgroup which is called the Frattini subgroup of the group G and denoted by $\Phi(G)$. The subgroup $\Phi(G)$ may be defined also as the intersection of all maximal subgroups of G. If G is a finite p-group then $\Phi(G)$ is the intersection of all subgroups of the index p. As usual, by G^n we denote the group generated by all powers g^n, $g \in G$. The following statement about Frattini subgroups is well known (see for example [11]):

Lemma 3. *If G is a finite p-group, then $\Phi(G) = G'G^p$.*

So if G is a p-group then $G/\Phi(G)$ is an elementary abelian p-group which may be idetified with an additive group of a linear space over $\mathbb{Z}_p$.

Lemma 4. *Let G be a p-group and let φ be a natural epimorphism from G to $G/\Phi(G)$ and $G/\Phi(G) \simeq \mathbb{Z}_p^k$. The set $\{u_1, u_2, \ldots, u_k\}$ of elements from G will be the minimal set of generators, if and only if $\varphi(u_1)$, $\varphi(u_2), \ldots$, $\varphi(u_k)$ is a basis of the linear space $\mathbb{Z}_p^k$ over $\mathbb{Z}_p$.*

Hence any two minimal (according inclusions) generating sets of G has the same size. For the group P_n the epimorhism φ is defined in the following way. Every element of $u \in P_n$ can be written in the form

$$[a_1, a_2x_1^{p-1}+f_2(X_1), a_3x_1^{p-1}x_2^{p-1}+f_3(X_2), ..., a_nx_1^{p-1}\cdot...\cdot x_{n-1}^{p-1}+f_n(X_{n-1})],$$

where $h(f_i) < p^{i-1}$ $(i = 2, \ldots, n)$. Then:

$$\varphi\,(u) = (a_1, a_2, \ldots, a_n)\ .$$

Now for a Sylow p-subgroup of a symmetric group we can formulate such statement:

Lemma 5. *For any Sylow p-subgroup H of symmetric group S_m, $m \geq 2$, the Frattini subgroup $\Phi(H)$ is equal to H'.*

Proof. 1) Let $m = p^n$, p is a prime number, $n \geq 1$. Then $H \simeq P_n$. Because $\Phi(P_n) = P_n' \cdot P_n^p$ it is sufficient to prove the inclusion $P_n^p \subset P_n'$. Let $u = [f_1, f_2(X_1), \ldots, f_n(X_{n-1})] \in P_n$. If $[u]_k = g_k^{(1)}(X_{k-1}) + g_k^{(2)}(X_{k-1})$, where $g_k^{(1)}(X_{k-1}) = a_kx_1^{p-1}\cdots x_{k-1}^{p-1}$, $h(g_k^{(2)}) \leq p^{k-1}-1$, then according to fact 1.3 the following equalities hold:

$$[u^p]_k = \sum_{i=0}^{p-1} g_k^{(1)}(X_{k-1}^{u^i_{(k-1)}}) + \sum_{i=0}^{p-1} g_k^{(2)}(X_{k-1}^{u^i_{(k-1)}})\ .$$

Because

$$h\left(\sum_{i=0}^{p-1} g_k^{(1)}(X_{k-1}^{u^i_{(k-1)}})\right) < p^{k-1}$$

we have

$$h([u^p]_k) \leq p^{k-1} - 1$$

for all $k = 1, 2, \ldots, n$. Hence, by lemma 2, $u^p \in P_n'$ and this case is proved.

2) Let m is a positive integer and $m = a_0 + a_1 p + \ldots + a_n p^n$. Then

$$H \simeq P_1^{a_1} \times \ldots \times P_n^{a_n} .$$

Hence

$$H' \simeq (P_1')^{a_1} \times \ldots \times (P_n')^{a_n} \text{ and } H^p \simeq (P_1^p)^{a_1} \times \ldots \times (P_n^p)^{a_n} .$$

Using the first part of the proof we obtain $H^p \subset H'$ and hence $H' \cdot H^p = H'$. □

Corollary 1. *Any minimal generating set of Sylow p-subgroups of finite symmetric group S_m, $m = a_0 + a_1 p + \ldots + a_k p^k$, contains*

$$d(m) = 1 \cdot a_1 + 2 \cdot a_2 + \ldots + k \cdot a_k$$

generators. In particular, if $m = p^n$ then $d(m) = n$.

We call an ordered minimal set of generators of some finite p-group G a basis of this group. Let $b(G)$ be the number of different bases of the group G.

Theorem 1. *For any integer $n \geq 2$ and prime p the following equality holds:*

$$b(P_n) = p^M \prod_{k=1}^{n} (p^k - 1) ,$$

where $M = n\left(\frac{p^n-1}{p-1} - \frac{1}{2}(1+n)\right)$.

Proof. Every basis of P_n/P_n' can be written in the form:

$$u_1 \cdot P_n',\ u_2 \cdot P_n', \ldots, u_n \cdot P_n'$$

where $\varphi(u_1), \ldots, \varphi(u_n)$ is a basis of the vector space $\mathbb{Z}_p^n$.

So every basis of P_n has a form:

$$u_1 v_1, u_2 v_2, \ldots, u_n v_n$$

where $v_i \in P'_n$ and $[u_i]_k$ is a monomial of maximal height equal p^{k-1} or 0 for $i, k = 1, \ldots, n$ and the set of $\{\varphi(u_1), \ldots, \varphi(u_n)\}$ is a basis in the vector space $\mathbb{Z}_p^n$. The set $u'_1v'_1, u'_2v'_2, \ldots, u'_nv'_n$ forms different basis of P_n if there exist i such that $u_i \neq u'_i$ or $v_i \neq v'_i$. It means that there exist j such that $[u_i]_j \neq [u'_i]_j$ (or $[v_i]_j \neq [v'_i]_j$). If $[u_i]_j \neq [u'_i]_j$ then $pc([u_i]_j) \neq pc([u'_i]_j)$. So $pc([u_iv_i]_j) \neq pc([u'_iv'_i]_j)$ and we have different basis. If $[v_i]_j \neq [v'_i]_j$ then $[u_iv_i]_j = [u_i]_j + [v_i]_j(X_{j-1}^{(u_i)(j-1)})$ and $[u_iv'_i]_j = [u_i]_j + [v'_i]_j(X_{j-1}^{(u_i)(j-1)})$ so $[u_iv_i]_j \neq [u_iv'_i]_j$ and we also have different basis. So $b(P_n) = |GL_n(\mathbb{Z}_p)||P'_n|^n$. Beacuse

$$|GL_n(\mathbb{Z}_p)| = (p^n - 1)(p^n - p) \cdot \ldots \cdot (p^n - p^{n-1}) = p^{\frac{(n-1)n}{2}} \prod_{k=1}^{n} (p^k - 1)$$

and

$$|P'_n|^n = \left(\frac{p^{1+p+\ldots+p^{n-1}}}{p^n} \right)^n = p^{\left(\frac{p^n-1}{p-1} - n\right)n}$$

our proof is completed. □

Now, we give a complete classification of 2-element generating sets of P_2. Let

- A be the family of pairs $\{\, [f_1, f_2(x_1)]\,, [0, g(x_1)]\,\}$, such that $f_1 \neq 0$, f_2 is an arbitrary reduced polynomial and $h(g) = p$;
- B be the family of pairs $\{\, [f_1, f_2(x_1)]\,, [g_1, g_2(x_1)]\,\}$, such that $f_1, g_1 \neq 0$, $h(f_2) < p$, $h(g_2) = p$;
- C be the family of pairs $\{\, [f_1, ax^{p-1} + f_2(x)]\,, [g_1, bx^{p-1} + g_2(x)]\,\}$ such that $f_1, g_1, a, b \neq 0$, $h(f_2) < p$, $h(g_2) < p$ and $a \neq f_1 g_1^{-1} b$.

Then $A \cup B \cup C$ is the set of all minimal generating set of P_2. It follows from definitions of sets A, B and C that their pairwise intersection is empty and

$$\begin{aligned} |A| &= (p-1)^2 p^{2p-1}\,, \\ |B| &= (p-1)^3 p^{2p-2}\,, \\ |C| &= \tfrac{1}{2}(p-1)^3(p-2)p^{2p-2}\,. \end{aligned}$$

Hence $b(P_2) = 2(|A| + |B| + |C|) = (p-1)(p^2-1)p^{2p-1}$.

The proof, that families A, B and C consists of generating sets of P_2 is the conclusion from lemma 4. We have to show that there is no other pairs of generators. It is obvious that one of the generators must have an

element not equal 0 on the first coordinate, and one of them must have a polynomial of degree $p-1$ on the second coordinate. There are only two possibilities left:
1) pairs $u = [f_1, ax^{p-1} + f_2(x)]$, $v = [g_1, bx^{p-1} + g_2(x)]$ such that degrees of polynomials f_2 and g_2 are lower then $p-1$ and $a = f_1 g_1^{-1} b$;
2) pairs $u = [f_1, f_2(x)]$, $v = [0, g(x)]$, such that $f_1 \neq 0$, f_2 is a polynomial of degree $p-1$ and g is a polynomial of degree lower then $p-1$;

In both cases we can easily check that we cannot generate an element which has 0 on the first coordinate and a polynomial of degree $p-1$ on the second coordinate.

4. Triangular bases of P_n

A sequence of tableaux of the type

$$\begin{aligned} u_1 &= [a_1^1, a_2^1(X_1), a_3^1(X_2), \ldots, a_n^1(X_{n-1})], \\ u_2 &= [0, a_2^2(X_1), a_3^2(X_2), \ldots, a_n^2(X_{n-1})], \\ &\vdots \\ u_n &= [0, 0, 0, \ldots, a_n^n(X_{n-1})] \end{aligned} \tag{5}$$

is called an upper triangular sequence and a sequence of tableaux

$$\begin{aligned} v_1 &= [a_1^1, 0, 0, \ldots, 0], \\ v_2 &= [a_1^2, a_2^2(X_1), 0 \ldots, 0], \\ &\vdots \\ v_n &= [a_1^n, a_2^n(X_1), a_3^n(X_2), \ldots, a_n^n(X_{n-1})] \end{aligned} \tag{6}$$

is called a lower triangular sequence.

Theorem 2. *An upper triangular sequence (5) (resp. a lower triangular sequence (6)) of tableaux from P_n is a basis of P_n if, and only if, the following equalities hold:*

$$h(a_i^i(X_{i-1})) = p^{i-1}\ , \quad i = 1, 2, \ldots, n\ . \tag{7}$$

Proof. We verify this statement only for upper triangular sequences of the type (5). Let the equality (7) holds. Then from lemma 4 we only need to show that $\varphi(u_1), \varphi(u_2), \ldots, \varphi(u_n)$ is a basis in the vector space $\mathbb{Z}_p^n$. According to the definition of the epimorphism $\varphi : P_n \to \mathbb{Z}_p^n$ we have

$$\begin{aligned}
&\varphi(u_1) = [pc(a_1^1), pc(a_2^1), pc(a_3^1), \ldots, pc(a_n^1)],\\
&\varphi(u_2) = [0, pc(a_2^2), pc(a_3^2), \ldots, pc(a_n^2)],\\
&\varphi(u_3) = [0, 0, pc(a_3^3), \ldots, pc(a_n^3)],\\
&\vdots\\
&\varphi(u_n) = [0, 0, 0, \ldots, pc(a_n^n)],
\end{aligned}$$

where $pc(a_i^i) \neq 0$, because $h(a_i^i) = p^{i-1}$. This is of course a basis of vector space $\mathbb{Z}_p^n$ because we have $pc(a_1^1) \cdot pc(a_2^2) \cdot \ldots \cdot pc(a_n^n) \neq 0$.

In the other hand, if there exist index i such that $h(a_i^i(X_{i-1})) < p^{i-1}$ then $pc(a_i^i) = 0$ and $pc(a_1^1) \cdot pc(a_2^2) \cdot \ldots \cdot pc(a_n^n) = 0$. Hence $\varphi(u_1)$, $\varphi(u_2), \ldots, \varphi(u_k)$ is not a basis of $\mathbb{Z}_p^n$ and $u_1, u_2, \ldots, u_n$ is not a basis of P_n.

For sequences of the type (6) the proof is similar. □

A particular case of upper triangular sequences is diagonal sequence of elements from P_n. A sequence of the type

$$\begin{aligned}
&u_1 = [a_1^1, 0, 0, \ldots, 0],\\
&u_2 = [0, a_2^2(X_1), 0, \ldots, 0],\\
&\vdots\\
&u_n = [0, 0, 0, \ldots, a_n^n(X_{n-1})]
\end{aligned} \tag{8}$$

where $h(a_i^i(X_{i-1})) = p^{i-1}$, is called a diagonal basis of P_n. Let D be the set of all diagonal bases of P_n. Then

$$|D| = (p-1)^n \cdot p^{\frac{p^n-1}{p-1}-n} .$$

From the point of view of the polynomial representation, diagonal bases are very natural for construction of decomposition elements of P_n into a product of generators. Namely, an arbitrary tableau $w = [f_1, f_2(X_1), f_3(X_2), ..., f_n(X_{n-1})]$ can be decomposed into the product

$$w = u_n u_{n-1} \cdots u_1 ,$$

where $u_i = [0, \ldots, 0[w]_i, 0, \ldots, 0]$ $(1 \leq i \leq n)$. Hence it is sufficient to construct decompositions for "coordinate" tableaux

$$u_i = [0, \ldots, 0, f_i(X_{i-1}), 0, \ldots, 0] .$$

Using statements from facts 1 and 2 for any height h, $0 \leq h \leq p^{i-1}$ it is possible to construct (step by step) the tableau

$$v_i^{(h)} = [0, \ldots, 0, f_i^{(h)}(X_{i-1}), 0, \ldots, 0]$$

such that $h(f_i^{(h)}(X_{i-1})) = h$ and $pc(f_i^{(h)}(X_{i-1})) = 1$. In such a way we obtain a sequence of tableaux $v_i^{(p^{i-1})}, v_i^{(p^{i-1}-1)}, \ldots, v_i^{(1)}$. Next, using such tableaux we can construct the sequence of tableaux $w_i^{(1)}, \ldots, w_i^{(p^{i-1})}$, for which $[w_i^{(k)}]_i$ is a monomial of the height k with the coefficient 1. And finally, using tableaux $w_i^{(k)}$ $(1 \leq k \leq p^{i-1})$ we can construct tableau u_i in the unique way.

5. The action $Aut(P_n)$ on minimal sets of generators

Let Σ_n be the family of all minimal generating sets of P_n, i.e.

$$\Sigma_n = \{\{u_1, u_2, \ldots, u_n\}\,;\, \langle u_1, u_2, \ldots, u_n\rangle = P_n\}\ .$$

The group $Aut(P_n)$ of all automorphisms of P_n acts on the set Σ_n according to the rule

$$\{u_1, u_2, \ldots, u_n\}^\sigma = \{u_1^\sigma, u_2^\sigma, \ldots, u_n^\sigma\}\ ,$$

where $\{u_1, u_2, \ldots, u_n\} \in \Sigma_n$ and $\sigma \in Aut(P_n)$.

Note that, for any element $u \in P_n$, $u \neq e$, the order $|u|$ belongs to the set $\{p, p^2, \ldots, p^n\}$.

Definition 2. *Let $U = \{u_1, u_2, \ldots, u_n\}$ be a minimal generating set of P_n. The multiset $\{\log_p |u_1|, \log_p |u_2|, \ldots, \log_p |u_n|\}$ is called the type of the set U and denoted by $t(U)$. For any basis $u_1, u_2, \ldots, u_n$ the type of the set $\{u_1, u_2, \ldots, u_n\}$ is called the type of this basis.*

We write the type $t(U)$ as a vector $(k_1, k_2, \ldots, k_n)$, $k_1 \leq k_2 \leq \ldots \leq k_n$, where $k_i = \log_p |u_{\sigma(i)}|$ for some permutation $\sigma \in S_n$.

Lemma 6. *Let $u = [f_1, f_2(X_1), \ldots, f_n(X_{n-1})]$, where*

$$f_i(X_{i-1}) = a_i x_1^{p-1} x_2^{p-1} \cdots x_{i-1}^{p-1}$$

for $i = 1, \ldots, n$. Then $|u| = p^s$, where $s = |\{i\,;\, a_i \neq 0\}|$.

Proof. Let j be the smallest index of nonzero a_j in u. Then $u_{(j-1)} = 0$ and $u_{(j)} = [0, f_j(X_{j-1})]$. We have

$$u_{(j)}^p = [0, p \cdot f_j(X_{j-1})] = [0, 0]\ ,$$

thus $|u_{(j)}| = p$. Now, let us assume that for some l the order of $u_{(l)}$ is equal to p^m $(m > 0)$. If $f_{l+1} \neq 0$, then according to the fact 1.3 we have

$$u_{(l+1)}^k = [u_{(l)}^k, \sum_{i=0}^{k-1} f_{l+1}(X_{j-1}^{u_{(l)}^i})]\ .$$

The smallest k, such that the first part $u^k_{(l)}$ is equal zero, is p^m. Then

$$u^{p^m}_{(l+1)} = [0, \sum_{i=0}^{p^m-1} f_{l+1}(X_{j-1}^{u^i_{(l)}})] ,$$

but $\sum_{i=0}^{p^m-1} f_{l+1}\Big(\underbrace{(0,0,\ldots,0)}_{j-1}{}^{u^i_{(l)}}\Big) = a_l(p-1)^m \neq 0$. Hence $|u_{(l+1)}| > p^m$.

Since

$$u^{p^{m+1}}_{(l+1)} = [0, p\cdot \sum_{i=0}^{p^m-1} f_{l+1}(X_{j-1}^{u^i_{(l)}})] = [0,0] ,$$

then $|u_{(l+1)}| = p^{m+1}$. □

Using lemma 6 we prove

Lemma 7. *The group P_n has minimal generating sets of types* $(1,1,...,1)$ *and* $(n,n,...,n)$.

Proof. The basis

$u_1 = [1,0,0,\ldots,0]$,
$u_2 = [0, x_1^{p-1}, 0, \ldots., 0]$,
$u_3 = [0,0,x_1^{p-1}x_2^{p-1},\ldots,0]$,
$\vdots$
$u_n = [0,0,0,\ldots,x_1^{p-1}x_2^{p-1}\cdot\ldots\cdot x_{n-1}^{p-1}]$

of P_n has the type $(1,1,\ldots,1)$.

For $n = 1$ there exist bases of the second type obviously. Let $n = 2$. Then we take elements $u_1 = [1, x_1^{p-1}]$ and $u_2 = [1,(p-1)x_1^{p-1}]$ from P_2. By lemma 6, $|u_1| = |u_2| = p^2$. Since

$$\det \begin{bmatrix} \varphi(u_1) \\ \varphi(u_2) \end{bmatrix} = \det \begin{bmatrix} 1 & 1 \\ 1 & p-1 \end{bmatrix} = (p-2) \neq 0 ,$$

then u_1 and u_2 form a basis of P_2.

Now, if $n > 2$, then we take tableaux

$u_1 = [(p-1), x_1^{p-1}, x_1^{p-1}x_2^{p-1},\ldots,x_1^{p-1}x_2^{p-1}\cdot x_{n-1}^{p-1}]$,
$u_2 = [1,(p-1)x_1^{p-1}, x_1^{p-1}x_2^{p-1},\ldots,x_1^{p-1}x_2^{p-1}\cdot x_{n-1}^{p-1}]$,
$\vdots$
$u_n = [1, x_1^{p-1}, x_1^{p-1}x_2^{p-1},\ldots,(p-1)x_1^{p-1}x_2^{p-1}\cdot x_{n-1}^{p-1}]$.

By lemma 6, $|u_1| = |u_2| = \ldots = |u_n| = p^n$. Since

$$\det \begin{bmatrix} \varphi(u_1) \\ \varphi(u_2) \\ \vdots \\ \varphi(u_n) \end{bmatrix} = \det \begin{bmatrix} p-1 & 1 & \ldots & 1 \\ 1 & p-1 & \ldots & 1 \\ \vdots & & \ddots & \\ 1 & 1 & \ldots & p-1 \end{bmatrix} =$$

$$= (p-2)^{n-1}(n-2) \neq 0$$

then $u_1, u_2, \ldots, u_n$ form a basis of P_n. □

Let $\mathcal{T} = \{(k_1, k_2, \ldots, k_n)\,;\, 1 \leq k_1 \leq \ldots \leq k_n \leq n\}$. We introduce the componentwise partial order $\preceq$ on the set $\mathcal{T}$, i.e. for $(k_1, k_2, \ldots, k_n)$ and $(l_1, l_2, \ldots, l_n)$ from $\mathcal{T}$ we put $(k_1, k_2, \ldots, k_n) \preceq (l_1, l_2, \ldots, l_n)$ if, and only if, $k_i \leq l_i$ for $i = 1, 2, \ldots, n$.

A vector $(1, 1, \ldots, 1)$ is the minimal element of the partially ordered set $(T, \preceq)$ and a vector $(n, n, \ldots, n)$ is the maximal element of $(T, \preceq)$.

Theorem 3. *For any vector $t = (k_1, k_2, \ldots, k_n) \in \mathcal{T}$ there exists a basis of P_n of the type t.*

Proof. Let us take some basis $U = \{u_1, \ldots, u_n\}$ of P_n, where $[u_j]_i = a_i^j x_1^{p-1} x_2^{p-1} \cdots x_{i-1}^{p-1}$ for $i, j \in \{1, \ldots, n\}$. Let us denote by M_U the matrix

$$M_U = \begin{bmatrix} \varphi(u_1) \\ \varphi(u_2) \\ \vdots \\ \varphi(u_n) \end{bmatrix} = \begin{bmatrix} a_1^1 & a_2^1 & \ldots & a_n^1 \\ a_1^2 & a_2^2 & \ldots & a_n^2 \\ \vdots & & \ddots & \\ a_1^n & a_2^n & \ldots & a_n^n \end{bmatrix}.$$

We choose coefficients of M_U according to the rules:
1) For every $j \in \{1, \ldots, n\}$ the number of nonzero coefficients a_i^j of u_j is equal to k_j;
2) $\det M_U \neq 0$.

First we assume that $(1, 1, \ldots, 1) \preceq t \preceq (1, 2, 3, \ldots, n)$. Then we can choose coefficients such that M_U has zeroes over its diagonal:

$$M_U = \begin{bmatrix} 1 & 0 & \ldots & 0 \\ a_1^2 & 1 & \ldots & 0 \\ \vdots & & \ddots & \\ a_1^n & a_2^n & \ldots & 1 \end{bmatrix}.$$

Coefficients under the diagonal are equal 0 or 1 according to the order of elements. Hence $\det M_U = 1$.

Now, let $(1, 2, 3, \ldots, n) \preceq t \preceq (n, n, \ldots, n)$. We define coefficients of M_U in the following way:

- if $j = k_j$, then $a_i^j = \begin{cases} 1\,, & \textit{for } 1 \leq i \leq j \\ 0\,, & j < i \leq n \end{cases}$;

- if $j < k_j$, then $a_i^j = \begin{cases} 2\,, & \textit{for } 1 \leq i \leq j \\ 1\,, & \textit{for } j < i \leq k_j \\ 0\,, & k_j < i \leq n \end{cases}$.

Note that, the last row of M_U always consists of 1. Now, we need to use Gauss elimination starting from the last row. We reduce M_U to the following form:

$$\begin{bmatrix} 1 & 0 & \dots & 0 \\ 1 & 1 & \dots & 0 \\ \vdots & & \ddots & \\ 1 & 1 & \dots & 1 \end{bmatrix}.$$

So $\det M_U = 1$. This ends the proof. □

Corollary 2. *The set of all types of bases of P_n has $\frac{(2n-1)!}{n!(n-1)!}$ elements.*

Since for arbitrary basis U and any automorphism $\alpha \in Aut(P_n)$ the equality

$$t(U^\alpha) = t(U)$$

holds, then the partition of Σ into subsets of generating sets with the same type is coarser than the partition of Σ into orbits of the action $Aut(P_n)$.

6. The isomorphism problem of Cayley graphs of P_n

Let us denote by $Cay(G, X)$ the Cayley graph of group G with respect to the set of generators X. We consider $Cay(G, X)$ as an undirected graph with the set of vertices G. Every vertex $g \in G$ is connected with vertex $gx^{\pm 1}$ for all $x \in X$.

A Cayley graph $Cay(G, X)$ with respect to a minimal set of generators X is called a minimal Cayley graph of G [1].

Definition 3. *A Caley graph $Cay(G, S)$ is called a CI-graph of G if, for any Cayley graph $Cay(G, T)$, whenever $Cay(G, S) \cong Cay(G, T)$, we have $S^\sigma = T$ for some $\sigma \in Aut(G)$.*

Definition 4. *A p-group G is called MCI-group if all Cayley graphs with recpect to minimal sets of generators are CI-graphs.*

One of the very interesting problems is a characterization of groups such that all its Cayley graphs are CI-graphs. This question has been strongly investigated. Many criterions for a Cayley graph to be a CI-graph were obtained. One of them mentioned below is very useful for our consideration (for details and examples see [9]):

Lemma 8. *[10] Let p be a prime and let G be a p-group. Then all Cayley graphs of degree at most $(2p-2)$ are CI-graphs.*

Using this statement for the group P_n we obtain the following result.

Theorem 4. *Let n ba a positive integer $n \geq 2$, p be a prime $p \geq 3$. If $n+1 \leq p$ then P_n is a MCI-group.*

Proof. It follows from corollary 1 that every minimal (according to inclusion) generating set of P_n has the size n. Since $p \geq 3$, then for any generator u we have $u \neq u^{-1}$. Hence degrees of all vertices of the Cayley graph $Cay(P_n, U)$ are equal to $2n$ for any minimal generating set U. If $n+1 \leq p$, then $2n \leq 2p-2$ and by lemma 8 the graph $Cay(P_n, U)$ is the CI-graph. Since U is an arbitrary minimal generating set, then the group P_n is a MSI-group. □

Due to this theorem, under the assumption $n+1 \leq p$, the isomorphism problem for minimal Cayley graphs of P_n can be reduced to the characterization of orbits of the action of the group $Aut(P_n)$ on the set Σ_n. The automorphism group $Aut(P_n)$ is well known (see [7], [8], [2]). $Aut(P_n)$ contains two natural subgroups: the subgroup of inner automorphisms $Inn(P_n)$ and the subgroup $A(P_n)$ consists of automorphisms of the type

$$[a_1, a_2(x_1), \ldots, a_n(x_1, x_2, \ldots x_{n-1})] \mapsto$$

$$[\alpha_1 a_1, \alpha_2 a_2(x_1\alpha_1^{-1}), \ldots, \alpha_n a_n(x_1\alpha_1^{-1}, x_2\alpha_2^{-1}, \ldots, x_{n-1}\alpha_{n-1}^{-1})]\ ,$$

where $[a_1, a_2(X_1), \ldots, a_n(X_{n-1})] \in P_n$, $\alpha_i \in \mathbb{Z}_p^*$ $(1 \leq i \leq n)$. It is easy to verify that the group $Aut_0(P_n) = \langle Inn(P_n), A(P_n)\rangle$ is decomposed into the semidirect product $A(P_n) \leftthreetimes Inn(P_n)$. For $n=2$ the equality $Aut_0(P_n) = Aut(P_n)$ holds, and for $n > 2$ we have inequality $Aut_0(P_n) < Aut(P_n)$.

Using the polynomial techniques described in the section 2 and a characterization of some automorphisms of P_n, we can formulate various necessary or sufficient conditions for an isomorphism of minimal Cayley graphs. We will present the following examples.

1. Let us consider the following class $\mathcal{U}$ of bases of P_n:

$$\begin{aligned}
&u_1(a_1) = [a_1, 0, 0, \ldots, 0],\\
&u_2(a_2) = [0, a_2 x_1^{p-1}, 0, \ldots, 0],\\
&u_3(a_3) = [0, 0, a_3 x_1^{p-1} x_2^{p-1}, \ldots, 0],\\
&\vdots\\
&u_n(a_n) = [0, 0, 0, \ldots, a_n x_1^{p-1} x_2^{p-1} \cdots x_{n-1}^{p-1}],
\end{aligned}$$

where $a_i \in \mathbb{Z}_p^*$ for $i = 1, 2, \ldots, n$.

Then, for any $U, V \in \mathcal{U}$ Cayley graphs $Cay(P_n, U)$ and $Cay(P_n, V)$ are isomorphic, because there exists an automorphism φ from the subgroup $A(P_n)$, which maps any basis $\{u_1(a_1), u_2(a_2), \ldots, u_n(a_n)\}$ onto

$\{u_1(1), u_2(1), \ldots, u_n(1)\}$. The coefficients of φ are the following:

$$\alpha_1 = a_1^{-1}, \alpha_2 = a_2^{-1}, \ldots, \alpha_n = a_n^{-1}. \square$$

2. Let us take an arbitrary basis U

$$\begin{array}{l} u_1 = [a_1^{(1)}, a_2^{(1)}(X_1), \ldots, a_n^{(1)}(X_{n-1})], \\ u_2 = [a_1^{(2)}, a_2^{(2)}(X_1), \ldots, a_n^{(2)}(X_{n-1})], \\ \vdots \\ u_n = [a_1^{(n)}, a_2^{(n)}(X_1), \ldots, a_n^{(n)}(X_{n-1})] \end{array},$$

where $h(a_i^{(k)}) = p^{k-1}$ $(i, k = 1, 2, \ldots, n)$. If $\widehat{U}$ is the orbit of U under the action $Aut(P_n)$ on Σ_n, then $|\widehat{U}| \geq p^{n-1}$. It follows from the facts described below.

Let us take the subset $B = \{[b_1, b_2, \ldots, b_{n-1}, 0] \,;\, b_i \in \mathbb{Z}_p^*\}$ of P_n. Every $b \in B$ defines an inner automorphism φ_b of P_n which acts as follows: For any $g = [g_1, g_2(X_1), \ldots, g_n(X_{n-1})] \in P_n$ we have

$$\varphi_b(g) = b^{-1}gb = [g_1, g_2(x_1 - b_1), \ldots, g_n(x_1 - b_1, \ldots, x_{n-1} - b_{n-1})] \,.$$

It is obvious that if $b \neq b'$ $(b, b' \in B)$ and there exists i such that $[g]_i$ is not a constant polynomial, then $[\varphi_b(g)]_i \neq [\varphi_{b'}(g)]_i$. Since for the basis U of P_n $(n > 1)$ there exists i such that $h([u_i]_n) = p^{n-1}$, then we have $|\widehat{U}| \geq |\{\varphi_b(U) \,;\, b \in B\}| = p^{n-1}$.

3. In general, the equality of types of two bases U and V does not follow the existence of isomorphism between Cayley graphs $Cay(P_n, U)$ and $Cay(P_n, V)$. Let us consider the following two bases of P_2 $(p \neq 2)$:

$$\begin{array}{ll} U: & V: \\ u_1 = [1, 0], & v_1 = [1, 0], \\ u_2 = [0, x_1^{p-1}], & v_2 = [0, 1 - x_1^{p-1}] \,. \end{array}$$

We have $t(U) = t(V) = (1, 1)$. We will show that there is no possibility to find automorphism $\sigma \in Aut_0(P_2)$ such that $\sigma(u_i) = v_i$ for $i = 1, 2$. Note that, any inner automorphisms do not change the first coordinate of any tableau and cannot change the coefficient of the monomial of maximal height on the second coordinate of this tableau. Let us take an arbitrary automorphism $\varphi \in A$. Since $\varphi(u_1) = v_1 = u_1$, then $\alpha_1 = 1$. This automorphism should also change the coefficient of monomial of maximal height so $\alpha_2 = p-1$. Then $\varphi(u_2) = [0, -x_1^{p-1}]$. Now we consider an inner automorphism ψ_a, where $a = [a_1, a_2(x_1)]$. Then $\psi_a(u_1) = a^{-1} \cdot u_1 \cdot a = [1, -a_2(x_1 - a_1) + a_2(x_1 - a_1 + 1)]$. So $a_2(x) = c$ from some $c \in \mathbb{Z}_p$ because second coordinate must be equal 0. Then $\psi_a(\varphi(u_2)) = a^{-1}[0, -x_1^{p-1}]a = [0, -(x_1-a)^{p-1}]$. The function $-(x_1-a)^{p-1}$ is equal 0 for $x_1 = a$ and 1 for the other x_1, so it cannot be equal to the function $1 - x_1^{p-1}$. Hence there is no possibility to have automorphism $\sigma = \varphi\psi$ such that $\sigma(u_2) = v_2$. Because $p \neq 2$ the group P_2 is a MPI-group. It follows that $Cay(P_2, U)$ and $Cay(P_2, V)$ are not isomorphic.

4. Finally, we present the example of two bases U and V of P_3:

$$\text{U:}\quad \begin{array}{l} u_1 = [1,\, x_1^2,\, x_1^2x_2^2] \\ u_2 = [1,\, 2x_1^2,\, x_1^2x_2^2] \\ u_3 = [1,\, x_1^2,\, 2x_1^2x_2^2] \end{array} \qquad \text{V:}\quad \begin{array}{l} v_1 = [2,\, x_1^2,\, x_1^2x_2^2] \\ v_2 = [1,\, 2x_1^2,\, x_1^2x_2^2] \\ v_3 = [1,\, x_1^2,\, 2x_1^2x_2^2] \end{array}$$

such that both of them have the type equals $(3, 3, 3)$ and Cayley graphs $Cay(P_3, U)$ and $Cay(P_3, V)$ are not isomorphic. Those graphs are not isomorphic because their diameters (i.e. the longest distance between vertices of a graph in the standard graph metric) are equal to 12 and 11 respectively. Such diameters were obtained by computer calculations. Note that, in this example the inequality $n + 1 \leq p$ does not hold.

References

[1] Babai L. *Automorphism Groups, Isomorphism, Recostruction.* In: Handbook of combinatorics, v. 2, Elsevier, 1995, 1447-1540.

[2] Bodnarchuk Y.V. *Structure of the group of automorphisms of Sylow p-subgroup of the symmetric group S_{p^n}* $(p \neq 2)$, Ukr. Math. Zhurn., v. 36, 1984, 688-694 (in ukrainian).

[3] Dixon J.D., Mortimer B., *Permutation Groups*, Springer-Verlag, 1996.

[4] Kaloujnine L. A. *Sur les p-group de Sylow du groupe symetrique du degre p^m*, C. R. Acad. Sci. Paris 221, 1945, 222-224.

[5] Kaloujnine L. A. *La structure des p-groupes de Sylow des groupes symŭtriques finis,* Annales scientifiques de l'Ĭcole Normale Supĭrieure, Sĭr. 3 , 65 1948, 239-276,

[6] Konstantinova E. *Some problems on Cayley graphs*, Linear Algebra and its Appl. 429 (2008) 2754-2769.

[7] Lentoudis P. *Le groupe des automorphismes du p-groupe de Sylow du groupe symétrique de degré p^m*, C. R. Math. Rep. Acad. Sci. Canada, 7(2):133-136, 1985.

[8] Lentoudis P., Tits J. *Sur le groupe des automorphismes de certains produits en couronne*, C. R. Acad. Sci. Paris 305, ser. I, 1987, 847-852.

[9] Li C.H., *On isomorphisms of finite Cayley graphs - a survey*, Discrete Mathematics, 256, 2002, 301-334.

[10] Li C.H., *On isomorphisms of connected Cayley graphs*, Discrete Mathematics , 178, 1998, 109-122.

[11] Shalev A. *Finite p-groups*, In: Seitz G., Borowik A.V., Bryant R.M. (ed) *Finite and locally finite groups*, Kluwer Acad. Publ., 1995, 401-450.

Contact information

A. J. Slupik
Institute of Mathematics
Silesian University of Technology
Gliwice
E-Mail: anna.slupik@polsl.pl

V. I. Sushchansky
Institute of Mathematics
Silesian University of Technology
Gliwice
E-Mail: vitaliy.sushchanskyy@polsl.pl

Received by the editors: 07.10.2009
and in final form 07.10.2009.