ZESZYTY NAUKOWE POLITECHNIKI ŚLĄSKIEJ 2015

Seria: MATEMATYKA STOSOWANA z. 5 Nr kol. 1945

Bartłomiej PAWLIK

Institute of Mathematics
Silesian University of Technology

INVOLUTIVE BASES OF SYLOW 2-SUBGROUPS OF SYMMETRIC AND ALTERNATING GROUPS

Summary. The paper presents a construction of Sylow 2-subgroups of symmetric and alternating groups, which bases contains only an involutions. Polynomial representation of Sylow 2-subgroups was used.

INWOLUTYWNE BAZY 2-PODGRUP SYLOWA GRUP SYMETRYCZNYCH I ALTERNUJĄCYCH

Streszczenie. W artykule przedstawiono konstrukcję takich 2-podgrup Sylowa grup symetrycznych i alternujących, których bazy zawierą wyłącznie inwolucje. Zastosowano reprezentację 2-podgrup Sylowa za pomocą zredukowanych wielomianów wielu zmiennych nad ciałem $\mathbb{Z}_2$.

1. Introduction

Let p be a prime. The Sylow p-subgroups of symmetric and alternating groups of order p^n, $n \in \mathbb{N}$ play an analogous role for finite p-groups, as symmetric and

2010 Mathematics Subject Classification: 20B35, 20D20, 20E22.
Keywords: Sylow p-subgroups, group base, wreath product of groups.
Corresponding author: B. Pawlik (bartlomiej.pawlik@polsl.pl).
Received: 03.09.2015.

alternating groups for finite groups. Every finite p-group can be isomorphically embedded into one of these groups, thus Sylow p-subgroups of symmetric and alternating groups are important in group theory. Other important applications of these groups involve various fields of discrete mathematics, like coding theory, sorting theory, etc. Especially generating sets of such p-groups are important in some investigations.

If $p \neq 2$, then every Sylow p-subgroup of the alternating group of order p^n is also Sylow p-subgroup of the symmetric group of the same order. It is well known, that the Frattini subgroup of any finite p-group G is equal to $G'G^p$. Hence, generating sets of such a group correspond to generating sets of p-abelianisation. So the Sylow p-subgroups of symmetric and alternating groups of degree p^n have equinumerous minimal in terms of inclusion, generating sets (bases) (see [5]).

Every involution (permutation of the order 2) can be written as a product of separable transpositions. Involutive base is a base in which every element is an involution. In this article we investigate involutive bases of Sylow 2-subgroups of the symmetric group S_{2^n} and the alternating group A_{2^n}, $n \in \mathbb{N}$. We use a polynomial representation of such Sylow 2-subgroups, e.g. in which elements are sequences of reduced polynomials over field $\mathbb{Z}_2$ of residues modulo 2 (see [2, 4]).

In Section 2 we recall basic and well known facts about Sylow p-subgroups of symmetric and alternating groups. In Section 3 we introduce the polynomial (Kaloujnine) representation of wreath product and some of its properties. The construction of involutive base of Sylow 2-subgroup of symmetric and alternating group is discussed in Section 4.

2. Sylow p-subgroups of symmetric and alternating groups

If $m = a_0 + a_1 p + a_2 p^2 + \ldots + a_k p^k$, where p is a prime, then the Sylow p-subgroup $\mathrm{Syl}_p(S_m)$ of symmetric group S_m is isomorphic (see e.g. [3]) to the direct product

$$\left(\mathrm{Syl}_p(S_p)\right)^{a_1} \times \left(\mathrm{Syl}_p(S_{p^2})\right)^{a_2} \times \ldots \times \left(\mathrm{Syl}_p(S_{p^k})\right)^{a_k}.$$

Alternating groups have similar property. The Sylow p-subgroup $\mathrm{Syl}_p(A_m)$ of the alternating group A_m is isomorphic to the product

$$\left(\mathrm{Syl}_p(S_p)\right)^{\underline{a_1}} \underline{\times} \left(\mathrm{Syl}_p(S_{p^2})\right)^{\underline{a_2}} \underline{\times} \ldots \underline{\times} \left(\mathrm{Syl}_p(S_{p^k})\right)^{\underline{a_k}},$$

where $G^{\underline{a}}$ is an even part of G^a (i.e. the intersection of G^a with the corresponding alternating group) and $G \underline{\times} H$ is an even part of $G \times H$.

So instead of Sylow p-subgroups of the symmetric group S_m or the alternating group A_m, we may investigate the subgroups of group S_{p^n}.

It is known that $\mathrm{Syl}_p(S_{p^n})$ is isomorphic (see e.g. [3]) to the iterated wreath produt of cyclic groups of order p:

$$\mathrm{Syl}_p(S_{p^n}) \cong \overset{n}{\underset{i=1}{\wr}} C_p.$$

The alternating subgroup has index 2 in symmetric group, so for every p prime, $p > 2$, the Sylow p-subgroups of A_n and S_n coincide. $\mathrm{Syl}_2(A_{2^n})$ is a proper subgroup of $\mathrm{Syl}_2(S_{2^n})$ and

$$[\mathrm{Syl}_2(S_{2^n}) : \mathrm{Syl}_2(A_{2^n})] = 2.$$

In order to describe $\mathrm{Syl}_2(A_{2^n})$ we use the polynomial representation of wreath product introduced by L. Kaloujnine (see e.g. [4, 5]).

3. Polynomial representation

The sequence of variables $x_1, x_2, \dots, x_i$ will be denoted by X_i.

Let $\mathbb{Z}_p$ be the field of residues modulo p. Naturally $\mathbb{Z}_p \cong C_p$. Thus

$$\mathrm{Syl}_p(S_{p^n}) \cong \overset{n}{\underset{i=1}{\wr}} \mathbb{Z}_p,$$

where $\overset{n}{\underset{i=1}{\wr}} \mathbb{Z}_p$ is a wreath product acting on set $\mathbb{Z}_p^n$ and its elements (*tableaux*) are of the form

$$f = [f_1, f_2(X_1), f_3(X_2), \dots, f_n(X_{n-1})], \tag{1}$$

where $f_1 \in \mathbb{Z}_p$ and $f_i : \mathbb{Z}_p^{i-1} \to \mathbb{Z}_p$ for $i = 2, \dots, n$ are reduced polynomials from the quotient ring $\mathbb{Z}[X_i]/\langle x_1^p - x_1, \dots, x_i^p - x_i \rangle$.

Every tableau of the form (1) acts on the set $\mathbb{Z}_p^n$ in the following way:

$$(u_1, u_2, \dots, u_n)^f = (u_1 + f_1, u_2 + f_2(u_1), \dots, u_n + f_n(u_1, \dots, u_{n-1})), \tag{2}$$

for any $(u_1, u_2, \dots, u_n) \in \mathbb{Z}_p^n$.

For more details about the group $\overset{n}{\underset{i=1}{\wr}} \mathbb{Z}_p$, see e.g. [5].

Groups S_{p^n} and A_{p^n} act on the set $\{1, 2, \dots, p^n\}$, so we have to determine a bijection φ between sets $\mathbb{Z}_p^n$ and $\{1, 2, \dots, p^n\}$. Let $(u_1, \dots, u_n) \in \mathbb{Z}_p^n$. The most natural bijection $\varphi : \mathbb{Z}_p^n \to \{1, \dots, p^n\}$ is

$$\varphi(u_1, \dots, u_n) = u_1 p^{n-1} + u_2 p^{n-2} + \dots + u_{n-1} p + u_n + 1.$$

We note that in this case

$$\varphi(0,0,\dots,0)=1$$

and

$$\varphi(p-1,p-1,\dots,p-1)=p^n.$$

For every polynomial on n variables we can define a height of a polynomial:

Definition 1. *The height of the nonzero monomial $x_1^{\alpha_1}x_2^{\alpha_2}\dots x_n^{\alpha_n}$ is defined to be the number*

$$h(x_1^{\alpha_1}x_2^{\alpha_2}\dots x_n^{\alpha_n})=1+\alpha_1+\alpha_2 p+\dots+\alpha_k p^{k-1}.$$

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

For every tableau $f\in \mathrm{Syl}_p(S_{p^n})$ of the form (1) we can now define a height vector of f (also called as a characteristic of f):

$$h(f)=[h(f_1),\dots,h(f_n)].$$

Observe that $0\le h(f_i)\le p^{i-1}$ for $i=1,\dots,n$.

In the set of height vectors we define a partial order. Let

$$g=[g_1,\dots,g_n(X_{n-1})]$$

be an element of $\mathrm{Syl}_p(S_{p^n})$. Then

$$h(g)\le h(f)\iff \forall\, i\in\{1,\dots,n\}\quad h(g_i)\le h(f_i).$$

Definition 2. *A subgroup G of $\mathrm{Syl}_p(S_{p^n})$ is called ideal if*

$$\forall\, u\in G\quad \big(u'\in \mathrm{Syl}_p(S_{p^n})\wedge h(u')\le h(u)\big)\Rightarrow u'\in G.$$

Observe that $\mathrm{Syl}_p(S_{p^n})$ is an ideal subgroup of S_{p^n}.

Every ideal subgroup G of $\mathrm{Syl}_p(S_{p^n})$ can be uniquely described by its so-called height vector of the form

$$h(G)=[\max_{g\in G}h(g_1),\max_{g\in G}h(g_2),\dots,\max_{g\in G}h(g_n)].$$

We note that

$$h(E)=[0,0,\dots,0]$$

and

$$h(\mathrm{Syl}_p(S_{p^n})) = [1, p, \dots, p^{n-1}].$$

Before we determine the height vector of the alternating group, we need a simple observation. The next lemma belongs to so-called mathematical folklore:

Lemma 3. *A reduced polynomial $w \in \mathbb{Z}_2[x_1, \dots, x_k]/\langle x_1^2 - x_1, \dots, x_k^2 - x_k\rangle$ has degree k iff it has odd number of zeros.*

The proof of Lemma 3 is proposed in [1].

Theorem 4. *The tableau $f = [f_1, f_2(x_1), \dots, f_n(X_{n-1})] \in \mathrm{Syl}_2(S_{2^n})$ is an element of $\mathrm{Syl}_2(A_{2^n})$ iff the height of f_n is less than 2^{n-1}.*

Proof. Let

$$a = [0, \dots, 0, a_n(X_{n-1})] \in \mathrm{Syl}_2(S_{2^n}),$$

where $h(a_n) = 2^{n-1}$ and let $u = (u_1, \dots, u_n) \in \mathbb{Z}_p^n$. We will show that a is odd (as a permutation), i.e. $a \notin A_{2^n}$.

There are two cases of the action of a on u:

1° $u^a = u$ iff $a_n(u_1, \dots, u_{n-1}) = 0$.

2° $u^a = (u_1, \dots, u_{n-1}, u_n + 1)$ iff $a_n(u_1, \dots, u_{n-1}) = 1$.

Since $h(a_n) = 2^{n-1}$, the degree of a_n is equal to $n-1$. From Lemma 3 we know that an odd number of sequences $(u_1, \dots, u_n)$ is fixed by a. The number of all sequences from $\mathbb{Z}_2^n$ is 2^n, which is an even number, so also a number of sequences from 2° is odd. Thus, a is a product of odd number of transpositions, so $a \notin A_{2^n}$.

Now let

$$g = [g_1, g_2(x_1), \dots, g_{n-1}(X_{n-2}), 0] \in \mathrm{Syl}_2(S_{2^n}).$$

Every orbit O_{n-1} of the tableau $\overline{g} = [g_1, \dots, g_{n-1}(X_{n-2})]$ on $\mathbb{Z}_2^{n-1}$ corresponds to two orbits O_n' and O_n'' of g on $\mathbb{Z}_2^n$ of the form

$$O_n' = O_{n-1} \times \{0\} = \{(u_1, \dots, u_{n-1}, 0) : (u_1, \dots, u_{n-1}) \in O_{n-1}\}$$

and

$$O_n'' = O_{n-1} \times \{1\} = \{(u_1, \dots, u_{n-1}, 1) : (u_1, \dots, u_{n-1}) \in O_{n-1}\}.$$

Thus number of orbits of g on $\mathbb{Z}_2^n$ is even, so g is an even permutation.

Every element

$$f = [f_1, f_2(x_1), \dots, f_n(X_{n-1})] \in \mathrm{Syl}_2(S_{2^n})$$

can be expressed as $f = a' \cdot g'$, where

$$a' = [0, \dots, 0, f_n(X_{n-1})],$$
$$g' = [f_1, f_2(x_1), \dots, f_{n-1}(X_{n-2}), 0].$$

As we have shown before in this proof, g' is even.

If $h(f_n) = 2^{n-1}$, then a' is odd. So $a' \cdot g'$ is odd. Thus, $f \notin A_{2^n}$.

If $h(f_n) < 2^{n-1}$, then a' can be presented as a product of tableaux of form $[0, 0, \dots, z]$, where z is constant or z is a monomial $x_{i_1} x_{i_2} \dots x_{i_l}$, where

$$1 \leq i_1 < i_2 < \dots < i_l < n - 1.$$

Every permutation of such type is a product of an even number of transpositions, because degree of a monomial z is less than $n-1$. Hence a' in this case is even as a product of even permutations, so $f \in A_{2^n}$. □

From Theorem 4 we get the following

Corollary 5. $h(\mathrm{Syl}_2(A_{2^n})) = [1, 2, \dots, 2^{n-2}, 2^{n-1} - 1]$.

4. Main results

Facts shown in the previous sections can be now used to present our main statement, i.e. the construction of involution bases of Sylow 2-subgroups of the symmetric and alternating group. Let (t', t'') be the transposition, which moves t' to t'', where $t' \neq t''$. We will use the notation $\prod_{i=1}^{j} (\tau_i', \tau_i'')$ for a product of transpositions.

Theorem 6. *Let*

$$\alpha_k = \prod_{i=1}^{2^{n-k}} \left(i,\, 2^{n-k} + i\right)$$

for $k = 1, \dots, n$ *and let*

$$\beta = (1,\, 2)(2^{n-1} + 1,\, 2^{n-1} + 2).$$

Then $\langle \alpha_1, \dots, \alpha_{n-1}, \alpha_n \rangle$ *is a base of* $\mathrm{Syl}_2(S_{2^n})$ *and* $\langle \alpha_1, \dots, \alpha_{n-1}, \beta \rangle$ *is a base of* $\mathrm{Syl}_2(A_{2^n})$.

Proof. Let $m(X_i)$ be the polynomial on $\{x_1, \dots, x_i\}$ with all coefficients equal to 1, e.g.

$$m(X_3) = x_1x_2x_3 + x_1x_2 + x_1x_3 + x_2x_3 + x_1 + x_2 + x_3 + 1.$$

Let $a_1 = [1, 0, \dots, 0]$ and for all $i = 2, \dots, n$ let a_i be a tableau with the unique nonzero element on k-th position, equal to $m(X_{k-1})$:

$$\begin{aligned} a_2 &= [0, x_1 + 1, 0, \dots, 0, 0], \\ a_3 &= [0, 0, x_1x_2 + x_1 + x_2 + 1, \dots, 0, 0] \\ &\vdots \\ a_n &= [0, 0, 0, \dots, 0, m(X_{n-1})], \end{aligned}$$

and let

$$b = m(X_{n-1}) - x_1x_2 \dots x_{n-1}.$$

Simple calculations show that $\alpha_k = a_k$ for all $k = 1, \dots, n$ and $\beta = b$. Now, recall that

$$h(m(X_{n-1})) = 2^{n-1}$$

and

$$h(b) = 2^{n-1} - 1.$$

Let $G_a = \langle a_1, \dots, a_n \rangle$ and $G_b = \langle a_1, \dots, a_{n-1}, b \rangle$. Then

$$\begin{aligned} h(G_a) &= [1, 2^1, 2^2, \dots, 2^{n-2}, 2^{n-1}], \\ h(G_b) &= [1, 2^1, 2^2, \dots, 2^{n-2}, 2^{n-1} - 1]. \end{aligned}$$

so G_a is isomorphic to $\mathrm{Syl}_2(S_{2^n})$ and G_b is isomorphic to $\mathrm{Syl}_2(A_{2^n})$. Thus,

$$\mathrm{Syl}_2(S_{2^n}) = \langle \alpha_1, \dots, \alpha_{n-1}, \alpha_n \rangle$$

and

$$\mathrm{Syl}_2(A_{2^n}) = \langle \alpha_1, \dots, \alpha_{n-1}, \beta \rangle.$$

□

The base $a_1, \dots, a_n$ used in the above proof is an example of the so-called diagonal base of group $\mathrm{Syl}_2(S_{2^n})$ (that is a base made of tableaux $t_1, \dots, t_n$ for which the unique nonzero element of i-th tableau is on i-th position). We also note that every diagonal base is an involutive base.

Acknowledgment

The author would like to thank to the anonymous reviewer for his valuable comments and suggestions.

References

1. Bajorska-Harapińska B.: *On the group normally generated by the binary adding machine*. Unpublished.
2. Bier A., Sushchansky V.: *Kaluzhnin's representations of Sylow p-subgropus of automorphism groups of p-adic rooted trees*. Algebra Discrete Math. **19**, no. 1 (2015), 19–38.
3. Dixon J.D., Mortimer B.: *Permutation Groups*. Springer-Verlag, New York 1996.
4. Kaluzhnin L.: *La structure des p-groupes de Sylow des groupes symetriques finis*. Ann. Sci. l'Ecole Norm. Sup. **65** (1948), 239–272.
5. Sushchansky V., Słupik A.: *Minimal generating sets and Cayley graphs of Sylow p-subgroups of finite symmetric groups*. Algebra Discrete Math. **4** (2009), 167–184.