Archivum Mathematicum

Yvona Coufalová

Polynomials over the permutation group of three elements

Archivum Mathematicum, Vol. 16 (1980), No. 2, 67--79

Persistent URL: http://dml.cz/dmlcz/107058

ARCH. MATH. 2, SCRIPTA FAC. SCI. NAT. UJEP BRUNENSIS
XVI: 67—80, 1980

POLYNOMIALS OVER THE PERMUTATION GROUP OF THREE ELEMENTS

YVONA COUFALOVÁ, Brno

(Received March 26, 1979)

The purpose of this paper is to determine the number of all the different polynomials of two variables with all the coefficients equal to the unit of the group, over the premutation group of three elements.

Let us first make a few remarks concerning the above problem. By a polynomial of n variables where n is an arbitrary positive integer over an arbitrary given group $(G, .)$ we generally understand any mapping of the Cartesian product G^n into G, in the form

$$a_0 \prod_{i=1}^{k} x_1^{r_i} x_2^{s_i} \dots x_n^{t_i} a_i;$$

k is an arbitrary positive integer, $r_i, s_i, \dots, t_i$ are, for $1 \leqq i \leqq k$, non-negative integers, $a_0, a_1, \dots, a_k$ are elements of the given group, called coefficients of the polynomial; $x_1, x_2, \dots, x_n$, called the variables of a given polynomial, run over all the elements of the group (see e.g. [1]). To determine the number and the list of all the different polynomials, thus defined, over an arbitrary group seems a rather difficult problem. Trying to solve it, at least a part of it, I proceeded in the following way: first, I determined the number and the list of all the polynomials of n variables whose coefficients equal the unit of the group, over an arbitrary Abelian group with a torsion. The result is given in [2] and proves that the number of all these different polynomials equals the least common multiple of the orders of all the elements of the given group, raised to n. Further, I considered the number of all the different polynomials of one variable with coefficients equal to the unit of the given group, over a non-Abelian group with a torsion. I arrived at the conclusion [3] that the number of all these different polynomials equals the least common multiple of the orders of all the elements of a given group. Furthermore, I considered the number of all the different polynomials of two variables with all the coefficients equal to the unit of the group, over a non-Abelian group of a small order. For that purpose I have chosen the permutation group of three elements, further denoted by $(S_3, .)$ or simply S_3.

To determine the number of all these different polynomials is the principal object of this work. The result is presented in Theorem 1, § 2. There is also the list of some of the different polynomials in question from which the procedure of determining all these polynomials follows (the complete list is in [4]). The number of all the different polynomials of three variables with coefficients equal to the unit of the group, over S_3, is found in § 3; but there is no proof of this formula. The last paragraph of the present paper generalizes the above theory for an arbitrary positive integer n and ends with a formula determining the number of all the different polynomials of n variables with coefficients equal to the unit of the group, over S_3; there is no proof of the formula.

Let us add that by a polynomial we mean, throughout the paper, a polynomial over the group S_3, all the coefficients of which are equal to the unit of the group S_3. The equality of two polynomials as well as the elementary notions concerning the group S_3 are introduced in § 1.

The problem was suggested to me by RNDr. Milan Sekanina, CSc., to whom I am grateful for valuable advice concerning the present work.

§ 1. THE EQUALITY OF POLYNOMIALS; GROUP S_3

Definition 1. *Two polynomials $f(x_1, x_2, \ldots, x_n)$, $g(x_1, x_2, \ldots, x_n)$ over the group S_3 are equal iff there holds, for any n elements $\alpha_i \in S_3$, $i = 1, 2, \ldots, n$*

$$f(\alpha_1, \alpha_2, \ldots, \alpha_n) = g(\alpha_1, \alpha_2, \ldots, \alpha_n).$$

Let us denote the elements of the permutation group S_3 of three elements as follows:

$$e = \begin{pmatrix}123\\123\end{pmatrix}, \quad a = \begin{pmatrix}123\\132\end{pmatrix}, \quad b = \begin{pmatrix}123\\213\end{pmatrix}, \quad c = \begin{pmatrix}123\\231\end{pmatrix}, \quad d = \begin{pmatrix}123\\312\end{pmatrix}, \quad f = \begin{pmatrix}123\\321\end{pmatrix}.$$

For the orders of the above elements there holds: $0(e) = 1$, $0(a) = 0(b) = 0(f) = 2$, $0(c) = 0(d) = 3$. Let us select, from the six possible pairs of generators of the group S_3, for example, the pair a, c. There holds

$$ca = ac^2$$

from which

$$ca^m = a^m c^{2m}$$

and therefore

$$(a^m c^n)^r = a^{mr} c^{n \frac{2^{mr}-1}{2^m-1}} \qquad \text{for } m \neq 0.$$

Since a, c are generators of S_3 and $0(a) = 2$, $0(c) = 3$, there holds

$$(\forall\, x \in S_3)\, (\exists\, m \in \{0, 1\})\, (\exists\, n \in \{0, 1, 2\})\, [x = a^m c^n].$$

§ 2. POLYNOMIALS $f(x_1, x_2)$ OVER S_3

Theorem 1. *There exist exactly* $6^2 . 3^3$ *different polynomials* $f(x_1, x_2)$ *of two variables over the group* S_3.

Proof. From the introduction of the present paper there follows that every polynomial of two variables over S_3 has the form

$$f(x_1, x_2) = x_1^{r_1} . x_2^{s_1} . x_1^{r_2} . x_2^{s_2} . \dots . x_1^{r_k} . x_2^{s_k}.$$

Since x_1, x_2 run over all the elements of S_3, there holds $f(x_1, x_2) = (a^m c^n)^{r_1} . (a^p c^q)^{s_1} . (a^m c^n)^{r_2} . (a^p c^q)^{s_2} . \dots . (a^m c^n)^{r_k} . (a^p c^q)^{s_k}$, where $m, p \in \{0, 1\} \wedge n, q \in \{0, 1, 2\}$.

The values $f(x_1, x_2)$ for $m \neq 0 \wedge p \neq 0$, i.e., the following forms of the numbers 22, 23, 24, 28, 29, 30, 34, 35, 36 in Table 1, can easily be determined by means of the formula

$$f(x_1, x_2) = (a^m c^n)^{r_1} (a^p c^q)^{s_1} \dots (a^m c^n)^{r_k} (a^p c^q)^{s_k} =$$

$$= a^{m \sum_1^k r_i + p \sum_1^k s_i} . c^{\mathrm{EXP}_k},$$

where

$$\mathrm{EXP}_k = \frac{n}{2^m - 1} (2^{m \sum_1^k r_i + p \sum_1^k s_i} - 2^{m \sum_2^k r_i + p \sum_1^k s_i} + \dots + 2^{mr_k + ps_k} - 2^{ps_k}) +$$

$$+ \frac{q}{2^p - 1} (2^{m \sum_2^k r_i + p \sum_1^k s_i} - 2^{m \sum_2^k r_i + p \sum_2^k s_i} + \dots + 2^{ps_k} - 1).$$

Thus we get, on the whole, the following possibilities of the values of the polynomial $f(x_1, x_2) = a^{\mathrm{Exp}_{fa}} . c^{\mathrm{Exp}_{fc}}$ (we write only the exponents Exp_{f_a}, Exp_{f_c}):

Table 1

	m	n	p	q	Exp_{f_a}	Exp_{f_c}
1	0	0	0	0	0	0
2	0	0	0	1	0	$\sum_1^k s_i$
3	0	0	0	2	0	$2 \sum_1^k s_i$
4	0	0	1	0	$\sum_1^k s_i$	0

Table 1 (Vorsetzung)

	m	n	p	q	Exp_{f_a}	Exp_{f_c}
5	0	0	1	1	$\sum_1^k s_i$	$2^{\sum_1^k s_i} - 1$
6	0	0	1	2	$\sum_1^k s_i$	$2 . (2^{\sum_1^k s_i} - 1)$
7	0	1	0	0	0	$\sum_1^k r_i$
8	0	1	0	1	0	$\sum_1^k r_i + \sum_1^k s_i$
9	0	1	0	2	0	$\sum_1^k r_i + 2 \sum_1^k s_i$
10	0	1	1	0	$\sum_1^k s_i$	$r_1 . 2^{\sum_1^k s_i} + r_2 . 2^{\sum_2^k s_i} + \ldots + r_k . 2^{s_k}$
11	0	1	1	1	$\sum_1^k s_i$	$r_1 2^{\sum_1^k s_i} + 2^{\sum_1^k s_i} + r_2 2^{\sum_2^k s_i} + \ldots + r_k 2^{s_k} - 1$
12	0	1	1	2	$\sum_1^k s_i$	$r_1 2^{\sum_1^k s_i} + 2 . 2^{\sum_1^k s_i} + r_2 2^{\sum_2^k s_i} + \ldots + r_k 2^{s_k} - 2$
13	0	2	0	0	0	$2 \sum_1^k r_i$
14	0	2	0	1	0	$2 \sum_1^k r_i + \sum_1^k s_i$
15	0	2	0	2	0	$2 \sum_1^k r_i + 2 \sum_1^k s_i$
16	0	2	1	0	$\sum_1^k s_i$	$2 . (r_1 2^{\sum_1^k s_i} + r_2 2^{\sum_2^k s_i} + \ldots + r_k 2^{s_k})$
17	0	2	1	1	$\sum_1^k s_i$	$2^{\sum_1^k s_i} - 1 + 2 . (r_1 2^{\sum_1^k s_i} + r_2 2^{\sum_2^k s_i} + \ldots + r_k 2^{s_k})$
18	0	2	1	2	$\sum_1^k s_i$	$2 . (2^{\sum_1^k s_i} - 1) + 2 . (r_1 2^{\sum_1^k s_i} + r_2 2^{\sum_2^k s_i} + \ldots + r_k 2^{s_k})$

Table 1 (Vorsetzung)

	m	n	p	q	Exp_{f_a}	Exp_{f_c}
19	1	0	0	0	$\sum_1^k r_i$	0
20	1	0	0	1	$\sum_1^k r_i$	$s_1 . 2^{\sum_2^k r_i} + s_2 . 2^{\sum_3^k r_i} + \ldots + s_k$
21	1	0	0	2	$\sum_1^k r_i$	$2 . (s_i 2^{\sum_2^k r_i} + s_2 2^{\sum_3^k r_i} + \ldots + s_k)$
22	1	0	1	0	$\sum_1^k r_i + \sum_1^k s_i$	0
23	1	0	1	1	$\sum_1^k r_i + \sum_1^k s_i$	$2^{\sum_2^k r_i + \sum_1^k s_i} - 2^{\sum_2^k r_i + \sum_2^k s_i} + 2^{\sum_3^k r_i + \sum_2^k s_i} - \ldots - 1$
24	1	0	1	2	$\sum_1^k r_i + \sum_1^k s_i$	$2 . (2^{\sum_2^k r_i + \sum_1^k s_i} - 2^{\sum_2^k r_i + \sum_2^k s_i} + \ldots + 2^{s_k} - 1)$
25	1	1	0	0	$\sum_1^k r_i$	$2^{\sum_1^k r_i} - 1$
26	1	1	0	1	$\sum_1^k r_i$	$2^{\sum_1^k r_i} - 1 + (s_1 2^{\sum_2^k r_i} + s_2 2^{\sum_3^k r_i} + \ldots + s_k)$
27	1	1	0	2	$\sum_1^k r_i$	$2^{\sum_1^k r_i} - 1 + 2 . (s_1 2^{\sum_2^k r_i} + s_2 2^{\sum_3^k r_i} + \ldots + s_k)$
28	1	1	1	0	$\sum_1^k r_i + \sum_1^k s_i$	$2^{\sum_1^k r_i + \sum_1^k s_i} - 2^{\sum_2^k r_i + \sum_1^k s_i} + \ldots + 2^{r_k + s_k} - 2^{s_k}$
29	1	1	1	1	$\sum_1^k r_i + \sum_1^k s_i$	$2^{\sum_1^k r_i + \sum_1^k s_i} - 1$
30	1	1	1	2	$\sum_1^k r_i + \sum_1^k s_i$	$2^{\sum_1^k r_i + \sum_1^k s_i} - 1 + 2^{\sum_2^k r_i + \sum_1^k s_i} - 2^{\sum_2^k r_i + \sum_2^k s_i} + \ldots - 1$
31	1	2	0	0	$\sum_1^k r_i$	$2 . (2^{\sum_1^k r_i} - 1)$
32	1	2	0	1	$\sum_1^k r_i$	$2 . (2^{\sum_2^k r_i} - 1) + s_1 2^{\sum_1^k r_i} + s_2 2^{\sum_3^k r_i} + \ldots + s_k$

Table 1 (Vorsetzung)

	m	n	p	q	Exp_{f_a}	Exp_{f_c}
33	1	2	0	2	$\sum_1^k r_i$	$2.(2^{\sum_1^k r_i} - 1) + 2.(s_1 2^{\sum_2^k r_i} + s_2 2^{\sum_3^k r_i} + \ldots + s_k)$
34	1	2	1	0	$\sum_1^k r_i + \sum_1^k s_i$	$2.(2^{\sum_1^k r_i + \sum_1^k s_i} - 2^{\sum_2^k r_i + \sum_1^k s_i} + \ldots + 2^{s_k + r_k} - 2^{s_k})$
35	1	2	1	1	$\sum_1^k r_i + \sum_1^k s_i$	$2.2^{\sum_1^k r_i + \sum_1^k s_i} - (2^{\sum_2^k r_i + \sum_1^k s_i} - \ldots + 2^{s_k} - 1)$
36	1	2	1	2	$\sum_1^k r_i + \sum_1^k s_i$	$2.(2^{\sum_1^k r_i + \sum_1^k s_i} - 1)$

If, for two polynomials $f(x_1, x_2)$, $g(x_1, x_2)$ over S_3, there holds $f(x_1, x_2) = g(x_1, x_2)$, then there must, by Definition 1, hold

$$(\overset{1}{\underset{0}{\forall}} m)(\overset{2}{\underset{0}{\forall}} n)(\overset{1}{\underset{0}{\forall}} p)(\overset{2}{\underset{0}{\forall}} q)\,[(a^m c^n)^{r_1} . (a^p c^q)^{s_1} \ldots (a^m c^n)^{r_k} . (a^p c^q)^{s_k} =$$

$$= (a^m c^n)^{u_1} . (a^p c^q)^{v_1} \ldots (a^m c^n)^{u_k} . (a^p c^q)^{v_k}],$$

thus

$$a^{\mathrm{Exp}_{f_a}} . c^{\mathrm{Exp}_{f_c}} = a^{\mathrm{Exp}_{g_a}} . c^{\mathrm{Ezp}_{g_c}},$$

so that

$$[\mathrm{Exp}_{f_a} \equiv \mathrm{Exp}_{g_a} \pmod 2] \wedge [\mathrm{Exp}_{f_c} \equiv \mathrm{Exp}_{g_c} \pmod 3].$$

Hence, from the conditions 1–36, we get exactly five independent conditions:

A_2^1: $\sum_1^k r_i \equiv \sum_1^k u_i \pmod 6$,

A_2: $\sum_1^k s_i \equiv \sum_1^k v_i \pmod 6$,

A_2^3: $r_1 2^{\sum_1^k s_i} + r_2 2^{\sum_2^k s_i} + \ldots + r_k 2^{s_k} \equiv u_1 2^{\sum_1^k v_i} + u_2 2^{\sum_2^k v_i} + \ldots + u_k 2^{v_k} \pmod 3$,

A_2^4: $s_1 2^{\sum_2^k r_i} + s_2 2^{\sum_3^k r_i} + \ldots + s_k \equiv v_1 2^{\sum_2^k u_i} + v_2 2^{\sum_3^k u_i} + \ldots + v_k \pmod 3$,

A_2^5: $2^{\sum_2^k r_i + \sum_1^k s_i} - 2^{\sum_2^k r_i + \sum_2^k s_i} + \ldots + 2^{s_k} - 1 \equiv 2^{\sum_2^k u_i + \sum_1^k v_i} - 2^{\sum_2^k u_i + \sum_2^k v_i} + \ldots + 2^{v_k} - 1 \pmod 3$.

In fact, if we prove that the above 5 conditions are really independent, then the number of all the different polynomials of two variables over S_3 will equal the number

$$6^2 \,.\, 3^3 = 972.$$

Now let us prove the independence of the conditions $\mathrm{A}_2^1 - \mathrm{A}_2^5$ for $k = 4$, in the form:

(i): $\sum_1^4 r_i \equiv a_1 \pmod 6$,

(ii): $\sum_1^4 s_i \equiv a_2 \pmod 6$,

(iii): $r_1 2^{\sum_1^4 s_i} + r_2 2^{\sum_2^4 s_i} + r_3 2^{s_3+s_4} + r_4 2^{s_4} \equiv a_3 \pmod 3$,

(iv): $s_1 2^{\sum_2^4 r_i} + s_2 2^{r_3+r_4} + s_3 2^{r_4} + s_4 \equiv a_4 \pmod 3$,

(v): $2^{\sum_2^4 r_i + \sum_1^4 s_i} - 2^{\sum_2^4 r_i + \sum_2^4 s_i} + 2^{\sum_3^4 r_i + \sum_2^4 s_i} - 2^{\sum_3^4 r_i + \sum_3^4 s_i} + 2^{r_4 + \sum_3^4 s_i} - 2^{r_4+s_4} + 2^{s_4} - 1 \equiv$
$\equiv a_5 \pmod 3$.

Remark 1. Since $2^n \equiv (-1)^n \pmod 3$, there follows $2^{\text{odd number}} \equiv -1 \pmod 3$ and $2^{\text{even number}} \equiv 1 \pmod 3$.

The independence of (i)–(v) can be proved by finding their solution by means of the method of elimination:

From the equation (i) there follows $r_1 \equiv a_1 - \sum_2^4 r_i \pmod 6$. From the equation (ii) we get

$$s_1 \equiv a_2 - \sum_2^4 s_i \pmod 6.$$

The equation (iv) implies

$$(a_2 - \sum_2^4 s_i) \,.\, 2^{\sum_2^4 r_i} + s_2 2^{r_3+r_4} + s_3 2^{r_4} + s_4 \equiv a_4 \pmod 3,$$

hence

$$s_2(2^{r_3+r_4} - 2^{\sum_2^4 r_i}) \equiv a_4 + 2^{\sum_2^4 r_i} (s_3 + s_4 - a_2) - s_3 2^{r_4} - s_4 \pmod 3.$$

So that we have

$$s_2 \,.\, 2^{r_3+r_4} \,.\, (1 - 2^{r_2}) \equiv a_4 + 2^{\sum_2^4 r_i} (s_3 + s_4 - a_2) - s_3 2^{r_4} - s_4 \pmod 3.$$

Suppose $r_3 + r_4$ to be even and r_2 odd, that is to say, r_2, r_3, r_4 will be chosen so that the above two conditions are satisfied. Hence we get

$$s_2 \equiv -a_4 - 2s_3 - 2s_4 + 2a_2 + s_3 2^{r_4} + s_4 \pmod 3,$$
$$s_2 \equiv -a_4 - 2s_3 - s_4 + 2a_2 + s_3 2^{r_4} \pmod 3,$$
$$s_2 = -a_4 - 2s_3 - s_4 + 2a_2 + s_3 2^{r_4} + 3l.$$

Consequently:

$$s_2 = -a_4 + 2a_2 - 2s_3 - s_4 + s_3 2^{r_4} + 3l.$$

From the equation (iii) there follows

$$(a_1 - \sum_2^4 r_i) \,.\, 2^{a_2} + r_2 \,.\, 2^{-a_4+3l+s_3} + r_3 \,.\, 2^{s_3+s_4} + r_4 2^{s_4} \equiv a_3 \pmod 3,$$

for $r_4 \neq 0$. Let all the $r_i, s_i, a_i \neq 0$. So that

$$r_2(2^{-a_4+s_3+3l} - 2^{a_2}) \equiv a_3 + 2^{a_2} \,.\, (r_3 + r_4 - a_1) - r_3 2^{s_3+s_4} - r_4 2^{s_4} \pmod 3.$$

Now consider two cases according as a_2 is even or odd.

A. a_2 even

Furthermore, suppose $-a_4 + s_3 + 3l$ is odd. If it were even, then a_4 in equation (iv) would be greater by 3. This would only change the parity of $-a_4 + s_3 + 3l$ because we should get $-a_4 - 3 + s_3 + 3l$, which would be odd. Consequently, whether a_4, s_3 is odd or even, we can arrange the expression $-a_4 + s_3 + 3l$ to be odd without changing the validity of the equation (i)–(v). Hence

$$r_2 \equiv a_3 + r_3 + r_4 - a_1 - r_3 2^{s_3+s_4} - r_4 2^{s_4} \pmod 3,$$

so that

$$r_2 = a_3 - a_1 + r_3 + r_4 - r_3 2^{s_3+s_4} - r_4 2^{s_4} + 3l'.$$

Since r_2 is odd, the above equation is true only if the expression $a_3 - a_1 + 3l'$ is odd. If the latter is not odd, we change the parity by increasing a_3 by 3.

From the equation (v) there follows

$$2^{\text{odd}+a_2} - 2^{\text{odd}-a_4+3l+s_3} + 2^{\text{even}-a_4+3l+s_3} - 2^{\text{even}+s_3+s_4} + 2^{r_4+s_3+s_4} -$$
$$- 2^{r_4+s_4} + 2^{s_4} - 1 \equiv a_5 \pmod 3,$$

hence

$$- 2^{s_3+s_4} + 2^{r_4+s_3+s_4} - 2^{r_4+s_4} + 2^{s_4} - 1 \equiv a_5 \pmod 3,$$

and consequently

$$2^{s_4} \,.\, (1 - 2^{r_4} + 2^{r_4+s_3} - 2^{s_3}) \equiv a_5 + 1 \pmod 3.$$

Let us now consider three different cases according as $a_5 \equiv 0 \pmod 3$, or $a_5 \equiv 1 \pmod 3$, or $a_5 \equiv 2 \pmod 3$.

I. $a_5 \equiv 0 \pmod 3$.
Then

$$2^{s_4} . (1 - 2^{r_4} + 2^{r_4+s_3} - 2^{s_3}) \equiv 1 \pmod 3.$$

The above equation is true if we choose s_4 even and r_4 odd and s_3 odd because

$$L = 2^{\text{even}} . (1 - 2^{\text{odd}} + 2^{\text{even}} - 2^{\text{odd}}) \equiv -2 \equiv 1 = R \pmod 3.$$

Hence $s_3 = 2\alpha + 1$. Inserting into r_2, s_2, s_1, r_1, we get the solution of equations (i)–(v):

$$\begin{aligned}
r_1 &= 2a_1 + 6n_1 - a_3 - 3l' - 2r_3 - 2r_4 + r_3 . 2^{2\alpha+1+s_4} + r_4 2^{s_4},\\
r_2 &= a_3 + 3l' - a_1 + r_3 + r_4 - r_3 . 2^{2\alpha+1+s_4} - r_4 . 2^{s_4},\\
s_1 &= a_2 + 6n_2 + a_4 - 2a_2 - 2\alpha . 2^{r_4} - 2^{r_4} - 3l + 2\alpha + 1,\\
s_2 &= -a_4 + 2a_2 - 4\alpha - 2 - s_4 + 2\alpha . 2^{r_4} + 2^{r_4} + 3l.
\end{aligned}$$

II. $a_5 \equiv 1 \pmod 3$
Then

$$2^{s_4} . (1 - 2^{r_4} + 2^{r_4+s_3} - 2^{s_3}) \equiv 2 \pmod 3.$$

This equation is true if we choose s_4 odd and s_3 odd and r_4 odd because

$$L = 2^{\text{odd}} . (1 - 2^{\text{odd}} + 2^{\text{even}} - 2^{\text{odd}}) \equiv 2 = R \pmod 3.$$

Consequently $s_3 = 2\alpha + 1$. The solution of equation (i)–(v) is the same as in A.I. but for a different condition as to s_4.

III. $a_5 \equiv 2 \pmod 3$
Then

$$2^{s_4} . (1 - 2^{r_4} + 2^{r_4+s_3} - 2^{s_3}) \equiv 0 \pmod 3.$$

This equation is true if we choose s_3 even and r_4 even because

$$L = 2^{s_4} . (1 - 2^{\text{even}} + 2^{\text{even}} - 2^{\text{even}}) \equiv 0 = R \pmod 3.$$

Hence $s_3 = 2\alpha$. Inserting into r_2, s_2, s_1, r_1, we obtain the solution of equations (i)–(v) of the form

$$\begin{aligned}
r_1 &= 2a_1 - a_3 + 6n_1 - 2r_3 - 2r_4 + r_3 2^{s_4} + r_4 2^{s_4} - 3l'\\
r_2 &= a_3 - a_1 + r_3 + r_4 - r_3 2^{s_4} - r_4 2^{s_4} + 3l'\\
s_1 &= -a_2 + a_4 + 6n_2 - 3l\\
s_2 &= -a_4 + 2a_2 - 2\alpha - s_4 + 3l\\
s_3 &= 2\alpha.
\end{aligned}$$

Now it remains to consider the case

B. a_2 odd

Suppose that $-a_4 + s_3 + 3l$ is even. Again, as in case **A.**, this condition can always be satisfied. Thus

$$r_2 \equiv -a_3 - 2r_3 - 2r_4 + 2a_1 + r_3 2^{s_3+s_4} + r_4 2^{s_4} \pmod 3,$$

so that

$$r_2 = -a_3 + 3l'' - 2r_3 - 2r_4 + 2a_1 + r_3 2^{s_3+s_4} + r_4 2^{s_4}.$$

Now, on condition that r_2 is odd, we get that $-a_3 + 3l''$ is odd, which can always be arranged by a convenient choice of a_3. From the equation (v) there follows

$$2^{s_4} . (1 - 2^{r_4} - 2^{r_4+s_3} - 2^{s_3}) \equiv a_5 + 1 \pmod 3,$$

which is the same equation as in case **A.** and the theorem is proved.

Remark 2. So we have proved that, to enumerate all the polynomials, it is sufficient to consider the products of eight factors. From the enumeration in [4] it is clear that even six factors are sufficient.

For $k = 3$ the equations (i)–(v) have the form (we write only the left sides of these equations):

$$r_1 + r_2 + r_3 \pmod 6$$

$$s_1 + s_2 + s_3 \pmod 6$$

$$r_1 2^{s_1+s_2+s_3} + r_2 2^{s_2+s_3} + r_3 2^{s_3} \pmod 3$$

$$s_1 2^{r_2+r_3} + s_2 2^{r_3} + s_3 \pmod 3$$

$$2^{r_2+r_3+s_1+s_2+s_3} - 2^{r_2+r_3+s_2+s_3} + 2^{r_3+s_2+s_3} - 2^{r_3+s_3} + 2^{s_3} - 1 \pmod 3;$$

so that the polynomials $f(x_1, x_2)$ can be written in the form

Table 2

	$f(x_1, x_2)$	(i)	(ii)	(iii)	(iv)	(v)
1.	$x_1^0 . x_2^0 . x_1^0 . x_2^0 . x_1^0 . x_2^0$	0 (mod 6)	0 (mod 6)	0 (mod 3)	0 (mod 3)	0 (mod 3)
2.	$x_1^2 . x_2^1 . x_1^3 . x_2^3 . x_1^1 . x_2^2$	0 (mod 6)	0 (mod 6)	0 (mod 3)	0 (mod 3)	1 (mod 3)
3.	$x_1^3 . x_2^3 . x_1^3 . x_2^3 . x_1^0 . x_2^0$	0 (mod 6)	0 (mod 6)	0 (mod 3)	0 (mod 3)	2 (mod 3)
4.	$x_1^1 . x_2^4 . x_1^5 . x_2^2 . x_1^0 . x_2^0$	0 (mod 6)	0 (mod 6)	0 (mod 3)	1 (mod 3)	0 (mod 3)
5.	$x_1^2 . x_2^1 . x_1^3 . x_2^1 . x_1^1 . x_2^4$	0 (mod 6)	0 (mod 6)	0 (mod 3)	1 (mod 3)	1 (mod 3)
	⋮					
972.	$x_1^0 . x_2^3 . x_1^5 . x_2^3 . x_1^0 . x_2^5$	5 (mod 6)	5 (mod 6)	2 (mod 3)	2 (mod 3)	2 (mod 3)

§ 3. POLYNOMIALS $f(x_1, x_2, x_3)$ OVER S_3

Every polynomial of three variables over S_3 is of the form

$$f(x_1, x_2, x_3) = x_1^{r_1} . x_2^{s_1} . x_3^{t_1} . x_1^{r_2} . x_2^{s_2} . x_3^{t_2} . \dots . x_1^{r_k} . x_2^{s_k} . x_3^{t_k}.$$

Since x_1, x_2, x_3 run over all the elements of S_3, there holds

$$f(x_1, x_2, x_3) = (a^m . c^n)^{r_1} . (a^p . c^q)^{s_1} . (a^\alpha . c^\beta)^{t_1} . \dots . (a^m . c^n)^{r_k} . (a^p . c^q)^{s_k} . (a^\alpha . c^\beta)^{t_k},$$

where $m, p, \alpha \in \{0, 1\}$ and $n, q, \beta \in \{0, 1, 2\}$. So we get $2^3 . 3^2$ different possibilities of the values of the polynomial $f(x_1, x_2, x_3)$. But from these possibilities we only get the following probably independent conditions for the equality of two polynomials (we write only the left sides of the congruences):

A_3^1: $\sum_1^k r_i \pmod 6$

A_3^2: $\sum_1^k s_i \pmod 6$

A_3^3: $\sum_1^k t_i \pmod 6$

A_3^4: $r_1 2^{\sum_1^k s_i} + \dots + r_k 2^{s_k} \pmod 3$

A_3^5: $r_1 2^{\sum_1^k t_i} + \dots + r_k 2^{t_k} \pmod 3$

A_3^6: $r_1 2^{\sum_1^k s_i + \sum_1^k t_i} + \dots + r_k 2^{s_k + t_k} \pmod 3$

A_3^7: $s_1 2^{\sum_2^k r_i} + \dots + s_k \pmod 3$

A_3^8: $s_1 2^{\sum_1^k t_i} + \dots + s_k 2^{t_k} \pmod 3$

A_3^9: $s_1 2^{\sum_2^k r_i + \sum_1^k t_i} + \dots + s_k 2^{t_k} \pmod 3$

A_3^{10}: $t_1 2^{\sum_2^k r_i} + \dots + t_k \pmod 3$

A_3^{11}: $t_1 2^{\sum_2^k s_i} + \dots + t_k \pmod 3$

A_3^{12}: $t_1 2^{\sum_2^k r_i + \sum_2^k s_i} + \dots + t_k \pmod 3$

$$A_3^{13}:\quad 2^{\sum_2^k r_i+\sum_1^k s_i} - 2^{\sum_2^k r_i+\sum_2^k s_i} + \ldots + 2^{s_k} - 1 \pmod 3$$

$$A_3^{14}:\quad 2^{\sum_2^k r_i+\sum_1^k t_i} - 2^{\sum_2^k r_i+\sum_2^k t_i} + \ldots + 2^{t_k} - 1 \pmod 3$$

$$A_3^{15}:\quad 2^{\sum_2^k si+\sum_1^k t_i} - 2^{\sum_2^k s_i+\sum_2^k t_i} + \ldots + 2^{t_k} - 1 \pmod 3$$

$$A_3^{16}:\quad 2^{\sum_2^k r_i+\sum_2^k s_i+\sum_1^k t_i} - 2^{\sum_2^k r_i+\sum_2^k s_i+\sum_2^k t_i} + \ldots + 2^{t_k} - 1 \pmod 3$$

$$A_3^{17}:\quad 2^{\sum_2^k r_i+\sum_1^k s_i+\sum_1^k t_i} - 2^{\sum_2^k r_i+\sum_2^k s_i+\sum_1^k t_i} + \ldots + 2^{s_k+t_k} - 2^{t_k} \pmod 3.$$

From these conditions it follows that the number of polynomials of three variables over S_3 equals the number $6^3 . 3^{14}$.

§ 4. POLYNOMIALS $f(x_1, x_2, \ldots, x_n)$ OVER S_3

In the same way as in § 2. we could derive the conditions for the equality of two polynomials of n variables over S_3, namely n conditions with regard to modul 6. The number of conditions with regard to modul 3 is:

$$(n-1)n + \binom{n-1}{2}n + \binom{n-1}{3}n + \ldots + \binom{n-1}{n-1}n +$$
$$+ \binom{n}{2} + \binom{n}{3}2 + \binom{n}{4}3 + \ldots + \binom{n}{n}(n-1) =$$
$$= \underbrace{n\left[\binom{n-1}{1} + \binom{n-1}{2} + \binom{n-1}{3} + \ldots + \binom{n-1}{n-1}\right]}_{P} + \underbrace{\sum_{k=1}^{n-1} k\binom{n}{k-1}}_{Q}.$$

Hence $P = n . (2^{n-1} - 1)$ and for Q we get

$$(k+1)\binom{n}{k+1} = n\binom{n-1}{k},$$
$$k\binom{n}{k+1} = (k+1)\binom{n}{k+1} - \binom{n}{k+1},$$
$$k\binom{n}{k+1} = n\binom{n-1}{k} - \binom{n}{k+1},$$
$$\sum_{k=1}^{n-1} k\binom{n}{k+1} = n\sum_{k=1}^{n-1}\binom{n-1}{k} - \sum_{k=1}^{n-1}\binom{n}{k+1} = 2^{n-1}(n-2) + 1;$$

so that $P + Q = (2^n - 1) . (n - 1)$ and we can say that the number of different polynomials of n variables over S_3 is equal to

$$6^n . 3^{(n-1).(2^n-1)}.$$

CONCLUSION

The basic relation of the present paper is the relation $ca = ac^2$ between the generators a, c of the group S_3; that means that the product xy of two arbitrary elements of S_3 may be expressed in the form $y^u . x^v$ where u, v are integers. This is no longer possible for the group S_4. Consequently, the question of the number of all the differen polynomials over the group S_n $(n > 3)$ and, therefore, even over an arbitrary non-Abelian group, will probably have to be solved in a different way. The answer to this question will help to answer the original question proposed in the Introduction, concerning the number and the list of all the different polynomials of n variables with arbitrary coefficients over an arbitrary group.

REFERENCES

[1] Lausch, H., Nöbauer, W.: *Algebra of Polynomials.* North-Holland Mathematical Library. 1973.

[2] Coufalová, Y.: *Polynomy nad konečnými abelovskými grupami.* Sborník PedF UJEP. Brno. 1975.

[3] Coufalová, Y.: *Polynomy jedné proměnné nad neabelovskými grupami.* Sborník PedF UJEP. Brno. 1978.

[4] Coufalová, Y.: *Polynomy na grupě permutací ze tří prvků.* Brno. 1972. (Not published, kept at the Faculty of Sciences, UJEP.)

Y. Coufalová
662 80 Brno, Poříčí 31
Czechoslovakia