SYMMETRIC OPERATIONS IN GROUPS

BY

ERNEST PŁONKA (WROCŁAW)

Introduction. We say that an operation $f$ on $A$ (i.e., a function $f: A^n \to A$) is generated by a set $F$ of operations on $A$, if $f$ is a composition of some operations belonging to $F$ and some trivial operations (= identity operations).

Let $G$ be a group. We denote by $A^{(n)}(G)$ the set of all operations on the set $G$ which are generated by the operations $xy$ and $x^{-1}$, or, in other words, the set of all $n$-ary algebraic operations in $G$ (see [1]), or else, the set of all words of $n$ variables $x_1, \ldots, x_n$. The set $A^{(n)}(G)$ forms a group, the multiplication being defined by juxtaposition. In this group we distinguish the subgroup of all symmetric operations $S^{(n)}(G)$, that is the set of all words $s(x_1, \ldots, x_n)$ for which the equation

$$s(x_1, x_2, \ldots, x_n) = s(x_{o_1}, x_{o_2}, \ldots, x_{o_n})$$

holds for every $x_1, x_2, \ldots, x_n \in G$ and for all permutations $o \in S_n$.

The purpose of this paper is to study symmetric operations and the possibility of generating the group operation $xy$ by symmetric operations of many (in general) variables. The class of groups in which this turns out to be possible we denote by $\mathcal{X}$.

In section I we give a complete description of $S^{(n)}(G)$ for nilpotent groups of class 2 and for arbitrary $n$, and, in section II, for normal products of $Z_p$ and $Z_2$ for $n = 2$.

In section III we investigate the class $\mathcal{X}$. It is clear that abelian groups belong to $\mathcal{X}$, and E. Marczewski (cf. [2]) raised a question whether these are the only groups in $\mathcal{X}$. Unexpectedly enough, it turns out (see section IV) that $\mathcal{X}$ contains the symmetric group on three letters $S_3$. This leaves an open question of giving a more accurate description of the class $\mathcal{X}$ (P 684).

I. Nilpotent groups of class 2. Now we are going to determine the symmetric operations in the nilpotent groups of class 2. Let us recall the well-known identity

$$[x^n, y] = [x, y^n] = [x, y]^n.$$
THEOREM 1. If $G$ is a nilpotent group of class 2, then operation $f \in A^{(n)}(G)$ is symmetric if and only if

$$f(x_1, x_2, \ldots, x_n) = x_1^a x_2^a \cdots x_n^a \prod_{1 \leq j < i \leq n} [x_i, x_j]^b,$$

where $a, b$ are integers and

$$a^2 \equiv 2b(\exp G').$$

Proof. Every word $f$ in $G$ is of the form

$$f(x_1, x_2, \ldots, x_n) = x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n} \prod_{1 \leq j < i \leq n} [x_i, x_j]^{b_{ij}}$$

and the condition $f(x_1, x_2, \ldots, x_n) = f(x_2, x_3, x_4, \ldots, x_n)$ together with (1) yields

$$x_1^{a_1} \cdots x_n^{a_n} \prod_{1 \leq j < i \leq n} [x_i, x_j]^{b_{ij}}$$

$$= x_2^{a_1} x_2^{a_2} x_3^{a_3} \cdots x_n^{a_n} \prod_{3 \leq j < i \leq n} [x_i, x_j]^{b_{ij}} \prod_{3 \leq i < n} [x_i, x_1]^{b_{i1}} \prod_{3 \leq i < n} [x_i, x_2]^{b_{i2}} [x_1, x_2]^{b_{21}}$$

$$= x_1^{a_2} x_2^{a_1} x_3^{a_3} \cdots x_n^{a_n} \prod_{3 \leq i < n} [x_i, x_1]^{b_{i2}} \prod_{3 \leq i < n} [x_i, x_1]^{b_{i1}} \prod_{3 \leq j < i \leq n} [x_i, x_j]^{b_{ij}} [x_2, x_1]^{a_i a_2 - b_{21}}.$$

Hence we have

$$a_1 \equiv a_2(\exp G'),$$

$$a_1, a_2 \equiv 2b_{21}(\exp G'),$$

$$b_{i1} \equiv b_{i2}(\exp G'), \quad i = 3, 4, \ldots, n.$$  

From the condition $f(x_1, \ldots, x_n) = f(x_2, x_3, \ldots, x_n, x_1)$ we infer by (1) that

$$x_1^{a_1} \cdots x_n^{a_n} \prod_{1 \leq j < i \leq n} [x_i, x_j]^{b_{ij}}$$

$$= x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n-1} x_1^{a_1} \prod_{1 \leq j < i \leq n} [x_i+1, x_j+1]^{b_{ij}} \prod_{1 \leq j < n} [x_1, x_j+1]^{b_{nj}}$$

$$= x_1^{a_1} x_2^{a_1} \cdots x_n^{a_1} \prod_{2 \leq i < n} [x_i, x_1]^{a_i-1} \prod_{1 \leq j < n} [x_i+1, x_j+1]^{b_{ij}} \prod_{1 \leq j < n} [x_j+1, x_1]^{b_{nj}}.$$

This yields

$$a_1 \equiv a_2 \equiv \cdots \equiv a_n(\exp G'),$$

$$b_{ij} \equiv b_{i+1,j+1}(\exp G') \quad \text{for } 1 \leq j < i < n,$$

$$b_{i1} + b_{n,i-1} \equiv a_{i-1} a_n(\exp G') \quad \text{for } 2 \leq i \leq n.$$
Now we shall prove the theorem by induction on \( n \). For \( n = 1, 2, 3 \) our statement readily follows from (4), (5) and (6). Suppose that (4)-(9) imply (2) and (3) for \( n - 1 \) \( (n \geq 4) \). This means that
\[
 a_i \equiv a(\exp G) \quad \text{for } 1 \leq i \leq n - 1,
 b_{ij} \equiv b(\exp G') \quad \text{for } 1 \leq j < i \leq n - 1,
 a^2 \equiv 2b(\exp G').
\]
In view of (7) we have \( a_n \equiv a(\exp G) \), while for \( k \) such that \( 1 < k < n \) the relation \( b_{ni} \equiv b_{n-1,i-1}(\exp G') \) follows from (8). Now using (6) for \( i = n \) as well as the induction hypothesis, we conclude that every \( n \)-ary symmetric operation must be of the form (2), and (3) holds.

If \( a_i \equiv a(\exp G), b_{ij} \equiv b(\exp G') \) for \( 1 \leq i < j \leq n \) and (3) is satisfied, then (4)-(9) are satisfied too. And since the cycles \((1, 2) \) and \((1, 2, \ldots, n) \) generate the symmetric group \( S_n \), \( f \) is symmetric. Thus the proof is completed.

II. Normal products \( Z_pZ_2 \). Let us consider the normal product \( Z_pZ_2 \) of a cyclic group \( Z_p \) (for a prime \( p > 2 \)) and the group \( Z_2 \), i.e. the group of pairs \((\varepsilon, k)\), where \( \varepsilon = +1 \) or \(-1, k \in Z_p \), and the multiplication being defined by the equality
\[
(\varepsilon, k)(\eta, l) = (\varepsilon\eta, \eta k + l).
\]
For the sake of brevity we write \( k \) instead of \((1, k)\) and \( kb \) instead of \((-1, k), k \in Z_p \).

Let us begin with the two simple facts:

(i) The commutator subgroup of \( Z_pZ_2 \) is \( Z_p \).

(ii) For every \( 0 \leq i < p \) and \( 0 \leq j < p \) there exists precisely one automorphism \( \varphi \) of \( Z_pZ_2 \) for which \( \varphi(1) = i \) and \( \varphi(0b) = jb \).

To verify (ii) define
\[
\varphi(kb) = (j + ki)b, \quad \varphi(k) = ki \quad \text{for } 0 \leq k < p,
\]
and check that \( \varphi \) is an automorphism of \( Z_pZ_2 \).

Now we prove the following useful

**Lemma.** Let \( w, w' \in A^2(Z_pZ_2) \). If \( w, w' \) are equal on the pairs \( \langle 1, 0 \rangle, \langle 0, 1 \rangle, \langle 0b, 1 \rangle, \langle 0b, 1b \rangle, \langle 1b, 0b \rangle \), then \( w, w' \) are identical everywhere in \( Z_pZ_2 \).

**Proof.** Let
\[
w = x^{a_1}y^{b_1} \ldots x^{a_n}y^{b_n}, \quad w' = x'^{a_1}y^{b_1} \ldots x'^{m}y^{b_m}.
\]
If \( w(1, 0) = w'(1, 0) \) and \( w(0, 1) = w'(0, 1) \), then
\[
\sum a_i = \sum c_{i}(p), \quad \sum b_i = \sum d_{i}(p),
\]
and therefore for every \( k, l \) with \( 0 \leq k, \ l < p \) we have
\[
\omega(k, l) = k^{x_1} l^{x_2} = \omega'(k, l)(p).
\]

Since \( \omega \) and \( \omega' \) must commute with each automorphism \( \varphi \) of \( \mathbb{Z}_p \mathbb{Z}_2 \), therefore if
\[
\varphi(1) = k, \quad \varphi(0b) = k' b,
\]
then we have
\[
\omega(k, k' b) = \omega'(k, k' b) \quad \text{and} \quad \omega(k' b, k) = \omega'(k' b, k)
\]
for all \( k, k' \) such that \( 0 < k < p, 0 \leq k' < p \).

If \( 0 \leq k' < k < p \), then the mapping \( \varphi \) defined by
\[
\varphi(1) = k' - k, \quad \varphi(0b) = kb
\]
is, by (ii), an automorphism of \( \mathbb{Z}_p \mathbb{Z}_2 \), and
\[
\varphi(1b) = (k + k' - k)b = k'b.
\]

Hence
\[
\omega(kb, k' b) = \omega'(kb, k' b) \quad \text{and} \quad \omega(k' b, kb) = \omega'(k' b, kb)
\]
for any \( k, k' \) with \( 0 \leq k < k' < p \).

Further, the mapping
\[
(11) \quad e: \mathbb{Z}_p \mathbb{Z}_2 \to \mathbb{Z}_p \mathbb{Z}_2,
\]
where \( e(k) = 0 \), and \( e(kb) = 0b \) for \( 0 \leq k < p \), is an endomorphism of \( \mathbb{Z}_p \mathbb{Z}_2 \), and thus
\[
\begin{align*}
\omega(1, 0b) &= \omega(0, 0b) = \omega'(0, 0b) = \omega'(1, 0b), \\
\omega(0b, 1) &= \omega(0b, 0) = \omega'(0b, 0) = \omega'(0b, 1).
\end{align*}
\]

Hence
\[
\omega(0, kb) = \omega'(0, kb) \quad \text{and} \quad \omega(kb, 0) = \omega'(kb, 0)
\]
because \( kb (1 \leq k < p) \) is an image of \( 0b \) by an automorphism. Finally, we have
\[
\omega(kb, kb) = \omega(kb, 0)\omega(0, kb) = \omega'(kb, 0)\omega'(0, kb) = \omega'(kb, kb)
\]
for all \( k (0 \leq k < p) \).

The following theorem gives a description of the symmetric binary words in \( \mathbb{Z}_p \mathbb{Z}_2 \).

**Theorem 2.** We have
\[
S^{(2)}(\mathbb{Z}_p \mathbb{Z}_2) = \text{gp}\{w_p, u\} \cong \mathbb{Z}_p \times \mathbb{Z}_p \mathbb{Z}_2,
\]
where
\[
(12) \quad w_p(x, y) = xy[y, x]^{(p+1)/2}, \quad u(x, y) = x^2 y^2.
\]
Proof. Since
\[ w_p(y, x) = yx[x, y]^{(p+1)/2} = xy[y, x]^{-(p+1)/2+1} = xy[y, x]^{(p+1)/2} = w_p(x, y), \]
\[ u(y, x) = y^2x^2 = x^2y^2 = u(x, y), \]
we get the inclusion
\[ \text{gp}\{w_p, u\} \subseteq S^{(2)}(Z_p Z_2). \]

Now we show that if \( s \in S^{(2)}(Z_p Z_2) \), then
\[ s(0b, 1b) = 0. \]  
(13)
If \( s(x, y) = x^{a_1}y^{b_1} \cdots x^{a_n}y^{b_n} \), then from \( s(0, 0b) = s(0b, 0) \) we obtain
\[ \sum a_i \equiv \sum b_i(2). \]

Consequently,
\[ s(0b, 0b) = 0^{\Sigma a_i}0b^{\Sigma b_i} = 0b^{\Sigma a_i+\Sigma b_i} = 0. \]  
(14)
Because \( s \) commutes with the endomorphism \( e \) defined in (11), the equality (14) implies
\[ 0 = s(0b, 0b) = s(e(0b), e(1b)) = es(0b, 1b), \]
and thus \( s(0b, 1b) \in Z_p \).

Let us suppose that \( s(0b, 1b) = k \), and consider an automorphism \( \varphi(1) = -1, \varphi(0b) = 1b. \) Hence we get
\[ \varphi(1b) = \varphi(0b \cdot 1) = \varphi(0b) \cdot \varphi(1) = 1b \cdot (-1) = 0b \]
and, furthermore,
\[ k = s(0b, 1b) = s(1b, 0b) = s(\varphi(0b), \varphi(1b)) = \varphi(k). \]

One can see that the only \( k \in Z_p \) for which the equality \( \varphi(k) = k \) holds is equal to 0. Therefore \( s(0b, 1b) = 0. \)

Let us consider the mapping \( \alpha: S^{(2)}(Z_p Z_2) \to Z_p \times Z_p Z_2 \) defined by
\[ \alpha(s) = \langle s(1, 0), s(1, 0b) \rangle. \]
Since
\[ \alpha(s_1s_2) = \langle s_1s_2(1, 0), s_1s_2(1, 0b) \rangle \]
\[ = \langle s_1(1, 0), s_1(1, 0b) \rangle \langle s_2(1, 0), s_2(1, 0b) \rangle = \alpha(s_1)\alpha(s_2), \]
\( \alpha \) is a homomorphism. Moreover, since \( s(0b, 1b) = 0 \) for all \( s \in S^{(2)} \), therefore, if \( s_1 \neq s_2 \), then, by the lemma, either \( s_1(1, 0) \neq s_2(1, 0) \) or \( s_1(1, 0b) \neq s_2(1, 0b) \). This means that the mapping \( \alpha \) is one-to-one. Observe now that
\[ \alpha(w_p) = \langle 1, 0b \rangle \text{ and } \alpha(u) = \langle 2, 2 \rangle \]
are the generators of \( Z_p \times Z_p Z_2 \), and therefore

\[
gp \{ w_p, u \} = S^{(2)}(Z_p Z_2) \cong Z_p \times Z_p Z_2.
\]

This completes the proof.

**III. The class \( \mathcal{X} \).**

**Theorem 3.** The class \( \mathcal{X} \) is closed under taking subgroups, homomorphism images, and direct powers.

**Proof.** Observe that if \( s \) is a symmetric operation in \( G \), then \( s \) is symmetric in any group of the variety of groups, i.e. in the \( HSP(G) \) generated by \( G \). If \( G \in \mathcal{X} \), then the operation \( xy \) is generated by symmetric operations, and the equation expressing this fact is satisfied in any group of \( HSP(G) \).

**Theorem 4.** If a nilpotent group \( G \) belongs to \( \mathcal{X} \), then \( G \) is abelian.

**Proof.** In view of Theorem 3 it is sufficient to prove Theorem 4 for nilpotent group of class 2. To do this we show\(^{(1)}\) that if \( s \in S^{(n)}(G) \), then

\[
s(x_1^{-1}, \ldots, x_n^{-1}) = s(x_1, \ldots, x_n)^{-1}.
\]

By theorem 1,

\[
s(x_1, \ldots, x_n) = x_1^a \cdots x_n^a \prod_{1 \leq j < i \leq n} [x_i, x_j]^b, \quad \text{where } a^2 \equiv 2b(\exp G'),
\]

whence

\[
s^{-1}(x_1, \ldots, x_n) = \prod_{1 \leq j < i \leq n} [x_i, x_j]^{-b} \cdot x_n^{-a} \cdots x_1^{-a} \]

\[= x_1^{-a} \cdots x_n^{-a} \prod_{1 \leq j < i \leq n} [x_i^{-a}, x_j^{-a}] \prod_{1 \leq j < i \leq n} [x_i, x_j]^{-b}.
\]

Hence, by (16), we get (15).

If algebraic operations \( s_1, \ldots, s_k \) satisfy (15), then so does the operation \( s_1(s_2, \ldots, s_k) \). Hence, since \( G \in \mathcal{X} \), we have \( x^{-1}y^{-1} = (xy)^{-1} \), which implies that \( G \) is abelian.

Theorems 3 and 4 produce an abundance of groups which are not in \( \mathcal{X} \). For example, we have the following

**Corollary.** If a finite group \( G \) has a non-abelian Šylow subgroup, then \( G \) is not in \( \mathcal{X} \). Consequently, \( S_n \notin \mathcal{X} \) for \( n \geq 4 \).

**IV. A non-abelian group in \( \mathcal{X} \).** In this section we show that \( S_3 \in \mathcal{X} \).

**Theorem 5.** In \( Z_2 Z_2 \) we have

\[
xy = w_3[w_3u(w_3u(x, y), y^4), w_3(w_3^4(x, y), s(x, y, x))],
\]

\(^{(1)}\) The idea of this proof is due to S. Fajtlowicz.
where \( w_3(x, y) = xy[x, y], u(x, y) = x^2y^2, \) and \( s(x, y, z) = [x, y, x] \times [x, y, z] \) is a ternary symmetric operation in \( Z_2Z_2 \). Consequently, \( Z_2Z_2 \in \mathcal{X} \).

**Proof.** First we check that \( s \) is symmetric. In fact, by virtue of Jacobi identity valid in meta-abelian groups, we have

\[
\begin{align*}
    s(y, x, z) &= [x, y, z][y, x, z] = [x, y, z]^2[y, z, x]^2 = s(x, y, z), \\
    s(y, z, x) &= [x, y, z][y, z, x] = [y, z, x][y, x, z]^2 = s(x, y, z).
\end{align*}
\]

To prove (17) we apply lemma and verify that:

\[
\begin{align*}
    R(0, 1) &= w_3(w_3u(0, 1), w_3(1, 0)) = w_3(0, 1) = L(0, 1), \\
    R(1, 0) &= w_3(w_3u(0, 0), w_3(1, 0)) = w_3(0, 1) = L(1, 0), \\
    R(1, 0b) &= w_3(w_3u(2b, 0), w_3(0, 0)) = w_3(2b, 0) = 2b = L(1, 0b), \\
    R(0b, 1) &= w_3(w_3u(2b, 1), w_3(0, 1)) = w_3(1b, 1) = 1b = L(0b, 1), \\
    R(0b, 1b) &= w_3(w_3u(0, 0), w_3(0, 1)) = w_3(0, 1) = L(0b, 1b), \\
    R(1b, 0b) &= w_3(w_3u(0, 0), w_3(0, 2)) = w_3(0, 2) = L(1b, 0b).
\end{align*}
\]

This completes the proof.

It is of interest that in \( S_3 \) the operation \( xy \) is not generated by the set of binary symmetric operations. More precisely, we prove

**Theorem 6.** Every algebraic binary operation \( f \) from the algebra

\[
\mathfrak{A} = \langle Z_2Z_2; S^{(1)} \cup S^{(2)} \rangle
\]

satisfies

\[
(18) \quad f(ib, jb) \epsilon \{0, 0b, 1b, \ldots, (p-1)b\} = B, \quad 0 \leq i, j < p.
\]

Consequently, the operation \( xy \) does not belong to \( A^{(2)}(\mathfrak{A}) \).

**Proof.** Since every element of \( B \) is of order \( \leq 2 \), every unary operation maps \( B \) into \( B \). If \( f \epsilon S^{(2)}(Z_2Z_2) \), then, by Theorem 2, the operation \( f \) is of the form \( w_3^ku^l \) with \( 0 \leq k < 2p, 0 \leq l < p \). We have

\[
\begin{align*}
    w_3^k(ib, jb) &= ib \cdot jb \cdot [jb, ib]^{(p+1)/2} = (j-i)[(i-j)(i-j)]^{(p+1)/2} = 0, \\
    u^l(ib, jb) &= 0.
\end{align*}
\]

Suppose now that \( f_1 \) and \( f_2 \) satisfy (18) and consider the superpositions \( w_3(f_1, f_2) \) and \( u(f_1, f_2) \). We see that

\[
\begin{align*}
    w_3^k(f_1(ib, jb), f_2(ib, jb)) \epsilon B, \\
    u(f_1(ib, jb), f_2(ib, jb)) = 0,
\end{align*}
\]

whence

\[
\begin{align*}
    w_3^k u^l(f_1(ib, jb), f_2(ib, jb)) \epsilon B,
\end{align*}
\]

and (18) follows.
Since $ib \cdot jb = j - i$, the operation $xy$ cannot be an algebraic operation in $\mathbb{A}$.

I wish to express my gratitude to Andrzej Hulanicki for his help in preparation of this paper.

The results of this paper were announced in [3].

REFERENCES


INSTITUTE OF MATHEMATICS OF THE WROCŁAW UNIVERSITY

Reçu par la Rédaction le 23. 4. 1969