Jan Ambrosiewicz

ON THE DECOMPOSITION OF AN ELEMENT IN A GROUP INTO A PRODUCT OF ELEMENTS OF THE SAME ORDER

In this note we prove a theorem concerning decompositions of an element in a group into a product of n elements of the same order and provide some of its application in the same order and provide some of its application in the study of properties of the group $Z_p * Z_q$.

We will use the following notation.

A group G generated by elements $a_1, a_2, \dots$ and with relations $R_1, R_2, \dots$ is denoted by

$$G = \langle a_1, a_2, \dots; R_1, R_2, \dots \rangle.$$

By C_j we mean the class of conjugate elements of G , by x_j the representant of C_j and by K_m the set

$$\{g \in G: |g| = m\}, m \in \{|g|, g \in G\}.$$

Theorem 1. If G is a group, then the following condition are equivalent:

(i) an element $g \in G$ is a product of n elements from K_m ,

(ii) there are such elements $g_1, g_2, \dots, g_n \in G$ that $g = g_1 g_2 \dots g_n$ and there is a system of representants x_{i_j} of the classes C_{i_j} ($j=1, \dots, n$) from K_m such that

$$(1) \quad g_1 x_{i_1} g_2 \dots x_{i_{n-1}} g_n \in K_m.$$

The theorem results from the following two lemmas.

L e m m a 1. If G is a group, then the following conditions are equivalent:

- (i) the element $g \in G$ is a product of n elements from K_m ,
- (ii) there are elements $g_1, g_2, \dots, g_n \in G$ that $g = g_1 g_2 \dots g_n$ and there is a system of elements $k_1, k_2, \dots, k_{n-1} \in K_m$ such that $g_1 k_1 g_2 \dots k_{n-1} g_n \in K_m$.

P r o o f . Let $g = k_1 k_2 \dots k_n, k_i \in K_m$. If we put $g_i = k_i$ ($i = 1, 2, \dots, n$) then there is a system $k_1^{-1}, k_2^{-1}, \dots, k_{n-1}^{-1}$ that $g_1 k_1^{-1} g_2 \dots k_{n-1}^{-1} g_n = k_n \in K_m$.

Conversely, if there are elements $g_1, g_2, \dots, g_n \in G$ such that $g_1 g_2 \dots g_n = g$ and $g_1 k_1^{-1} g_2 \dots k_{n-1}^{-1} g_n = k_n \in K_m$ then by the normality of the set K_m we have

$$g_1 g_2 \dots g_n = (k_{n-1})^{g_n} (k_{n-2})^{g_{n-1} g_n} \dots (k_1)^{g_2 \dots g_n} g_1 g_2 \dots g_2.$$

Therefore the element g is a product of n elements of the set K_m .

L e m m a 2. If for each system $g_1, g_2, \dots, g_n \in G$ ($g_1 g_2 \dots g_n = g$) and for k_i from the set K_m the element

$$(2) \quad g_1 k_1^{-1} g_2 \dots k_{n-1}^{-1} g_n$$

does not belong to K_m , then the element

$$(3) \quad g_1 \left(k_1^{-1}\right)^{s_1} g_2 \dots \left(k_{n-1}^{-1}\right)^{s_{n-1}} g_n$$

with $\left(k_i^{-1}\right)^{s_i} = s_i^{-1} k_i^{-1} s_i$ does not belong to K_m for each $s_i \in G$, too.

P r o o f . Since the set K_m is normal, the following expressions are equivalent:

$$\begin{aligned}
 &g_1 k_1^{-1} g_2 \dots k_{n-1}^{-1} g_n \notin K_m, \\
 &k_1^{-1} g_2 k_2^{-1} \dots k_{n-1}^{-1} g_n g_1 \notin K_m, \\
 &g_2 k_2^{-1} g_3 \dots k_{n-1}^{-1} g_n g_1 \notin k_1 K_m, \\
 &k_2^{-1} g_3 \dots k_{n-1}^{-1} g_n g_1 g_2 \notin k_1 g_2 K_m, \\
 &\dots\dots\dots \\
 (4) \quad &g_1 g_2 \dots g_n \notin k_{n-1}^{-1} k_{n-2}^{-1} \dots k_1^{-1} g_n g_{n-1} g_n \dots g_2 g_3 \dots g_n K_m.
 \end{aligned}$$

By analogous transformations we see that (3) is equivalent to

$$(5) \quad (g_1 g_2 \dots g_n)^x \notin \left(k_{n-1}^{g_n}\right)^x \left(k_{n-2}^{g_{n-1} g_n}\right)^x \dots \left(k_1^{g_2 g_3 \dots g_n}\right)^x K_m$$

for each $x \in G$. Hence $g_1 g_2 \dots g_n \notin C_{n-1} C_{n-2} \dots C_1 K_m$ (C_j is the class of conjugate elements with a representative x_j) which implies (5) and also (3). This ends the proof of Lemma 2.

We say that a group G has the property W if $K_m K_m \leq G$ for each m (see [1]).

T h e o r e m 2. The group $G = \langle a, b; a^2, b^2 \rangle$ has the property W .

P r o o f . There are only the sets K_1, K_2, K_∞ of the type K_m in the group G . We have $K_2 = \{a^x, b^y; x, y \in G\}$. Let us consider the set K_2^4 . If $g \in K_2^4$ and $g \neq 1$, then

$$I) g = ab \dots ab \quad \text{or} \quad II) g = ba \dots ba,$$

where the number of factors is even and greater or equal to 4. Replacing in (1) the symbols x_{i_1}, g_1, g_2 by $x_{i_1} = b, g_1 = 1, g_2 = g$ in the case I) and by $x_{i_1} = a, g_1 = 1, g_2 = g$ in the case II), the formula (1) becomes either $bab...ab$ or $aba...ba$ depending on the case.

It is trivial that both elements have order 2. So by Theorem 1, we have $g \in K_2^2$. Hence $K_2^4 \subseteq K_2^2$ and obviously $K_2^2 \subseteq K_2^4$. Thus $K_2^4 = K_2^2$ and $K_2 K_2 \leq G$.

The set K_∞ has only elements of the form: $(ab)^n$ or $(ba)^n, n \geq 1$. Hence the element $g \neq 1$ of the set K_∞^4 has an even number of factors.

Putting in (1) $g_1 = 1, g_2 = g$ and either $x_{i_1} = ab$ if $g = ab...ab$ or $x_{i_1} = ba$ if $g = ba...ba$, we get elements of order ∞ . By Theorem 1, $g \in K_\infty^2$ i.e. $K_\infty^4 \subseteq K_\infty^2$.

The commutant G' of $G = \langle a, b; a^2, b^2 \rangle$ is a cyclic group and $G' = \langle (ab)^2 \rangle$ (see [2] p.248). From the construction of K_2^4 and K_∞^4 and from Theorem 2 we have the following result.

C o r o l l a r y 2.1. In the group $G = \langle a, b; a^2, b^2 \rangle$ we have $G' = K_2^2 = K_\infty^2$.

T h e o r e m 3. The group $G = \langle a, b; a^p, b^q \rangle$ does not have the property W, where p, q are prime numbers and $p \geq 2, q \geq 3$.

P r o o f. The element $g = ba^{-1}baba^{-1}ba$ belongs to K_q^4 . In our situation the elements of the form (1) can all be listed as follows

$$(bx_j)a^{-1}baba^{-1}ba,$$

$$ba^{-1}(bx_j)aba^{-1}ba,$$

$$ba^{-1}ba(bx_j)a^{-1}ba,$$

$$ba^{-1}baba^{-1}(bx_j)a.$$

By Theorem 1, $g \notin K_q K_q$ so $K_q^4 \not\subset K_q^2$ and $K_q K_q \neq G$.

Obviously $K_p K_p \neq G$ for $p > 2$.

Considering the element

$$g = (b^2 aba)(bab^2 a)^2 (b^2 aba)^2 (bab^2 a)^3$$

in the same way, we can prove also that $K_2 K_2 \neq G$.

Since the group $PSL(2, Z)$ and $\langle a, b; a^2, b^3 \rangle$ are isomorphic, we have the following result.

C o r o l l a r y 3.1. The group $PSL(2, Z)$ does not have the property W.

The problem of factoring a matrix $A \in PSL(2, Z)$ into the product of n elements of finite order leads to the problem of solving complicated Diophant's equation of $2(n-1)$ degree with $2(n-1)$ variables.

Since there is a simple algorithm, based on the use of transvections permitting to pass from the element $A \in PSL(2, Z)$ to a corresponding element $\bar{A}$ of $\langle a, b; a^2, b^3 \rangle$, then the Theorem 1 reduces the difficult problem of factoring a matrix into n factors of order m to very easy calculations.

Theorem 1 gives us also the possibility of deciding about solvability of certain Diophantine equations without solving them.

The method of factorizing of element from $PSL(2, Z)$ can be transferred to certain classes of groups $GL(n, K)$, where K is a ring or field, because we have

$$GL(n, K) = \text{gr} \left(t_{ij}(\alpha), d(\beta) : \alpha, \beta \in K, i \neq j \right) \quad (\text{see [3]}).$$

In several papers (for examples in [4]) the authors study the problem of covering a group by sets $C_m C_m$. If $C_m = C_m \cup C_m^{-1}$ then to this covering problem we can use Theorem 1 too.

REFERENCES

- [1] E. A m b r o s i e w i c z : On groups having the property W, Demonstratio Math. 10 (1977)
- [2] В. М а г н у с , А. К а р р а с , Д. С о л и - т э р : Комбинаторная теория групп, Москва, 1974.
- [3] М.И. К а р г а п о л о в , Ю.И. М е р з л я к о в : Основы теории групп, Москва, 1977.
- [4] J, L. B r e n n e r , M. R a n d a l l , I. R i d - d e l : Covering theorems for finite non-abelian simple groups. I. Colloq. Math. 32 (1974) Fasc.1.

INSTITUTE OF MATHEMATICS, UNIVERSITY OF WARSAW, BIAŁYSTOK BRANCH
Received February 13, 1979.