COLLOQUIUM MATHEMATICUM

VOL. XXX 1974 FASC. 2

ON GROUP OPERATIONS IN GROUPS OF EXPONENT k

BY

A. SOLECKI (WROCŁAW)

In this note we are concerned with group operations of a specific form in groups of Burnside varieties and we estimate their number by means of the exponent k of the group.

Consider the following property of a group G:

(*) In the group G there exists an operation (word)

$$x \circ y = x^{a_1} y^{b_1} \dots x^{a_r} y^{b_r},$$

where a_i, b_i are integers for $i = 1, 2, \dots, r$, different from the operations xy and yx (i. e. not identically equal to xy or yx) such that:

(i) the elements of G form a group G_0 under the operation $x \circ y$;

(ii) xy is an operation in G_0, i. e. there exist integers c_j and d_j for $j = 1, 2, \dots, s$ such that

$$xy = (x)_0^{c_1} \circ (y)_0^{d_1} \circ \dots \circ (x)_0^{c_s} \circ (y)_0^{d_s},$$

where $(x)_0^a$ denotes a^{th} power of x with respect to the multiplication $\circ$ in G_0.

The problem of existence of groups with property (*) was raised by Marczewski and Goetz in [1] and positively solved by Hulanicki and Świerczkowski in [2]. In [3] A. P. Street gave description of group operations in some classes of groups.

Professor C. Ryll-Nardzewski has observed that in the variety of groups of finite exponent k any word $x \circ y = (x^m y^m)^n$, where $mn = k+1$, is a group operation. The associativity of this operation as well as the identity $xy = (x^n \circ y^n)^m$ follow immediately from the identity $z^{mn} = z$ (we may write z^a instead of $(z)_0^a$ because these operations are identical; cf. [1]). It has been left to check whether this operation differs from xy and yx.

PROPOSITION 1. *Let G be a non-abelian group of finite exponent k and let $mn = k+1$. If the conditions $(m-1, n-1) = 1$ and $(m+1, n+1) = 1$ are satisfied, then $x \circ y = (x^m y^m)^n$ is the group operation different from xy and yx.*

(The symbol (a, b) denotes the g.c.d. of the integers a and b.)

Proof (indirect). Let $x \circ y = xy$ for all $x, y \in G$. Then $x^{-1} \circ y \circ x = x^{-1}yx$. But $x^{-1} \circ y \circ x = (x^{-m}y^m x^m)^n = x^{-m}yx^m$. Hence $x^{m-1}y = yx^{m-1}$ and thus $x^{m-1} \in Z(G)$ (centre of G) for every $x \in G$.

The condition $(m-1, n-1) = 1$ is equivalent to $(m-1, k) = 1$ because $k = mn-1 = (m-1)n+(n-1)$ and, therefore, $x^{m-1} \in Z(G)$ implies $x \in Z(G)$, contradictory to the assumption that G is non-abelian.

Next, suppose that $x \circ y = yx$ for all $x, y \in G$. Similarly, we obtain $x^{-1} \circ y \circ x = xyx^{-1}$ and $x^{-1} \circ y \circ x = x^{-m}yx^m$. Hence we have $yx^{m+1} = x^{m+1}y$ and thus $x^{m+1} \in Z(G)$ for every $x \in G$. And again, the condition $(m+1, n+1) = 1$ is equivalent to $(m+1, k) = 1$ because $k = mn+1 = (m+1)n - (n+1)$ and, therefore, $x^{m+1} \in Z(G)$ implies $x \in Z(G)$, which is a contradiction.

These conditions are not necessary, as the case of the group S_{11} (permutations of 11-element set) examplifies: $k = \exp S_{11} = 27720$ (the product $5 \cdot 7 \cdot 8 \cdot 9 \cdot 11$); this number can be written in the form $k = 19 \cdot 1459 - 1$. It is easy to check (e. g. by taking two non-commuting cycles of length 7) that the operation $(x^{19}y^{19})^{1459}$ is different from xy and yx although not both conditions of Proposition 1 are satisfied.

Let us look for conditions implying existence of a group operation of the form $(x^m y^m)^n$ different from xy and yx in a group G of exponent k and estimate the number of such operations. First, observe that we use the congruence $mn \equiv 1 \pmod{k}$ rather than the equality $mn = k+1$. Using this we find a group operation of the given form in the smallest non-abelian simple group, namely A_5 (even permutations of 5-element set). Here $k = \exp A_5 = 30$ and $7 \cdot 13 = 3k+1$, and so the operation $(x^7y^7)^{13}$ is the group one in A_5. It is easy to check (e. g., by taking two non-commuting cycles of length 5) that it is different from xy and yx. Let us remark that in [2] and [3] the group operations were described for varieties of nilpotent and soluble groups.

Proposition 2. *Let G be a group of finite exponent k. If there exists an element a of order p^i, where p is a prime greater than 3, which does not belong to the centre of G, then there exists a group operation $\circ$ in G of the form $(x^m y^m)^n$ different from xy and yx.*

Proof. Take m prime satisfying $m \not\equiv 1 \pmod{p}$ and $m \not\equiv p-1 \pmod{p}$. Moreover, to guarantee $(m, k) = 1$ assume $m > k$. The existence of m follows from the Dirichlet theorem: if $(s, t) = 1$, then the arithmetical progression $\{s+rt\}_{r=1}^{\infty}$ contains infinite number of primes. Put $t = p$ and, say, $s = 2$. There exists n such that $mn \equiv 1 \pmod{k}$ because — in virtue of $(m, k) = 1$ — there exists a solution of the equation $nm+lk = 1$. Then $x \circ y = (x^m y^m)^n$ is the operation we need. Take $b \in G$ such that $ab \neq ba$. If $x \circ y$ were identically equal to xy or yx, then (cf. the proof of Proposition 1) $a^{m-1}b = ba^{m-1}$ or $a^{m+1}b = ba^{m+1}$, respectively. But $(m-1, p^i) = 1$

and $(m+1, p^i) = 1$ and in both cases we would obtain $ab = ba$, a contradiction.

PROPOSITION 3. *Let G be a group of finite exponent k. If there exist elements $a_1, \ldots, a_s$ G of orders $p_1^{\alpha_1}, \ldots, p_s^{\alpha_s}$, respectively, where $p_1, \ldots, p_s$ are different primes greater than 2, which do not belong to the centre of G, then the number of group operations of the form $(x^m y^m)^n$ in G such that any of them is different from the others and from the ones obtained from the others by the transposition of variables x and y is not smaller than*

$$\frac{1}{2}\prod_{i=1}^{s}(p_i-1).$$

Moreover, if $k = q_1^{\beta_1} \ldots q_t^{\beta_t}$ $(k \neq 2)$ is the decomposition of k into the product of primes, then the number of such operations is not greater than

$$\frac{1}{2}\prod_{i=1}^{t}(q_i^{\beta_i} - q_i^{\beta_i - 1}).$$

Proof. Let $m \equiv r_i \pmod{p_i}$, $i = 1, \ldots, s$, be a system of congruences with non-vanishing residues. Take arithmetical progressions $\{r_i + rp_i\}_{r=1}^{\infty}$. They overlap because their differences p_i's are relatively prime and so their intersection is also an arithmetical progression $\{u_i\}_{i=1}^{\infty}$ with the difference $p_1 \ldots p_s$. This difference is relatively prime with the first element u_1 as it is — being an element of the progression $\{r_i + rp_i\}_{r=1}^{\infty}$ — relatively prime with p_i for each $i = 1, \ldots, s$. Using again Dirichlet's theorem we find m prime satisfying the system of congruences (in order to guarantee $(m, k) = 1$ assume $m > k$). Next, take n such that $nm \equiv 1 \pmod{k}$. Thus, for the given residues $r_1, \ldots, r_s$ we find a group operation $(x^m y^m)^n$.

Take two operations $(x^m y^m)^n$ and $(x^{m'} y^{m'})^{n'}$ corresponding to the sequences of residues $r_1, \ldots, r_s$ and $r_1', \ldots, r_s'$, respectively. If they were identical, then $(x^{-m} y^m x^m)^n = (x^{-m'} y^{m'} x^{m'})^{n'}$ and hence $x^{m'-m} y = y x^{m'-m}$.

Suppose $r_l \neq r_l'$. Then $m' - m \not\equiv 0 \pmod{pl}$. Take $b \in G$ such that $a_l b \neq b a_l$. By $(m' - m, p_l^{\alpha_l}) = 1$, the equality $a_l^{m'-m} b = b a_l^{m'-m}$ would imply $a_l b = b a_l$, contrary to our assumption.

On the other hand, suppose that $(x^m y^m)^n = (y^{m'} x^{m'})^{n'}$ for all $x, y \in G$. Then $(x^{-m} y^m x^m)^n = (x^{m'} y^{m'} x^{-m'})^{n'}$ and $y x^{mm'} = x^{mm'} y$.

Argument similar to the previous one shows that $r_i + r_i' = p_i$ for $i = 1, \ldots, s$. Thus, only if the above equalities hold, two different sequences of residues may lead to operations differing by transposition of variables. Hence we obtain

$$\frac{1}{2}\prod_{i=1}^{s}(p_i - 1)$$

as the lower bound of the number of essentially different group operations in G.

The upper bound of this number follows immediately from the remark that the condition $(m, k) = 1$, which is necessary for the existence of n such that $nm \equiv 1 \pmod{k}$, is equivalent to the conjunction of conditions $(m, q_j) = 1, j = 1, \ldots, t$. The number of m's satisfying the j^{th} condition and giving different residues mod $q_j^{\beta_j}$ is equal to $q_j^{\beta_j} - q_j^{\beta_j - 1}$. (Evidently, for a given m, if $nm \equiv 1 \pmod{k}$, then the residue of n mod k is uniquely determined.) We divide the product of these numbers by 2 because if $m + m' \equiv q_j^{\beta_j} \pmod{k}$ for $j = 1, \ldots, t$, then the respective group operations $(x^m y^m)^n$ and $(x^{m'} y^{m'})^{n'}$ differ by the transposition of variables x and y.

PROPOSITION 4. *Groups G with the operation xy and G_0 with the operation $x \circ y = (x^m y^m)^n$ are isomorphic. The isomorphism $h\colon G \to G_0$ is given by $h(x) = x^n$.*

Proof. We have

$$h(xy) = (xy)^n = (x^{nm} y^{nm})^n = x^n \circ y^n = h(x) \circ h(y).$$

Thus, in a group of exponent k raising to the n^{th} power is an automorphism if and only if for $mn \equiv 1 \pmod{k}$ the operations $(x^m y^m)^n$ and xy are identically equal.

REFERENCES

[1] A. Goetz, *On weak isomorphisms and weak homomorphisms of abstract algebras*, Colloquium Mathematicum 14 (1966), p. 163-167.

[2] A. Hulanicki and S. Świerczkowski, *On group operations other than xy and yx*, Publicationes Mathematicae Debrecen 9 (1962), p. 142-148.

[3] A. P. Street, *Subgroup-determining functions on groups*, Illinois Journal of Mathematics 12 (1968), p. 99-120.

TECHNICAL UNIVERSITY, WROCŁAW

Reçu par la Rédaction le 1. 11. 1972