Časopis pro pěstování matematiky, roč. 101 (1976), Praha

ON THE NUMBER OF NORMAL SUBGROUPS OF A GIVEN PRIME INDEX

JIŘÍ PAROBEK, Praha

(Received December 10, 1974)

Our aim in this short note is to give an optimum upper bound to the number of normal subgroups of index p, p a prime, in groups of order n. Our result is divided into two theorems: Theorem 1 gives the estimate, Theorem 2 states its optimality.

Remark on notation and terminology. By $|X|$ we mean the cardinality of a set X (or its order if it is a group). If A, B are two complexes in a group G, then AB means, as usual, the complex in G consisting of all ab where $a \in A$, $b \in B$. The sign $\otimes$ denotes the direct product of groups. A normal subgroup of index p (in a group G) will also be briefly called an Np-subgroup (of G). The word "group" means "finite group" throughout the paper.

Lemma. *Let N_1, N_2 be two distinct Np-subgroups of a group G. Then $N_1 \cap N_2$ is an Np-subgroup of N_1.*

Proof. The second (or the first as it is sometimes called) theorem on isomorphism states, if applied to our subgroups N_1, N_2, that $N_1/N_1 \cap N_2$ is isomorphic to N_1N_2/N_2. As both N_1, N_2 are of a prime index, we have $N_1N_2 = G$, and the proof follows immediately.

Theorem 1. *For the number $s_p(G)$ of normal subgroups of index p, p a prime, in a group G of order n, the following inequality holds:*

$$s_p(G) \leqq \frac{p^r - 1}{p - 1}, \tag{1}$$

where r is the greatest integer such that $p^r \mid n$.

Proof. For an arbitrary group X, let $r_p(X)$ denote the greatest integer such that $p^{r_p(X)} \mid |X|$. We shall prove (1) by induction with respect to $r_p(G)$. The case $r_p(G) = 0$ is obvious, the case $r_p(G) = 1$ follows immediately from the lemma since if N_1, N_2

are two distinct Np-subgroups of G, then $|G| = p|N_1| = p^2|N_1 \cap N_2|$ so that $r_p(G) \geqq 2$. Hence, let r be an integer, $r \geqq 2$, and suppose that (1) holds for all groups X for which $r_p(X) \leqq r - 1$. Let G be a group of order n with $r_p(G) = r$. Suppose that G has exactly q Np-subgroups $N_1, N_2, \ldots, N_q$. We clearly may assume $q \geqq 2$. Let us now take the set $\mathscr{B} = \{N_2, N_3, \ldots, N_q\}$ and partition it into β disjoint nonempty subsets $\mathscr{A}_i$ such that N_j and N_k $(2 \leqq j, k \leqq q)$ belong to the same class if and only if $N_1 \cap N_j = N_1 \cap N_k$. Thus, among the groups $N_1 \cap N_2, N_1 \cap N_3, \ldots$ $\ldots, N_1 \cap N_q$, there are exactly β distinct ones. Since all these groups are Np-subgroups of N_1 (as follows from the lemma) and since $r_p(N_1) = r - 1$, we have by hypothesis

$$\beta \leqq \frac{p^{r-1} - 1}{p - 1}. \tag{2}$$

Further, we shall prove

$$\alpha_i \leqq p \quad \text{for} \quad i = 1, \ldots, \beta \tag{3}$$

where $\alpha_i = |\mathscr{A}_i|$. Without any loss of generality, let $\mathscr{A}_i$ (i arbitrary) consist of the first α_i elements of $\mathscr{B}$. Thus, let $N_1 \cap N_2 = N_1 \cap N_3 = \ldots = N_1 \cap N_{\alpha_i+1} = Q$. By an easy argument we find that

$$N_j \cap N_k = Q \quad \text{for any} \quad 1 \leqq j \leqq \alpha_i + 1 \quad \text{and} \quad 2 \leqq k \leqq \alpha_i + 1\,. \tag{4}$$

Indeed, we have $N_j \cap N_k \supset (N_1 \cap N_j) \cap (N_1 \cap N_k) = Q$ and $|N_j \cap N_k| = |Q|$ by the lemma. According to (4), the sets $Q, N_1 - Q, \ldots, N_{\alpha_i+1} - Q$ must be disjoint. Hence, in view of the relations $|Q| = n/p^2$, $|N_l - Q| = n/p - n/p^2$ $(1 \leqq l \leqq$ $\leqq \alpha_i + 1)$ following from the lemma, we get the condition

$$\left(\frac{n}{p} - \frac{n}{p^2}\right)(\alpha_i + 1) + \frac{n}{p^2} \leqq n$$

implying (3). By (3) and (2), we have

$$q - 1 = \sum_{i=1}^{\beta} \alpha_i \leqq \beta p \leqq p\,\frac{p^{r-1} - 1}{p - 1}$$

whence

$$q \leqq \frac{p^r - 1}{p - 1}.$$

This completes our proof.

Theorem 2. *The estimate* (1) *of Theorem* 1 *is best possible since for any pair p, n, p a prime, of positive integers, at least one group G of order n exists for which the equality sign takes place in* (1).

Our proof is based on a certain well-known assertion of the theory of abelian groups, see e.g. [1], p. 53, Satz 51.

Proof of Theorem 2. For given n, p, let r, m be those integers for which $n = p^r m$, $p \nmid m$. Let H be an arbitrary group of order m and let A denote the (elementary) abelian group of order p^r and of type $(p, \ldots, p)$. Put $G = A \otimes H$. (For $m = 1$ or $r = 0$, this reduces to $G = A$ and $G = H$, respectively.) To prove Theorem 2, it evidently suffices to show that A possesses $(p^r - 1)/(p - 1)$ distinct subgroups of index p (that is just a special case of the assertion mentioned above; we shall, however, give its proof for the sake of completeness). Indeed, if B_1, B_2 are two distinct subgroups of index p in A, then $B_1 \otimes H$, $B_2 \otimes H$ are two distinct Np-subgroups of G. — To determine the number of Np-subgroups in A (we retain our short notation though the normality is trivial in this case), let us first note that each Np-subgroup of A is of type $(p, \ldots, p)$ since its invariants must be divisors of those of A. The basis of each Np-subgroup therefore consists of $r - 1$ elements. Any independent $(r - 1)$-tuple of elements of A may evidently be chosen in the following manner: In the first step, we choose an arbitrary element $a_1 \in A$, $a_1 \neq 1$; the elements $a_1, \ldots, a_{i-1}$ being already chosen, in the i-th step $(2 \leqq i \leqq r - 1)$ we choose an arbitrary element $a_i \in A$ not belonging to the group generated by the elements $a_1, \ldots, a_{i-1}$. In this way, just $n_1 = (p^r - 1)(p^r - p)\ldots(p^r - p^{r-2})$ distinct independent $(r - 1)$-tuples may be chosen. Analogously, we find that for each Np-subgroup of A, exactly $n_2 = (p^{r-1} - 1)(p^{r-1} - p)\ldots(p^{r-1} - p^{r-2})$ distinct independent $(r - 1)$-tuples may be chosen out of its elements. Thus, among the total of n_1 distinct independent $(r - 1)$-tuples made up of the elements of A, every n_2 of them generate the same Np-subgroup. The number of distinct Np-subgroups in A is therefore given by $n_1/n_2 = (p^r - 1)/(p - 1)$. The same number of (distinct) Np-subgroups will, as remarked above, exist in the group $G = A \otimes H$. The proof is hereby completed.

In the end of our note, let us mention two special cases of Theorem 1 which perhaps are of certain importance since they are concerned with the class of all, not explicitly normal, subgroups.

Corollary 1. *For the number $s_p(G)$ of subgroups of a given prime index, p, in an abelian group G of order n, the estimate (1) of Theorem 1 holds and is best possible.*

Corollary 2. *For the number $s_2(G)$ of subgroups of index 2 in a group G of order n, the inequality*

$$s_2(G) \leqq 2^r - 1$$

holds where r is the greatest integer such that $2^r \mid n$. This estimate is best possible.

Proof of Corollary 1 is obvious (the optimality is secured by Theorem 2 — just taking H abelian), proof of Corollary 2 follows from the well-known fact that in