ON FINITE NILPOTENT GROUPS

G. BACHMAN

1. Introduction and notations. It is well known that if $(n, \phi(n)) = 1$, where $\phi(n)$ denotes the Euler ϕ-function, then the only group of order n is the cyclic group. This is a special case of a more general result due to Dickson (**2**, p. 201); namely, if

$$n = p_1^{\alpha_1} \ldots p_s^{\alpha_s}$$

where the p_i are distinct primes and each $\alpha_i > 0$, the necessary and sufficient conditions that the only groups of order n are abelian are (1) each $\alpha_i \leqslant 2$ and (2) no

$$p_i^{\alpha_i} - 1$$

is divisible by any $p_1, \ldots, p_s$.

We wish to establish a theorem which includes these two results. We let $G(n)$ equal the number of groups of order n where

$$n = \prod_{i=1}^{s} p_i^{\alpha_i},$$

and we seek necessary and sufficient conditions on n so that

$$G(n) = \prod_{i=1}^{s} G(p_i^{\alpha_i}).$$

Clearly, this problem is equivalent to finding necessary and sufficient conditions on n so that all existing groups of order n be nilpotent.

It will be shown that the following is true:

THEOREM 1. *Let*

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_s^{\alpha_s},$$

where $p_1, \ldots, p_s$ are distinct primes and each $\alpha_i > 0$. The necessary and sufficient conditions that the only groups of order n be nilpotent are: no p_i, $i = 1, \ldots, s$, shall divide any

$$p_j^{\alpha_j} - 1, p_j^{\alpha_j - 1} - 1, \ldots, p_j - 1, j = 1, \ldots, s.$$

We introduce the following notations: the centre of a group A by $Z(A)$, the group of all automorphisms of A by $\Phi(A)$, the group of all inner automorphisms of A by $\Phi'(A)$, the factor group $\Phi(A)|\Phi'(A)$ by $\mathfrak{A}(A)$, the direct

Received November 17, 1958. The author wishes to express his appreciation to Professor H. N. Shapiro for suggesting this problem to him.

https://doi.org/10.4153/CJM-1960-007-x Published online by Cambridge University Press

product of the two groups A and B by $A \times B$, and the direct product of the n groups $A_1, \ldots, A_n$ by

$$\mathop{\times}_{i=1}^{n} A_i,$$

the order of the finite group A by $|A|$, and a Sylow p-group of a group G by S_p.

Let B be a group such that each element $\alpha \in B$ is associated with an automorphism $a \to a^\alpha$ of A. Let G be an extension of A by B, that is, A is a normal subgroup of G and $G|A \simeq B$. Then the elements of G can be written as $g_\alpha a$ where the g_α are in one-to-one correspondence with the $\alpha \in B$, and $a \in A$; also

$$g_\alpha a \,.\, g_\beta b = g_{\alpha\beta} f(\alpha, \beta) a^\beta b$$

where $f(\alpha, \beta)$ is a factor system. Moreover,

$$g_\alpha^{-1}\, a\, g_\alpha = a^\alpha,$$

and

$$(a^\alpha)^\beta = (a^{\alpha\beta})^{f(\alpha,\beta)}.$$

Finally, to the extension G there corresponds a well-defined homomorphism θ of B into $\mathfrak{A}(A)$ (**3**, pp. 121–126). If N is a normal subgroup of G whose order is prime to its index, then G splits over N (Schur's theorem) (**4**, p. 132).

In general, if A is abelian, then $\mathfrak{A}(A) = \Phi(A)$ and B is a group of operators for A, that is, A is a B-module. It is well known that the second cohomology group $H^2(B, A)$ is the group of all group extensions of A by B. If A and B are finite and $(|B|, |A|) = 1$, then $H^r(B, A) = 0$ for all r (**1**, p. 237), in particular, $H^2(B, A) = 0$, so the only extensions of A by B are splitting extensions, that is, we can take $f(\alpha, \beta) = 1$, and, therefore, G contains a subgroup $B' \simeq B$ such that $A \cap B' = e$, the identity element, and $G = AB'$.

The consideration of non-abelian groups A is reduced to the abelian case by the following theorem: There exists a one-to-one correspondence between all non-equivalent extensions of A by B associated with θ and all non-equivalent extensions of $Z(A)$ by the group of operators B corresponding to the homomorphism θ (**3**, pp. 142-145).

In the case of an abelian group A, the non-equivalent splitting extensions of A by B are in one-to-one correspondence with the distinct homomorphisms of B into $\Phi(A)$ (**3**, p. 149). The kernel of the homomorphism will be denoted by W. If $W = B$, then we say that B acts trivially on A.

2. Proof of Theorem 1. (1) *Sufficiency*: To proceed by induction, we assume that the statement is true for every

$$n' = p_1^{\beta_1} \ldots p_s^{\beta_s},\ \beta_i \leqslant \alpha_i,\ n' < n.$$

Now since

$$(|G|, (p_i^{\alpha_i} - 1)(p_i^{\alpha_i - 1} - 1) \ldots (p_i - 1)) = 1,$$

https://doi.org/10.4153/CJM-1960-007-x Published online by Cambridge University Press

we have, by Frobenius' Theorem (**4**, p. 143), that the maximal p_i-factor group of G is isomorphic to every Sylow p_i-group of G, that is, G contains a normal subgroup N such that $G/N \simeq S_{p_i}$, and G is a splitting extension of N. But there exists a one-to-one correspondence between all non-equivalent extensions of N by S_{p_i} associated with θ and all non-equivalent extensions of $Z(N)$ by the group of operators S_{p_i} corresponding to the homomorphism θ. Thus we must consider splitting extensions, H, of the S_{p_i}-module $Z(N)$. By the induction hypothesis,

$$N = \mathop{\times}_{\substack{j=1\\ j\neq i}}^{s} S_{p_j}, \qquad \text{so} \qquad Z(N) = \mathop{\times}_{\substack{j=1\\ j\neq i}}^{s} Z(S_{p_j}).$$

$Z(S_{p_j})$ is an abelian group of order $p_j^{\gamma_j}$, $1 \leqslant \gamma_j \leqslant \alpha_j$, from which it follows (**4**, p. 112) that $|\Phi(Z(N))|$ is a divisor of

$$\prod_{\substack{j=1\\ j\neq i}}^{s} (p_j^{\gamma_j} - 1)(p_j^{\gamma_j} - p_j) \ldots (p_j^{\gamma_j} - p_j^{\gamma_j - 1});$$

whence it is clear that we can only take $W = S_{p_i}$, which means trivial action, that is, the only extension of $Z(N)$ by S_{p_i} is $S_{p_i} \times Z(N)$. Therefore, by the one-to-one correspondence there is only one extension of N by S_{p_i} associated with a given homomorphism θ. Thus, the non-equivalent extensions of N by S_{p_i} are in one-to-one correspondence with those homomorphisms of S_{p_i} into $\mathfrak{A}(N)$ which are associated with extensions of N by S_{p_i}. But

$$\Phi(N) = \mathop{\times}_{\substack{j=1\\ j\neq i}}^{s} \Phi(S_{p_j}) \qquad \text{and} \qquad |\Phi(N)|$$

is a divisor of

$$\prod_{\substack{j=1\\ j\neq i}}^{s} (p_j^{\alpha_j} - 1)(p_j^{\alpha_j} - p_j) \ldots (p_j^{\alpha_j} - p_j^{\alpha_j - 1}).$$

Hence $|\mathfrak{A}(N)|$ is also a divisor of this number. Therefore, it is clear that the only possible homomorphism is the trivial one which implies that the only extension of N by S_{p_i} is $S_{p_i} \times N$. But

$$N = \mathop{\times}_{\substack{j=1\\ j\neq i}}^{s} S_{p_j};$$

hence

$$G = \mathop{\times}_{j=1}^{s} S_{p_j},$$

and G is nilpotent.

(2) *Necessity*: Suppose some

$$p_i/(p_j^{\alpha_j} - 1) \ldots (p_j - 1).$$

Then we consider the following arrangement. Let

$$A(\alpha_j, p_j) = C_{p_j} \times C_{p_j} \times \ldots \times C_{p_j} \qquad (\alpha_j \text{ times})$$

where C_{p_j} is the cyclic group of order p_j. We denote by $G(\alpha_i, p_i)$ a group of order $p_i^{\alpha_i}$. Now, clearly,

$$\Phi\left(\mathop{\times}_{\substack{j=1\\ j\neq i}}^{s} A(\alpha_j, p_j)\right) = \mathop{\times}_{\substack{j=1\\ j\neq i}}^{s} \Phi(A(\alpha_j, p_j)).$$

Since, by assumption,

$$\mathop{\times}_{\substack{j=1\\ j\neq i}}^{s} \Phi(A(\alpha_j, p_j))$$

contains a subgroup of order p_i, there exists a homomorphism:

$$G(\alpha_i, p_i) \to \Phi\left(\mathop{\times}_{\substack{j=1\\ j\neq i}}^{s} A(\alpha_j, p_j)\right)$$

with kernel a normal subgroup W of order $p_i^{\alpha_i - 1}$. Associated with this homomorphism, there is a splitting extension G of

$$\mathop{\times}_{\substack{j=1\\ j\neq i}}^{s} A(\alpha_j, p_j) \qquad \text{by } G(\alpha_i, p_i)$$

for which W is the normal subgroup of $G(\alpha_i, p_i)$ which acts trivially on

$$\mathop{\times}_{\substack{j=1\\ j\neq i}}^{s} A(\alpha_j, p_j).$$

G is, of course, a group of order

$$n = \prod_{i=1}^{s} p_i^{\alpha_i},$$

but the extension G is not equivalent to

$$G(\alpha_i, p_i) \times \left(\mathop{\times}_{\substack{j=1\\ j\neq i}}^{s} A(\alpha_j, p_j)\right).$$

In fact, G is not isomorphic to this group for $S_{p_i} = G(\alpha_i, p_i)$ is not normal in G. Namely, if $a^{-1}g_\alpha a = g_\beta$ then $g_\alpha^{-1}a^{-1}g_\alpha a = g_\alpha^{-1}g_\beta$, that is, $(a^{-1})^\alpha a = g_\alpha^{-1}g_\beta$, but the left side belongs to

$$\mathop{\times}_{\substack{j=1\\ j\neq i}}^{s} A(\alpha_j, p_j)$$

while the right side belongs to S_{p_i}. However,

$$S_{p_i} \cap \left(\mathop{\times}_{\substack{j=1\\ j\neq i}}^{s} A(\alpha_j, p_j)\right) = e,$$

so $g_\beta = g_\alpha$. Now if S_{p_i} were normal in G, then we would have $a^{-1}g_\alpha a = g_\alpha$ for all $g_\alpha \in S_{p_i}$ and all

$$a \in \mathop{\times}_{\substack{j=1\\ j\neq i}}^{s} A(\alpha_j, p_j),$$

that is $(a^{-1})^\alpha = a^{-1}$ for all α and all a, which implies that S_{p_i} acts trivially on

$$\bigtimes_{\substack{j=1\\ j\neq i}}^{s} A(\alpha_j, p_j), \quad \text{or} \quad W = S_{p_i},$$

which is a contradiction.

Therefore, S_{p_i} is not normal in G; hence G, of order n, is not nilpotent.

COROLLARY 1. *Let $G(n)$ be the number of groups of order n. If*

$$n = \prod_{i=1}^{s} p_i^{\alpha_i},$$

then the necessary and sufficient conditions in order that

$$G(n) = \prod_{i=1}^{s} G(p_i^{\alpha_i})$$

are that no p_i, $i = 1, 2, \ldots, s$, divides any

$$(p_j^{\alpha_j} - 1)(p_j^{\alpha_j - 1} - 1) \ldots (p_j - 1).$$

Proof. There are $G(p_i^{\alpha_i})$ groups of order $p_i^{\alpha_i}$. By taking all possible direct products it is clear that

$$G(n) \geqslant \prod_{i=1}^{s} G(p_i^{\alpha_i}),$$

and we have equality, if and only if the only groups of order n are direct products of their Sylow subgroups.

It is clear that to have only abelian groups of order n, we must have $\alpha_j \leqslant 2$ for all j; hence we get Dickson's theorem as a special case of Theorem 1.

REFERENCES

1. H. Cartan and S. Eilenberg, *Homological algebra* (Princeton, 1956).
2. L. E. Dickson, Trans. Amer. Math. Soc. *6* (1905), 201.
3. A. G. Kurosh, *The theory of groups*, vol. II (New York, 1956).
4. H. Zassenhaus, *The theory of groups* (New York, 1949).

Rutgers University