REVUE DE MATHÉMATIQUES
PURES ET APPLIQUÉES
Tome I, 1956, N° 2

A CHARACTERIZATION OF THE CYCLIC GROUPS

BY

F. SZÁSZ
(Debrecen—Hungary)

§ 1. Introduction

In this paper we shall discuss the following problem from the *group theory*. Let k be a fixed natural number not necessarily different from zero, and let G be an arbitrary not necessarily abelian group written *multiplicatively*. *The k-th power of the group G* is a subgroup denoted by G^k generated by the set of k-th powers of all group elements. We shall call an arbitrary group G a *group with property P* if for every cyclic subgroup H of G there exists a natural number k for which $H = G^k$ holds. E.g. every cyclic group has the property P. The aim of this paper is to give an *elementary* proof of the converse statement, namely we are going to prove that a group with property P is necessarily cyclic, i.e. property P is characteristic of cyclic groups. We can make a brief survey of all torsion-free groups with property P but it is not too simple to prove that a torsion group with property P cannot be a group without centre. The non-trivial abelian and cyclic behaviour of all groups with property P will be found out almost simultaneously at the end of this paper.

§ 2. Preliminaries

The characterization of cyclic groups will be easier to survey, if we first prove seven Lemmas. First of all, let us make some *terminological* remarks.

We shall not assume the commutativity of the groups considered, and therefore we use multiplicative notation throughout. We denote the *order* of the element g by the symbol $O(g)$. A group is called *torsion-free*, if it contains no element of finite order other than the unity. On the other hand, groups every element of which is of finite order are called *torsion groups*. A group is termed a *p-group*, if the orders of all its elements are powers of a fixed prime number p. If a torsion group G contains an element of maximal order m, we say that G is an *m-bounded group*. As it is well known, abelian groups of bounded order are direct products of cyclic groups. [2], [3].

A group is called *metabelian*, if its centre contains its derived group i.e. the subgroup generated by the set of commutators $[a, b] = a^{-1} b^{-1} a\, b$ of all group elements a and b. In metabelian groups the relation

$$[a, b] \cdot [a, c] = [a, b.c]$$

holds for arbitrary elements a, b, c, moreover

$$(a\, b)^n = a^n \cdot b^n \cdot [b, a]^{\binom{n}{2}},$$

where $\binom{n}{2} = \frac{n(n-1)}{2}$ ([2], [4]). The elements of the group G which commute with a given subset S of G form a subgroup N_S called the *normalizer* of S in G, and the elements which commute with all elements of the given subset S form a subgroup Z_S called the *centralizer* of S in G. Obviously the normalizer of every normal subgroup in G and the centralizer of every subgroup of the centre in G is the group G itself.

We shall now prove seven Lemmas:

LEMMA 1. *If G is an arbitrary p-group and A subgroup of order p of G, then the centralizer Z_A of A in G coincides with the normalizer N_A of A in G**)

Proof. It is clear that $Z_A \subseteq N_A$. Let now g be an arbitrary element of N_A and a an element of A. By n we denote a natural number, for which $g^{-1} a\, g = a^n$ holds. If $O(g) = p^t$ then we successively obtain the equations:

$$a = g^{-p^t} \cdot a \cdot g^{p^t} = g^{-p^t+1} \cdot a^n \cdot g^{p^t-1} = \ldots = a^{n^{p^t}}$$

since, by $O(a) = p$ we have $n^{p^t} \equiv 1 \pmod{p}$. Repeated application of *Fermat*'s theorem from the number theory yields $n \equiv 1 \pmod{p}$ and $a^n = a$. Therefore $g^{-1} ag = a$ namely g is contained in Z_A.

LEMMA 2. *Every homomorphic image of a group with property P is a group with property P.*

Proof. Let G be an arbitrary group with property P and φ a homomorphic mapping of G onto the group G'. If H' is the cyclic subgroup generated by the arbitrary element h' of G', then there exists an element h of G for which $h\varphi = h'$ holds. Let $\{h\} = H = G^k$ and thus $h = g_1^k \ldots g_s^k$ with certain elements $g_1, \ldots, g_s$ of G. Obviously $(h')^n = (h^n)\,\varphi$ and thus $H\varphi = (G^k)\,\varphi = H'$. Then $h' = (g_1\varphi)^k \ldots (g_s\varphi)^k$ since $(G^k)\,\varphi \subseteq (G')^k$. On the other hand, if $g \in G$, then $(g^k)\,\varphi = (g\varphi)^k \in H'$, therefore we can write $(G')^k \subseteq H\varphi = (G^k)\,\varphi$ and thus $H' = (G')^k$.

LEMMA 3. *Every cyclic subgroup of a group with property P is normal***).

Proof. Let ε be an arbitrary endomorphism of the group G with property P and H a cyclic subgroup of G. Then, by the proof of Lemma 2, $(G^n)\varepsilon = (G\varepsilon)^n$ is valid for any natural number n, and obviously, if $H = G^k$ then $H\varepsilon = (G^k)\,\varepsilon = (G\varepsilon)^k \subseteq G^k$ since $H\varepsilon \subseteq H$.

---

*) Similarly we can prove that the centralizer Z_A of the direct product $A = \prod_\alpha A_\alpha$, where A_α is of order p in an arbitrary p-group, coincides with the intersection $\bigcap_\alpha N_{A_\alpha}$ of the normalizers of all direct factors A_α of the subgroup A of G.

**) But then every subgroup is also mapped into itself, because if S is an arbitrary subgroup of G and $h \in S$, then $\{h\} \subseteq S$ and $h\varepsilon \in \{h\}\,\varepsilon \subseteq \{h\} \subseteq S$ holds for every endomorphism ε of G.

LEMMA 4. *A p-group with property P always has a non-trivial centre.*

Proof. Let G be an arbitrary p-group with property P. Every element of order p of the group G generates a cyclic subgroup which by Lemma 3, is also a normal subgroup in G. However, by Lemma 1, this normal subgroup of order p is contained in the centre of the group G.

LEMMA 5. *Any two elements a, b of a group G with property P generate a metabelian subgroup $T = \{a, b\}$.*

Proof. Let Z be the centre of T. Let us consider the commutator element $[a, b] = a^{-1} b^{-1} ab$ of a and b. By Lemma 3, $c = [a, b]$ is contained in the cut $\{a\} \cap \{b\}$ from the set theory, and therefore $c \in Z$. In this view the commutator of two arbitrary elements of T, which we can write in the form $a^n b^m$ and $a^s b^t$, obviously is $[a^n b^m, a^s b^t] = [a, b]^k$ where k is the determinant of order two $\begin{vmatrix} n & m \\ s & t \end{vmatrix}$, since $c^k \in Z$.

LEMMA 6. *In the group G with property P all elements of p-power order form a subgroup G_p called the p-component of G.*

Proof. Let $a, b \in G_p$ and $O(a) = p^m$, $O(b) = p^n$, moreover $l = \max(p^m, p^n)$. Then $O(a^{-1}) = O(a)$ since $a^{-1} \in G_p$ and therefore we now consider the subgroup $T = \{a, b\}$, which, by Lemma 5, is metabelian, since in T and thus also in G the identity

$$(a\,b)^{l^2} = (a^l \cdot b^l \cdot [b, a]^{\binom{l}{2}})^l$$

holds. By Lemma 3, $c = [b, a] \in \{a\} \cap \{b\}$ and thus $c = a^m$, so that

$$(a\,b)^{l^2} = (1 \cdot 1 \cdot a^{m\binom{l}{2}})^l$$

since by $O(a\,b) \mid l^2$ the relation $ab \in G_p$ obviously holds.

LEMMA 7. *A torsion group G with property P always has non-trivial centre.*

Proof. If the prime numbers p and q are different, then the intersection $G_p \cap G_q$ of the p-component and of the q-component of G is obviously the subgroup $\{1\}$. But $O(x^{-1}gx) = O(g)$, since by Lemma 6 G_p and G_q are normal subgroups of G, therefore $G_p \subseteq Z_{G_q}$ and $G_q \subseteq Z_{G_p}$. Thus we can write the direct product $D = \prod_\nu G_{p_\nu}$ of all p_ν-components of the group G. Now we prove that $D = G$. Let $g \in G$ and $O(g) = n = p_1^{\alpha_1} \dots p_s^{\alpha_s}$. We define the natural numbers $n_1, \dots, n_s$ as follows; $n = n_1 p_1^{\alpha_1} = \dots = n_s p_s^{\alpha_s}$. Then the numbers $n_1, \dots, n_s$ are relatively primes, since there exists a system $t_1, \dots, t_s$ of rational integers, for which $n_1 t_1 + \dots + n_s t_s = 1$ holds. Let $g_j = g^{n_j t_j}$, then $g_j \in G_{p_j}$ and $g = g_1 \dots g_s \in D$. Therefore $G = D$. But every p-component, as a direct factor of G is by Lemma 4 a subgroup with property P without centre. The centre of a direct product is the direct product of the centres of all direct factors, therefore the torsion group G with property P, itself, is never without centre.

§ 3. A description of the class of the cyclic groups

Of late years many group-theoretical investigations originated with the purpose of giving an explicit characterization of some class of groups defined by some fixed property. We now prove the following

THEOREM. *An arbitrary group is cyclic if and only if it has the property* P*).

Proof. First let G be an arbitrary not torsion-free group with property P, and let $g \in G$, where $O(g) = n > 1$. If $\{g\} = G^k$ then G is an m-bounded group with $m \leqq nk$. In this case we prove our theorem by induction on m. The theorem is clear for $m = 1$. Now we assume that it holds for all s-bounded groups with property P, for which $s < m$. By Lemma 7, there exists in the centre Z of G a cyclic subgroup $C = G^l \neq \{1\}$, and in view of the equality $l = mq + r$ $(0 \leqq r < m)$ and of $G^m = \{1\}$ we can put $l < m$. Then by our hypothesis of induction the factor group G/C is cyclic, because by Lemma 2 it is a group with property P and on the other hand G/C has no greater bound than t. Namely G itself is an m-bounded abelian group with property P. Then in every p-component $G_p \neq \{1\}$ of G there exists a cyclic direct factor $A_p \neq \{1\}$ of G_p [3], so that $G_p = A_p \times B_p$ with a certain subgroup B_p of G_p. But $A_p = G^n$ and on the other hand $G = A_p \times B_p \times M$. Therefore $A_p = A_p^n \times B_p^n \times M^n$ since $B_p^n = M^n = \{1\}$ namely $A_p = A_p^n$ so that $(n, p) = 1$. But then $B_p = \{1\}$, and therefore $G_p = A_p$ is a cyclic subgroup of the group G. The number of all p-components of the group G of bounded order is finite, therefore in this case G itself is a finite cyclic group.

Let now a and b be two arbitrary elements of the torsion-free group G with property P. The subgroup $T = \{a, b\}$ is, by Lemma 5, a metabelian group, and the commutator $c = [a, b]$ is contained in the cut $\{a\} \cap \{b\}$ from the set theory. If $c = a^s = b^t$, then $c^{st} = [a, b]^{st} = [a^s, b^t] = [c, c] = 1$ and thus $[a, b] = 1$. Therefore G is an abelian group. If $n \neq 0$ then the mapping φ of G into itself $g\varphi = g^n$ is an isomorphism. Let $g \in G$ and $g \neq 1$. If $\{g\} = G^k$, then obviously G itself is cyclic.

On the other hand, it is clear that every cyclic group has the property P, which completes the proof of our theorem.

REFERENCES

1. R. BAER, *Situation der Untergruppen und Struktur der Gruppen*, S. B. Heidelberg. Akad., 1933, **2**, 12—17.
2. A. G. KUROS, *Tyeorija group*. Moskow, 1953.
3. T. SZELE, *On Direct Decomposition of Abelian Groups*, Journal London Math. Soc., 1953, **28**, 247—250.
4. H. ZASSENHAUS, *Lehrbuch der Gruppentheorie*, Leipzig a. Berlin, 1937.

*) By our theorem it is clear that if a group G has the property P then to every subgroup H of G there exists a natural number n for which $H = G^n$. In a previous paper, published in Hungarian with a German summary (*Über zyklische Gruppen*, Acta Scientiarum Universitatis Debreceniensis de Ludovico Kossuth nominatae, 1955) I have proved the theorem in this paper in the following weaker form: if for every subgroup H of the group G there exists a natural number n, so that $H = G$, then G is necessarily cyclic. The proof made use of the fundamental theorem of R. Baer [1], [4].