Чехословацкий математический журнал, т. 10 (85) 1960, Прага

ON CYCLIC GROUPS

VLASTIMIL DLAB, Khartoum, Sudan

(Received April 27, 1959)

In the present paper the author proves in an elementary way the following two assertions:

1. Let G be such a group that there exist relatively prime integers $m_1, m_2, \ldots, m_k$ for which the m_i-powers $\{G^{m_i}\}$ are cyclic subgroups ($i = 1, 2, \ldots, k$). Then the group G is cyclic as well.

2. Let G be a group such that every its cyclic subgroup is a power $\{G^m\}$ of the group G for a suitable natural number m. Then G is cyclic.

1. INTRODUCTION

It is a well-known fact that every subgroup of a cyclic group G is also cyclic and that it is a power G^m of the group G for some natural number m. F. SZÁSZ has on the contrary shown in his paper [3] that such a group every (non-trivial) power of which is a cyclic subgroup is cyclic itself. The present paper shows in an elementary way that the same assertion follows already from the assumption that there exist relatively prime integres $m_1, m_2, \ldots, m_k$ such that the m_i-th powers of the fundamental group are cyclic (Corollary 2). It is shown at the same time that the assumption cannot be weakened even in the case that G is abelian (Remark 2). More generally, the following statement is proved: If t is the greatest common divisor of integers $m_1, m_2, \ldots, m_k$ and $\{G^{m_i}\}$ are cyclic subgroups of G ($i = 1, 2, \ldots, k$), then $\{G^t\}$ is also cyclic (Theorem 2). Now, the following assertion follows readily from the result obtained (see F. Szász [1], [2]): If every cyclic subgroup of a group G is a power $\{G^m\}$ for a suitable natural number m, then the group G is cyclic (and thus every subgroup of G is a power of the given group) (Theorem 3). The assumptions of the preceding theorem may be formally weakened. Let G be a group with the following property: For every cyclic subgroup $\{h\}$ of G there exists a cyclic subgroup $\{g\}$, $\{h\} \subseteq \{g\} \subseteq G$, such that $\{g\} = \{G^m\}$ for some natural number m. This property is equivalent with the proposition that G is a group with maximal cyclic subgroups which are powers of the group G. Then one can easily prove that G is a cyclic group (Remark 3).

A useful lemma is also proved in the paper, asserting that every automorphism of a subgroup of a cyclic group can be extended to an automorphism of the whole group (Lemma 1, Remark 1).

Througout this paper, the letter G (resp. with indices) always denotes a (multiplicatively written) group; elements of a group will be denoted by small Latin letters from the beginning of the alphabet while the remaining letters will denote rational integers. For any non-void subset A of G, $\{A\}$ is used to denote the subgroup of G generated by the elements of A; by G^m for a fixed integer m we shall denote the subset of the group G consisting of the elements g^m with $g \in G$; the subgroup $\{G^m\}$ is said to be the m-th power of the group G.[1] The cardinality of a group G (i. e. the order of G) will be always denoted by $\mathrm{m}(G)$, the order of an element $g \in G$ by $\mathrm{O}(g)$ and the identity element of G by e. The symbol $(m_1, m_2, \ldots, m_k)$ is used to denote the greatest common divisor of integers $m_1, m_2, \ldots, m_k$ and $m_1 | m_2$ (resp. $m_1 \nmid m_2$) denotes that m_2 is (resp. is not) divided by m_1; the symbols $\cup$, resp. $\cap$ denote, of course, the set-theoretical union, resp. intersection. $A \subset B$ means in contrast with $A \subseteq B$ that $A \neq B$.

A subgroup $\{g_0\}$ with $g_0 \in G$ is said to be a maximal cyclic subgroup of G if there does not exist any cyclic subgroup $\{g\}$ with $g \in G$ satisfying $\{g_0\} \subset \subset \{g\} \subseteq G$. If any cyclic subgroup is contained in a maximal cyclic subgroup of G, then the group G is called a group with maximal cyclic subgroups.

2. LEMMAS

First of all we are going to prove the following lemmas:

Lemma 1. *Let a cyclic group $\{a\}$ and a natural number m be given. Let b be a generator of the subgroup $\{a^m\} \subseteq \{a\}$. Then there exists an element $\bar{a} \in \{a\}$ for which the relations*

$$\bar{a}^m = b \quad \text{and} \quad \{\bar{a}\} = \{a\} \tag{2,1}$$

hold.

Proof. If $\mathrm{O}(a) = \infty$, then $\{a^m\}$ is the infinite cyclic group and it follows either $b = a^m$ or $b = a^{-m}$. Thus, it suffices to put either $\bar{a} = a$ or $\bar{a} = a^{-1}$ in this case and the relations (2,1) are obviously valid.

If $\mathrm{O}(a) < \infty$, let us denote by w the order of $a^m : \mathrm{O}(a^m) = w$; consequently

$$\mathrm{O}(a) \mid mw\,. \tag{2,2}$$

Further, we have the equality $b = a^{mt}$ with

$$(t, w) = 1\,. \tag{2,3}$$

[1]) Especially, if G is abelian, then, of course, $\{G^m\} = G^m$.

We see immediately that the elements $a_i = a^{t+iw}$, where i denotes a natural number, satisfy the equality $a_i^m = b$. Let

$$u = (t, m) \text{ and } v = (m, w) ;$$

hence, according to (2,3) also $(u, v) = 1$. Let

$$t = ut_1 , \quad w = vw_1 , \quad m = uvm_1 , \tag{2,4}$$

i. e.

$$(t_1, m_1) = 1 . \tag{2,5}$$

Let $p_1, p_2, \ldots, p_k$ be all prime numbers satisfying

$$p_l \mid m_1 , \quad p_l \nmid u \quad (l = 1, 2, \ldots, k) .$$

Further, let q be a prime number with $q \nmid u$. Now, let us denote by i_0 the product

$$i_0 = p_1 p_2 \ldots p_k q . \tag{2,6}$$

We are going to prove that the numbers $t + i_0 w$ and mw are relatively prime. Assume, in the contrary, that $t + i_0 w$ and also mw are divided by a prime number p_0; then, by (2,3) necessarily $p_0 \mid m$. Thus, according to (2,4) $p_0 \mid um_1$.

Now, $p_0 \mid u$ implies in view of (2,4) $p_0 \mid t$ and therefore $p_0 \mid i_0 w$ holds. By (2,4) we obtain $p_0 \mid i_0$ in the contradiction to (2,6). Thus, we have

$$p_0 \mid m_1 \quad \text{and} \quad p_0 \nmid u . \tag{2,7}$$

Then, according to (2,6) we deduce $p_0 \mid i_0 w$ and therefore $p_0 \mid t$; we obtain by virtue of (2,5) the contradiction with (2,7). On the whole we have

$$(t + i_0 w , \ mw) = 1 ,$$

and in view of (2,2) also

$$(t + i_0 w , \ \mathrm{O}(a)) = 1 . \tag{2,8}$$

Thus, if we define $\bar{a} = a^{t+i_0 w}$, it follows firstly $\bar{a}^m = b$ and further by (2,8) $\{\bar{a}\} = \{a\}$.

This completes the proof of Lemma 1.

Remark 1. Thanks are due to V. Vilhelm for having remarked that the assertion of Lemma 1 can be expressed in the following way: *Let H be a subgroup of a cyclic group G. Then every automorphism of H can be extended to an automorphism of the given group G.*

Lemma 2. a) *The following inclusions hold for any integers m, n*

$$\{G^{mn}\} \subseteq \{\{G^m\}^n\} \subseteq \{G^m\} . \tag{2,9}$$

b) *If $\{G^m\}$ is abelian, then even*

$$\{G^{mn}\} = \{G^m\}^n .$$

Proof. a) An arbitrary element $g \in G^{mn}$ is expressible in the form

$$g = g_1^{mn} g_2^{mn} \dots g_k^{mn} \, , \quad g_i \in G \ \text{ for } i = 1, 2, \dots, k \, , \tag{2,10}$$

from where immediately $g \in \{G^m\}^n$ follows and therefore also the relation (2,9).

b) It is sufficient to prove the converse inclusion. Let

$$g_0 = g_1^m g_2^m \dots g_k^m \, , \quad g_i \in G \ \text{ for } \ i = 1, 2, \dots, k \, , \tag{2,11}$$

be an arbitrary element of $\{G^m\}$; in consequence of commutativity the element $g = g_0^n \in \{G^m\}^n$ can be expressed in the form (2,10) and hence, in fact, $\{G^m\}^n \subseteq \subseteq \{G^{mn}\}$, q. e. d.

Lemma 3. *The subgroup $\{G^m\}$ is normal in G for every natural number m.*

Proof. Every element $g_0 \in \{G^m\}$ can be expressed in the form (2,11). If g is an arbitrary element of G, then we have the equality

$$g^{-1} g_0 g = g^{-1} g_1^m g g^{-1} g_2^m g \dots g^{-1} g_k^m g = (g^{-1} g_1 g)^m (g^{-1} g_2 g)^m \dots (g^{-1} g_k g)^m \, ,$$

and thus $g^{-1} g_0 g \in \{G^m\}$, i. e. $\{G^m\}$ is, in fact, normal in G.

Lemma 4. *Let $G = G_1 G_2$, where $G_j (j = 1, 2)$ are infinite cyclic subgroups normal in G. Then G is abelian.*

Proof. Let $G = \{a_1\}$ and $G_2 = \{a_2\}$ with

$$\mathrm{O}(a_j) = \infty \quad (j = 1, 2) \, . \tag{2,12}$$

If $G_1 \cap G_2 = (e)$, then G is obviously abelian.[2]) Thus, let $G_1 \cap G_2 \neq (e)$, i. e. there exist non-zero integers u_1, u_2 such that

$$a_1^{u_1} = a_2^{u_2} \, . \tag{2,13}$$

Since

$$a_1^{-1} a_2 a_1 = a_2^v \text{ for a suitable } v \, , \tag{2,14}$$

we have according to (2,13)

$$a_1^{u_1} = a_1^{-1} a_1^{u_1} a_1 = a_1^{-1} a_2^{u_2} a_1 = a_2^{u_2 v} = a_1^{u_1 v} \, ,$$

from where we deduce in view of (2,12) $v = 1$. Thus, G is by (2,14) abelian, as desired.

Lemma 5. *Let G^* be a cyclic normal subgroup of G. Then every subgroup of the group G^* is normal in G, as well.*

Proof. The assertion of Lemma 5 follows readily from the fact that every subgroup of a cyclic group is characteristic.

Lemma 6. *Let $G = G_1 G_2$, where $G_j (j = 1, 2)$ are finite cyclic normal subgroups of G with a non-zero intersection G_3. Let*

$$\mathrm{m}(G_j) = m_j w \quad (j = 1, 2), \ \textit{where } (m_1, m_2) = 1 \ \textit{ and } \ \mathrm{m}(G_3) = w \, . \tag{2,15}$$

---

[2]) By this assumption G is abelian generally for arbitrary abelian groups G_j $(j = 1, 2)$ normal in G; G is simply the direct product $G_1 \times G_2$.

Then there exists a cyclic subgroup $\overline{G}_1$ normal in G satisfying the relations $G = \overline{G}_1 G_2$, $G_1 \cap G_2 = \overline{G}_3$ and the following property: If we denote

$$\mathrm{m}(\overline{G}_1) = \overline{m}_1 \overline{w}\,, \quad \mathrm{m}(G_2) = \overline{m}_2 \overline{w} \quad \text{and} \quad \mathrm{m}(\overline{G}_3) = \overline{w}\,, \tag{2,16}$$

then

$$\overline{m}_2 \mid \overline{w} \tag{2,17}$$

and

$$(\overline{m}_1, \overline{m}_2) = 1\,. \tag{2,18}$$

At the same time the following implication holds: If $m_1|w$, then $\overline{m}_1|\overline{w}$.

Proof. By Lemma 1 there exist by (2.15) elements $a_j \in G_j (j = 1, 2)$ and $c \in G_3$ such that

$$G_j = \{a_j\}\ (j = 1, 2),\ G_3 = \{c\} \text{ and } a_1^{m_1} = a_2^{m_2} = c\,, \quad (m_1, m_2) = 1\,. \tag{2,19}$$

Thus, $\mathrm{O}(a_j) = m_j w\ (j = 1, 2)$. If $m_2 \mid w$, it suffices to put $\overline{G}_1 = G_1$ and the assertion of lemma follows in a trivial way.

In the contrary case, let $(m_2, w) = z$; consequently, there exist integers $u_j, v_j (j = 1, 2)$ such that

$$u_1 m_2 + u_2 w = z \tag{2,20}$$

and

$$m_2 = v_1 z\,, \quad w = v_2 z\,. \tag{2,21}$$

The subgroup G_3 is obviously normal in G; consider that the quotient group G/G_3 is abelian (see the footnote[2]) and that, consequently,

$$a_1^{-1} a_2 a_1 = a_2^{1+km_2} \quad \text{for a certain integer } k\,;$$

hence

$$a_1^{-1} a_2^w a_1 = a_2^w\,. \tag{2,22}$$

Then, using (2,20) and (2,19) together with (2,22) we obtain

$$a_1^{-1} a_2^z a_1 = a_1^{-1} a_2^{u_1 m_2} a_1 a_1^{-1} a_2^{u_2 w} a_1 = a_2^{u_1 m_2} a_2^{u_2 w} = a_2^z\,, \tag{2,23}$$

i. e. the elements a_1 and a_2^z are commutative. Since $(m_1, m_2) = 1$, we have by (2,21) $(m_1, v_1) = 1$ and therefore there exist integers $l_j\ (j = 1, 2)$ such that

$$l_1 m_1 + l_2 v_1 = 1\,. \tag{2,24}$$

Let us put

$$b = a_1^{l_2} a_2^{z l_1}\,. \tag{2,25}$$

Then in view of (2,25), (2,23), (2,21), (2,19) and (2,24) we can deduce

$$b^{v_1} = a_1^{l_2 v_1} a_2^{z l_1 v_1} = a_1^{l_2 v_1} a_2^{l_1 m_2} = a_1^{l_2 v_1} a_1^{l_1 m_1} = a_1$$

and

$$b^{m_1} = a_1^{l_2 m_1} a_2^{z l_1 m_1} = a_2^{l_2 m_2} a_2^{z l_1 m_1} = a_2^{z(l_2 v_1 + l_1 m_1)} = a_2^z\,. \tag{2,26}$$

The group $\overline{G}_1 = \{b\}$ is by (2,25) obviously the group union of its subgroups $G_1 = \{a_1\}$ and $\{a_2^z\}$ which are by Lemma 5 normal in G; thus, $\overline{G}_1$ is also normal in G. Since, obviously, $\{\overline{G}_1 \cup G_2\} = G$, we have $G = \overline{G}_1 G_2$. Let $\overline{G}_1 \cap G_2 = \overline{G}_3$ and let (2,16) holds. Since $\{a_2^z\} \subseteq \overline{G}_3$ and since by (2,21) $\mathrm{O}(a_2^z) = v_1 w$, it follows

$$w \mid \overline{w} \quad \text{and} \quad \overline{m}_2 \mid z \,, \tag{2,27}$$

and hence according to (2,21) the relation (2,17) is fulfilled. Further, since $\overline{m}_2 \mid m_2$ in view of (2,27) and (2,21) and $\overline{m}_1 \mid m_1$ in view of (2,26), we deduce that (2,18) is also valid.

Finally, the validity of $m_1 \mid w$ implies in consequence of $\overline{m}_1 \mid m_1$ and $w \mid \overline{w}$ also $\overline{m}_1 \mid \overline{w}$.

This completes the proof of Lemma 6.

Lemma 7. *Let $G = \tilde{G}_1 \tilde{G}_2$, where $\tilde{G}_j$ $(j = 1, 2)$ are finite cyclic normal subgroups of G with non-zero intersection $\tilde{G}_3$. Let*

$$\mathrm{m}(\tilde{G}_j) = \tilde{m}_j \tilde{w} \ (j = 1, 2) \ \textit{with} \ (\tilde{m}_1, \tilde{m}_2) = 1 \ \textit{and} \ \mathrm{m}(\tilde{G}_3) = \tilde{w} \,. \tag{2,28}$$

Let, further,

$$\tilde{m}_j \mid \tilde{w} \quad \textit{for} \quad j = 1, 2 \,. \tag{2,29}$$

Then G is abelian.

Proof. According to Lemma 1 there exist by virtue of (2,28) elements $b_j \in \tilde{G}_j$ $(j = 1, 2)$ and $d \in \tilde{G}_3$ such that

$$\tilde{G}_j = \{b_j\} \ (j = 1, 2) \,, \quad \tilde{G}_3 = \{d\} \,, \quad b_1^{\tilde{m}_1} = b_2^{\tilde{m}_2} = d \,, \quad (\tilde{m}_1, \tilde{m}_2) = 1 \,. \tag{2,30}$$

Hence,

$$\mathrm{O}(b_j) = \tilde{m}_j \tilde{w} \quad \text{for} \quad j = 1,2 \,. \tag{2,31}$$

By (2,29) there exist, moreover, integers $\tilde{u}_j (j = 1,2)$ satisfying

$$\tilde{w} = \tilde{u}_j \tilde{m}_j \ (j = 1,2) \,. \tag{2,32}$$

Let

$$b_1^{-1} b_2 b_1 = b_2^r \,. \tag{2,33}$$

Thus, by virtue of (2,30) and (2,33) we obtain

$$b_2^{\tilde{m}_2} = b_1^{-1} b_2^{\tilde{m}_2} b_1 = b_2^{r \tilde{m}_2} \,,$$

i. e.

$$\tilde{m}_2 \equiv \tilde{m}_2 r \pmod{\tilde{m}_2 \tilde{w}} \,. \tag{2,34}$$

Further, (2,30) and (2,33) imply that

$$b_2 = b_1^{-\tilde{m}_1} b_2 b_1^{\tilde{m}_1} = b_2^{r^{\tilde{m}_1}} \,,$$

i. e.

$$r^{\tilde{m}_1} \equiv 1 \pmod{\tilde{m}_2 \tilde{w}} \,. \tag{2,35}$$

Now, in view of (2,34) and (2,35) we get the equalities

$$r = k\tilde{w} + 1 \tag{2,36}$$

and

$$(k\tilde{w} + 1)^{\tilde{m}_1} - 1 = l\tilde{m}_2\tilde{w} \tag{2,37}$$

for suitable integers k, l. From (2,37) we readily derive by a simple computation

$$\sum_{i=0}^{\tilde{m}_1-1} \binom{\tilde{m}_1}{i} k^{\tilde{m}_1-i}\tilde{w}^{\tilde{m}_1-i-1} = l\tilde{m}_2 ,$$

i. e. according to (2,32)

$$k\tilde{m}_1 \left(\sum_{i=0}^{\tilde{m}_1-2} \binom{\tilde{m}_1}{i} k^{\tilde{m}_1-i-1}\tilde{w}^{\tilde{m}_1-i-2}\tilde{u}_1 + 1 \right) = l\tilde{m}_2 . \tag{2,38}$$

Since $(\tilde{m}_1, \tilde{m}_2) = 1$, it follows by (2,32) $\tilde{m}_2 \mid \tilde{u}_1$ and hence

$$\left(\tilde{m}_2, \sum_{i=0}^{\tilde{m}_1-2} \binom{\tilde{m}_1}{i} k^{\tilde{m}_1-i-1}\tilde{w}^{\tilde{m}_1-i-2}\tilde{u}_1 + 1 \right) = 1 .$$

Now, $\tilde{m}_2 \mid k$ follows immediately from (2,38). At last, using (2,36) and (2,31) together with (2,33) we get

$$b_1 b_2 = b_2 b_1$$

and thus, G is abelian, as desired.

3. THEOREMS

Theorem 1. *Let G be such a group that there exist two integers m_1, m_2 satisfying the condition that $\{G^{m_1}\}$ and $\{G^{m_2}\}$ are cyclic. If $(m_1, m_2) = t$, then the subgroup $\{G^t\}$ is cyclic, too.*

Proof. The subgroup $\{G^{m_1}\}$ and $\{G^{m_2}\}$ are, in view of Lemma 3, normal in G. According to Lemma 2a) it follows readily $\{G^t\} \supseteq \{G^{m_j}\}$ and, further, $\{G^{m_j}\}$ are, obviously, normal in $\{G^t\}$ $(j = 1, 2)$. We can easily see that

$$\{G^t\} = \{G^{m_1}\} \{G^{m_2}\} . \tag{3,1}$$

For $(m_1, m_2) = t$ implies the existence of integers k_1, k_2 such that

$$k_1 m_1 + k_2 m_2 = t , \tag{3,2}$$

and thus we have for an arbitrary element $g \in G^t$ in view of (3,2) the relations (with a suitable element $g_0 \in G$)

$$g = g_0^t = g_0^{k_1 m_1 + k_2 m_2} = (g_0^{m_1})^{k_1} (g_0^{m_2})^{k_2} \in \{G^{m_1}\} \{G^{m_2}\} ,$$

and every element of the group $\{G^t\}$ is then a product of elements of G^t. Now, (3,1) follows already from the fact that $\{G^{m_j}\}$ are normal in $\{G^t\}$ $(j = 1, 2)$.

Further, there exist integers m_1', m_2' such that

$$m_1 = m_1' t , \quad m_2 = m_2' t , \quad (m_1', m_2') = 1 , \tag{3,3}$$

and hence by virtue of Lemma 2b) we deduce

$$\{G^{m_1}\}^{m_2'} = G^{m_1 m_2'} = G^{m_1' m_2} = \{G^{m_2}\}^{m_1'} . \tag{3,4}$$

If $\{G^{m_1}\} = \{\bar{a}_1\}$, $\{G^{m_2}\} = \{\bar{a}_2\}$, it follows by (3,4)

$$\{\bar{a}_1^{m_2'}\} = \{a_2^{m_1'}\} ,$$

and therefore according to Lemma 1 there exists an element $\bar{a}_2 \in \{G^{m_2}\}$ such that $\{G^{m_2}\} = \{\bar{a}_2\}$ and that

$$\bar{a}_1^{m_2'} = \bar{a}_2^{m_1'} \tag{3,5}$$

holds.

Now, let us consider the following two cases which may take place.

A. If

$$\{G^{m_1}\} \cap \{G^{m_2}\} = (e) , \tag{3,6}$$

then the group $\{G^t\}$ is evidently commutative (see the footnote[2]).[3]) Also in the case that G contains an element of the infinite order the group $\{G^t\}$ is necessarily in view of Lemma 4 commutative, for $\{G^{m_1}\}$ and $\{G^{m_2}\}$ are infinite cyclic groups with (3,1) normal in $\{G^t\}$. Now, we can already easily prove that $\{G^t\}$ is a cyclic group generated by the element $\bar{g}$ of the form

$\bar{g} = \bar{a}_1^{k_1}\bar{a}_2^{k_2}$, where k_j $(j = 1, 2)$ are the integers satisfying (3,2).

For, using the commutativity of the elements $\bar{a}_1$ and $\bar{a}_2$ we have according to (3,5), (3,2) and (3,3)

$$\bar{g}^{m_1'} = \bar{a}_1^{k_1 m_1'}\,\bar{a}_2^{k_2 m_1'} = \bar{a}_1^{k_1 m_1'}\bar{a}_1^{k_2 m_2'} = \bar{a}_1$$

and

$$\bar{g}^{m_2'} = \bar{a}_1^{k_1 m_2'}\bar{a}_2^{k_2 m_2'} = \bar{a}_2^{k_1 m_1'}\bar{a}^{k_2 m_2'} = \bar{a}_2 .$$

B. It remains to consider the case when both subgroups $\{G^{m_1}\}$ and $\{G^{m_2}\}$ are finite cyclic groups and (3,6) does not hold. We can easily see that the assumptions of Lemma 6 are fulfilled. The double use of Lemma 6 gives us the following expression for the group $\{G^t\}$:

$$\{G^t\} = \tilde{G}_1\tilde{G}_2 , \quad \tilde{G}_1 \cap \tilde{G}_2 = \tilde{G}_3 ,$$

where $\tilde{G}_j$ $(j = 1, 2)$, resp. $\tilde{G}_3$ are cyclic subgroups of the orders $\tilde{m}_j\tilde{w}$, resp. $\tilde{w}$, normal in G and

$$\tilde{m}_j \mid \tilde{w}\ (j = 1, 2) \text{ and } (\tilde{m}_1, \tilde{m}_2) = 1 . \tag{3,7}$$

Then, in view of Lemma 7 $\{G^t\}$ is certainly commutative even in this case. Further, by Lemma 1 there exist elements $\tilde{b}_j \in \tilde{G}_j$ such that

$$\tilde{G}_j = \{\tilde{b}_j\}\ (j = 1, 2) \text{ and } \tilde{b}^{\tilde{m}_1} = \tilde{b}^{\tilde{m}_2} . \tag{3,8}$$

[3]) Thus, by (3,5) and (3,6) the relations $\mathrm{O}(\bar{a}_1)|m_2'$ and $\mathrm{O}(\bar{a}_2)|m_1'$ follow for the generators $\bar{a}_j$ $(j = 1, 2)$ and hence $(\mathrm{O}(\bar{a}_1), \mathrm{O}(\bar{a}_2)) = 1$, from where we readily obtain that $\{G^t\}$ is cyclic.

In consequence of (3,7) there exist integers l_j ($j = 1, 2$) satisfying

$$l_1\tilde{m}_1 + l_2\tilde{m}_2 = 1$$

and then we can easily derive by virtue of (3,8) again that

$$\{G^t\} = \{\tilde{g}\}, \quad \text{where} \quad \tilde{g} = \tilde{b}_1^{l_2}\tilde{b}_2^{l_1}\,.$$

This completes the proof of Theorem 1.

Corollary 1. *Let a group G be given. If there exist integers m_1, m_2 which are relatively prime such that $\{G^{m_1}\}$ and $\{G^{m_2}\}$ are cyclic subgroups, then G itself is cyclic.*

Now, we are going to prove by means of Theorem 1 the main result.

Theorem 2. *Let G be such a group that there exist integers $m_1, m_2, \ldots, m_k$ for which the m_i-th powers $\{G^{m_i}\}$ are cyclic subgroups ($i = 1, 2, \ldots, k$). If $(m_1, m_2, \ldots, m_k) = t$, then the subgroup $\{G^t\}$ is cyclic, too.*

Proof. We prove the above theorem by induction. The assertion is trivial when $k = 1$. Assume that the assertion is valid for a certain i, $1 \leqq i \leqq k$, i. e. that $\{G^{t_i}\}$ is cyclic, where $t_i = (m_1, m_2, \ldots, m_i)$. But then, according to Theorem 1, also the subgroup $\{G^{t_{i+1}}\}$ is cyclic, where

$$t_{i+1} = (t_i, m_{i+1}) = (m_1, m_2, \ldots, m_{i+1})\,.$$

This concludes the proof of Theorem 2.

Corollary 2. *Let a group G be given. If there exist integers $m_1, m_2, \ldots, m_k$ which are relatively prime such that $\{G^{m_i}\}$ ($i = 1, 2, \ldots, k$) are cyclic subgroups, then G is cyclic itself.*

Remark 2. Let us observe that the assumptions of Theorem 2 (resp. Theorem 1) can not be weakened, even at the supplementary assumption of commutativity of the group G. That is quite clear, if we take into account that G can be, e. g., the direct product of its subgroup $\{G^t\}$ and a subgroup with elements the orders of which are divisors of t.

It follows from Theorem 2 immediately also the following result (see F. Szász [1], [2]):

Theorem 3. *If every cyclic subgroup of a group G is a power $\{G^m\}$ of this group for a suitable integer m, then G is cyclic.*

Proof. By our assumption there correspond to every cyclic subgroup $\{g\} \subseteq G$ certain integers m for which $\{G^m\} = \{g\}$. Let us denote by $\mathscr{M}$ the set of integers thus obtained for all cyclic subgroups of G. Let t be the greatest common divisor of the elements of $\mathscr{M}$; then there exists already a finite number of elements $m_1, m_2, \ldots, m_k$ of $\mathscr{M}$ such that $(m_1, m_2, \ldots, m_k) = t$. Thus, according to Theorem 2, $\{G^t\}$ is cyclic.

Now, it is easy to prove that $\{G^t\} = G$. For, if g is an arbitrary element of the group G, then

$$\{g\} = \{G^{tw}\} \text{ for a suitable integer } w.$$

In view of Lemma 2 a) we obtain

$$\{g\} = \{G^{tw}\} \subseteqq \{G^t\}, \quad \text{i. e.} \quad g \in \{G^t\}$$

and the proof of Theorem 3 is complete.

Remark 3. Let us observe that the group every cyclic subgroup of which is a power $\{G^m\}$ of G is a group with maximal cyclic subgroups. For, if $\{g_0\}$ is a cyclic subgroup which is not contained in a maximal one, then there exists an infinite ascending series of cyclic subgroups

$$\{g_0\} \subset \{g_1\} \subset \{g_2\} \subset \ldots \subset \{g_i\} \subset \ldots,$$

where

$$g_{i-1} = g_i^{m_i} \text{ with } m_i \geqq 2 \text{ for } i = 1, 2, \ldots$$

Since $\{g_0\} = \{G^{m_0}\}$, we get

$$m_1 m_2 \ldots m_i \mid m_0 \text{ for every } i = 1, 2, \ldots$$

and obtain a contradiction. Now, one can easily see that the whole proof of Theorem 3 may be repeated at the only assumption that the maximal cyclic subgroups are powers of the group G. Thus, we can formally express Theorem 3 as follows:

Let G be a group with the following property: For every cyclic subgroup $\{h\}$ of G there exists a cyclic subgroup $\{g\}$, $\{h\} \subseteqq \{g\} \subseteqq G$, such that $\{g\} = \{G^m\}$ for a suitable integer m.[4]) *Then G is cyclic.*

Bibliography

[1] *F. Szász:* On groups every cyclic subgroup of which is a power of the group, Acta Math. Acad. Sci. Hung., *6* (1955), 475—477.

[2] *F. Szász:* On cyclic groups, Fundamenta Math., *43* (1956), 238—240.

[3] *F. Szász:* Über Gruppen, deren sämtliche nicht-triviale Potenzen zyklische Untergruppen der Gruppe sind, Acta Sci. Math. Szeged, *17* (1956). 83—84.

[4]) Of course, by Lemma 2b) $\{h\} = \{g^n\} = \{g\}^n = \{G^m\}^n = \{G^{mn}\}$.

Резюме

О ЦИКЛИЧЕСКИХ ГРУППАХ

ВЛАСТИМИЛ ДЛАБ (Vlastimil Dlab), Кхартоум, Судан

В настоящей статье доказывает автор элементарным способом следующие утверждения, обобщающие результаты Ф. Саса (см. [1] и [2]):

Теорема 2. *Пусть G обладает следующим свойством: Существуют целые числа $m_1, m_2, \ldots, m_k$ так, что подгруппы $\{G^{m_i}\}$*[1] *цикличны ($i = 1, 2, \ldots, k$). Пусть t — наибольший общий делитель чисел $m_1, m_2, \ldots, m_k$. Тогда $\{G^t\}$ есть циклическая подгруппа.*

Следствие 2. *Пусть G — группа. Если существуют взаимно простые числа $m_1, m_2, \ldots, m_k$ такие, что $\{G^{m_i}\}$ суть циклические подгруппы ($i = 1, 2, \ldots, k$), то группа G также циклична.*

В статье показано также, что утверждения нельзя уже усилить (ни в случае, когда G — абелева группа). Утверждение теоремы 2 вытекает непосредственно по индукции из теоремы 1, доказательство которой опирается на сравнительно сложные леммы (лемма 6 и лемма 7). При помощи этих лемм мы получаем следующий результат:

Пусть $G = G_1G_2$, где G_j ($j = 1, 2$) — конечные, циклические нормальные делители в G. Пусмь индекцы пересечения $G_1 \cap G_2$ в G_1 и в G_2 взаимно просты. Тогда группа G является абелевой.

В статье автор существенным способом пользуется тоже утверждением леммы 1, обеспечивающим *продолжаемость всякого автоморфизма подгруппы циклической группы до автоморфизма всей группы.*

Из теоремы 2 далее легко вытекает

Теорема 3. (См. Ф. Сас [3]) *Если всякая циклическая подгруппа группы G является степенью $\{G^m\}$ этой группы для подходящего m, то группа G циклична.*

[1]) $\{G^{m_i}\}$ обозначает подгруппу, образованную всеми элементами g^{m_i}, $g \in G$.