Note di Matematica **23,** n. 1, 2004, 1–6.

Nonperiodic product of subsets and Hajós' theorem

Sándor Szabó
Department of Mathematics
Institute of Mathematics and Informatics, University of Pécs,
Ifjúság u. 6. H-7624 Pécs, HUNGARY
sszabo7@hotmail.com

Received: 4/4/1998; accepted: 3/10/2003.

Abstract. G. Hajós proved that if a finite abelian group is a direct product of its cyclic subsets, then at least one of the factors must be a subgroup. We give a new elementary proof of this theorem based on the special case for p-groups.

Keywords: factorization of finite abelian groups, Hajós-Rédei theory.

MSC 2000 classification: 20K01 (primary); 52C22.

1 Introduction.

Throughout this paper we will use multiplicative notation in connection with abelian groups. Let $A_1, \dots, A_n$ be subsets of the finite abelian group G. If the product $A_1 \cdots A_n$ is direct and is equal to G, then we say that $G = A_1 \cdots A_n$ is a *factorization* of G. The subset A of G is called *cyclic* if there is a prime p and an element a of G such that $|a|$ the order of a is at least p and

$$A = \{e, a, a^2, \dots, a^{p-1}\}.$$

Here e is the identity element of G.

In 1941 G. Hajós proved that if a finite abelian group is factored into cyclic subsets, then at least one of the factors must be a subgroup.

We say that a subset A of G is *periodic* with period g if $g \in G$, $Ag = A$ and $g \neq e$. Under certain conditions the product of nonperiodic subsets is itself nonperiodic. This observation suggests a plan to prove Hajós' theorem. Suppose that $G = A_1 \cdots A_n$ is a factorization of the finite abelian group G into cyclic subsets which are not subgroups. From this we can draw two contradictory conclusions. As A_1 is not a subgroup, it follows that $A_2 \cdots A_n$ is periodic. On the other hand the subsets $A_2, \dots, A_n$ satisfy a conditions that guarantees that the product $A_2 \cdots A_n$ is not periodic.

2 Nonperiodic products

Let A and A' be subsets of G. We say that A is *replaceable* by A' if $G = AB$ is a factorization of G gives rise to a factorization $G = A'B$ of G for each subset B of G.

The subset A of G is called a PP ("periodicity preventing") subset if

(i) $A = \{e, a, a^2, \ldots, a^{p-1}\}$, $|a| = p^\alpha$, $\alpha \geq 2$

or

(ii) $A = \{e, a, a^2, \ldots, a^{p-2}, a^{p-1}d\}$, $|a| = p$, $|d| = q$ are distinct primes.

1 Lemma. *Suppose that $G = AB$ is a factorization of the finite abelian group G, where $A = \{e, a, a^2, \ldots, a^{p-1}\}$ is a cyclic subset.*

(a) *Then $B = a^pB$ and A can be replaced by*

$$A' = \{e, a^r, a^{2r}, \ldots, a^{(p-1)r}\}$$

for each integer r which is relatively prime to p.

(b) *If A is not a subgroup of G, then A can be replaced by a PP subset A^*.*

Proof. The fact that $G = AB$ is a factorization is equivalent to that

$$G = B \cup aB \cup a^2B \cup \cdots \cup a^{p-1}B$$

is a partition of G. Multiplying the factorization $G = AB$ by a we get the factorization $G = Ga = (aA)B$ and so

$$G = aB \cup a^2B \cup \cdots \cup a^{p-1}B \cup a^pB$$

is a partition of G. Comparing the two partitions gives that $B = a^pB$. This implies that if $i \equiv j \pmod p$, then $a^iB = a^jB$. As $0, r, 2r, \ldots, (p-1)r$ is a permutation of $0, 1, 2, \ldots, p-1$ modulo p, it follows that

$$G = B \cup a^rB \cup a^{2r}B \cup \cdots \cup a^{(p-1)r}B$$

is a partition of G and consequently $G = A'B$ is a factorization of G. This completes the proof of part (a).

In order to prove part (b) assume that A is not a subgroup and write $|a|$ in the form $|a| = p^\alpha r$, where p is relatively prime to r. Let $c = a^r$ and set

$$C = \{e, c, c^2, \ldots, c^{p-1}\}.$$

By part (a) A can be replaced by C to get the factorization $G = CB$.

Clearly $|c| = p^\alpha$ and so in the $\alpha \geq 2$ case with the $A^* = C$ choice we are done. Suppose that $\alpha = 1$. As A is not a subgroup, there is a prime q such that $q \mid r$. Let $x = a^{r/q}$ and set

$$X = \{e, x, x^2, \ldots, x^{p-1}\}.$$

Now $|x| = pq$, $|c| = p$. By part (a), A can be replaced by X. From the factorization $G = XB$ by part (a), it follows that $B = x^p B$. Let $d = x^p$. Here $|x^p| = q$. The factorization $G = CB$ is equivalent to that

$$G = B \cup cB \cup c^2 B \cup \cdots \cup c^{p-2} B \cup c^{p-1} B$$

is a partition of G. Using $B = dB$ we get that

$$G = B \cup cB \cup c^2 B \cup \cdots \cup c^{p-2} B \cup c^{p-1} dB$$

is a partition of G. Therefore A is replaceable by

$$A^* = \{e, c, c^2, \ldots, c^{p-2}, c^{p-1} d\},$$

where $|c| = p$, $|d| = q$ are distinct primes. This completes the proof. $\boxed{QED}$

2 Lemma. *Let A, B be subsets and let H be a subgroup of the finite abelian group G such that*

(i) $B \subset H$,

(ii) *the elements of A are incongruent modulo H,*

(iii) *A and B are not periodic,*

(iv) *A is a PP subset.*

If the product AB is direct, then AB is not periodic.

Proof. Let $A = \{a_0, a_1, \ldots, a_{p-1}\}$, where $a_i = a^i$ for $0 \leq i \leq p-2$ and either $a_{p-1} = a^{p-1}$ or $a_{p-1} = a^{p-1} d$. Since the product AB is direct

$$AB = a_0 B \cup a_1 B \cup \cdots \cup a_{p-1} B$$

is a partition of AB. In order to prove that AB is not periodic assume the contrary that AB is periodic with period g. We may assume that $|g| = r$ is a prime. Since $B \subset H$ and since elements of A are incongruent modulo H, it follows that the sets $a_0 B, a_1 B, \ldots, a_{p-1} B$ fall into distinct cosets $a_0 H, a_1 H, \ldots, a_{p-1} H$

modulo H. Multiplying all the cosets modulo H by g permutes these cosets. Hence multiplying the sets $a_0B, a_1B, \ldots, a_{p-1}B$ by g permutes these sets.

There is an i, $0 \leq i \leq p-1$ such that $ga_iB = a_{p-1}B$. Since B is not periodic, it follows that $g = a_{p-1}a_i^{-1}$. If $i = p-1$, then $g = e$. This is not the case and so $0 \leq i \leq p-2$. Thus $a_i = a^i$. If $a_{p-1} = a^{p-1}$, then $g = a_{p-1}a_i^{-1} = a^{p-1-i}$. Here $1 \leq p-1-i \leq p-1$. This leads to the $r = |g| = |a^{p-1-i}| = p^\alpha$, $\alpha \geq 2$ contradiction. If $a_{p-1} = a^{p-1}d$, then $g = a_{p-1}a_i^{-1} = a^{p-1-i}d$ with $1 \leq p-1-i \leq p-1$. This leads to the $r = |g| = |a^{p-1-i}d| = pq$ contradiction which completes the proof. $\boxed{QED}$

3 Hajós' theorem

If G is a p-group we can apply [2] pages 157–161. We may assume that G is not a p-group.

3 Theorem. *If $G = A_1 \cdots A_n$ is a factorization of the finite abelian group G into cyclic subset $A_1, \ldots, A_n$ of prime order, then at least one of the factors must be a subgroup of G.*

Proof. We introduce some notations. Let

$$A_i = \{e, a_i, a_i^2, \ldots, a_i^{p_i-1}\}.$$

and call the number

$$h(A_1, \ldots, A_n) = |a_1| \cdots |a_n|$$

the *height* of the cyclic subsets $A_1, \ldots, A_n$.

Assume that there is a factorization $G = A_1 \cdots A_n$ of the finite abelian group G into cyclic subsets such that none of the factors is a subgroup of G. We assume that n is minimal and for this n the height of the factors is minimal as well.

Choose a prime divisor p of $|G|$ and consider the factors among $A_1, \ldots, A_n$ whose order is p. Suppose that $A_1, \ldots, A_m$ are these factors. If a_i is a p-element for each i, $1 \leq i \leq m$, then the direct product $A_1 \cdots A_m$ is equal to the p-component of G and so by Lemma 3 of [2] page 160, it follows that one of the factors is a subgroup of G. This contradiction shows that one of the elements $a_1, \ldots, a_m$, say a_1, is not a p-element. There is a prime divisor r of $|a_1|$ such that $r \neq p$.

In the factorization $G = A_1 \cdots A_n$ replace A_1 by

$$A_1' = \{e, a_1^r, a_1^{2r}, \ldots, a_1^{(p-1)r}\}$$

to get the factorization $G = A_1' A_2 \cdots A_n$. Here $|a_1^r| < |a_1|$ and so

$$h(A_1', A_2, \ldots, A_n) < h(A_1, \ldots, A_n).$$

The minimality of the height of $A_1, \ldots, A_n$ gives that one of the factors $A_1', A_2, \ldots, A_n$ is a subgroup of G. This is a contradiction unless $A_1' = H_1$ is a subgroup of G. Note that $G^{(1)} = A_2^{(1)} \cdots A_n^{(1)}$ is a factorization of the factor group $G^{(1)} = G/H_1$, where

$$A_i^{(1)} = (A_i H_1)/H_1 = \{aH_1 : a \in A_i\}.$$

The minimality of n yields that one of the factors $A_2^{(1)}, \ldots, A_n^{(1)}$, say $A_2^{(1)}$, is a subgroup of $G^{(1)}$. Hence $H_1 A_2 = H_2$ is a subgroup of G and we get the factorization $G^{(2)} = A_3^{(2)} \cdots A_n^{(2)}$ of the factor group $G^{(2)} = G/H_2$, where $A_i^{(2)} = (A_i H_2)/H_2$. Repeating this argument leads to the ascending chain of subgroups

$$H_1 = A_1', \quad H_2 = A_1' A_2, \ldots, H_n = A_1' A_2 \cdots A_n.$$

By Lemma 1, in the factorizations $G = A_1 A_2 \cdots A_n$, $H_i = A_1' A_2 \cdots A_i$, $1 \le i \le n$ each factor A_j, $2 \le j \le n$ can be replaced by a PP subset A_j^* to get the factorizations $G = A_1 A_2^* \cdots A_n^*$ and $H_i = A_1' A_2^* \cdots A_i^*$.

The factorization $H_3 = H_2 A_3^*$ implies that the elements of A_3^* are incongruent modulo H_2. As $A_2^* \subset H_2$, Lemma 2 is applicable and gives that the product $A_2^* A_3^*$ is not periodic. In a similar way step by step we can conclude that

$$A_2^* A_3^* A_4^*, \ldots, A_2^* \cdots A_n^*$$

are not periodic.

On the other hand from the factorization $G = A_1(A_2^* \cdots A_n^*)$ by Lemma 1, it follows that $A_2^* \cdots A_n^*$ is periodic with period $a_1^{p_1}$. This contradiction completes the proof. $\boxed{QED}$

References

[1] G. Hajós: *Über einfache und mehrfache Bedeckung des n-dimensionalen Raumes mit einem Würfelngitter*, Math. Z. **47** (1983), 427–467.

[2] S. Stein, S. Szabó: Algebra and Tiling, Carus Mathematical Monograph, No. 25, MAA, 1994.