Beiträge zur Algebra und Geometrie
Contributions to Algebra and Geometry
Volume 38 (1997), No. 2, 241-248.

An Axiomatic Approach for the Hajós Theorem

Keresztély Corrádi and Sándor Szabó

Department of Computer Sciences, Eötvös University Budapest
H–1088 Budapest, Hungary
e-mail: kcorradi@ludens.elte.hu

Department of Mathematics, University of Bahrain
P. O. Box 32038 Isa Town, State of Bahrain
e-mail: es050@isa.cc.uob.bh

Abstract. Hajós' theorem asserts that if a finite abelian group is a direct product of cyclic subsets, then in fact at least one of the factors must be a subgroup of the group. A cyclic subset is the "front end" of a cyclic subgroup. We replace the cyclicity of the factors by an abstract P property in Hajós' theorem for finite abelian groups whose 2-component is cyclic.

MSC 1991: 20K01 (primary), 52C22 (secondary)
Key words and phrases: factorization of finite abelian groups, Hajós-Rédei theory

1. Introduction

Let G be a finite abelian group written multiplicatively with identity element e. If $B, A_1, \ldots, A_n$ are subsets of G such that each b in B is uniquely expressible in the form

$$b = a_1 \cdots a_n, \qquad a_1 \in A_1, \ldots, a_n \in A_n,$$

and each product $a_1 \cdots a_n$ belongs to B, that is, if the product $A_1 \cdots A_n$ is direct and is equal to B, then we say that B is factored by subsets $A_1, \ldots, A_n$. The equation $B = A_1 \cdots A_n$ is also said to be a *factorization* of B. If $e \in B \cap A_1 \cap \cdots \cap A_n$, then the factorization $B = A_1 \cdots A_n$ and the subsets $B, A_1, \ldots, A_n$ are said to be *normed*.

Clearly the product $A_1 \cdots A_n$ is a factoring of B if and only of $A_1 \cdots A_n = B$ and $|A_1| \cdots |A_n| = |B|$. Direct product of subsets is a straightforward generalization of direct product of subgroups which is a commonly used construction. However factoring a finite abelian group into certain type of subsets also admits important applications.

The subset A of G is called *cyclic* if it is of form $\{e, a, a^2, \dots, a^{r-1}\}$, where a is an element of $G \setminus \{e\}$ and r is a positive integer. Loosely speaking this cyclic subset consists of the "first consecutive" r elements of $\langle a \rangle$, the cyclic subgroup generated by the element a. We would like to point out that it is assumed that $|a|$, the order of a, is at least r.

G. Hajós [3] proved that if a finite abelian group is a direct product of cyclic subsets, then at least one of the factors must be a subgroup of the group.

We say that the subset A of the finite abelian group is *periodic* if there is an element $g \in G \setminus \{e\}$ such that $gA = A$. We refer such g elements as *periods* of A. It turns out that if a cyclic subset is periodic, then it is a subgroup of G. Therefore we may reformulate Hajós' theorem into the next form. If a finite abelian group is a direct product of cyclic subsets, then at least one of the factors is periodic.

We replace the cyclicity of the factors by an abstract property of the factors which still guarantees that at least one of the factors is periodic.

Let G be a finite abelian group, A a subset and ϕ a homomorphism of G into another group. We say that a subset A of G posseses the P property if for each homomorphism ϕ and subset B of $\phi(G)$ the factorization $\phi(G) = \phi(A)B$ implies that either $\phi(A)$ or B is periodic.

The main result of the paper is the following. If the 2-component of a finite abelian group is cyclic and the group is a direct product of subsets possessing the P property, then at least one of the factors is periodic.

As we will see cyclic subsets do have the P property and there are further examples of subsets with the P property. Therefore this result extends Hajós' theorem for finite abelian groups whose 2-component is cyclic.

2. Examples for subsets with the P property

Let G be a finite abelian group and let A be a subset of G. If there is a subgroup H of G such that $|H| = |A|$ and $|H \cap A| \geq |A| - 1$, then we say that A is a *simulated* subset of G. A simulated subset is either a subgroup or differs from a subgroup in one element. In order to avoid trivial cases we assume that for a simulated subset $|A| \geq 2$. When $|A| = 2$, then the simulated subset A is a cyclic subset. Simulated subsets were introduced in [1].

When A is the cyclic subset $\{e, a, a^2, \dots, a^{r-1}\}$, then A and aA differ mutually in at most one elements, that is, there is at most one element of A which is not in aA and conversely there is at most one element of aA which is not in A. Motivated by this observation Fuchs [2] introduced the concept of weakly periodic subset. The subset A of G is called *weakly periodic* if there is an element $a \in G \setminus \{e\}$ such that A and aA differ mutually in at most one element. We give a more explicit description of a weakly periodic set. Consider the one-to-one map $f : G \to G$ defined by $f(g) = ga$ for each $g \in G$. The map f as a permutation of the elements of G can be decomposed into disjoint cycles. Each cycle has the same length. Namely this common length is $|a|$, the order of a. Elements belonging to the same cycle form a coset modulo $\langle a \rangle$, the subgroup generated by a. The elements of A are distributed over these cycles. Some cycles are completely filled by elements of A. There is at most only one cycle which is not completely filled. The elements on this cycle form one connected arc. Thus a quasi periodic subset is of the form $C\langle a\rangle \cup b\{e, a, a^2, \ldots, a^{r-1}\}$, where C is a subset, b an element of G, further the union is disjoint and the products are direct. When C is empty, A is a translate of a cyclic subset. When the translated cyclic part is missing, A is periodic.

We call the subset A a *distorted cyclic* subset if it is of form

$$\{e, a, a^2, \ldots, a^{i-1}, a^i d, a^{i+1}, \ldots, a^{r-1}\},$$

where $a, d \in G$. When $d = e$, then A is a cyclic subset. When $a^r = e$, that is, when $\{e, a, a^2, \ldots, a^{r-1}\}$ is a subgroup, then A is a simulated subset.

Let D be a periodic subset of G with period a. Thus the elements of D fill complete cosets modulo $\langle a\rangle$. Choose elements $d \in D$ and $c \in G$ and set $A = \{c\} \cup \big(D \setminus \{d\}\big)$. We call A a *distorted periodic* subset. If $c = d$, then $A = D$ and so A is periodic. If $c \in D \setminus \{d\}$, then $A = D \setminus \{d\}$ and so A is a weakly periodic subset. If $D = H$ is a subgroup of G, then A is a simulated subset.

In general the homomorphic image of a subset is not even a subset rather it might be a multiset which contains elements with multiplicities distinct from 1 and 0. In order to see the details more sharply consider a homomorphism ϕ from the group G onto the group G' and let A be a subset of G. Let K be the kernel of ϕ. By the homomorphism theorem the factor group G/K is isomorphic to $\phi(G) = G'$. In the factor group G/K the homomorphic image $\phi(A)$ of A corresponds to the collection of cosets aK, where $a \in A$. If elements of A are incongruent modulo K, then the cosets aK are distinct and so $\phi(A)$ is a subset of $\phi(G) = G'$. In our considerations the only type of homomorphism ϕ occurring for which $\phi(G) = \phi(A)B$ is a factorization of $\phi(G)$. In these cases clearly $\phi(A)$ must be a subset and not merely a multiset of $\phi(G)$.

Consider the cyclic subset $A = \{e, a, a^2, \ldots, a^{r-1}\}$ of G and assume that elements of A are incongruent modulo K. Now $\phi(A)$ consists of the cosets $eK, aK, a^2K, \ldots, a^{r-1}K$ and these cosets are distinct elements of the factor group G/K. Further as these cosets can be written in the forms $(aK)^0, (aK)^1, (aK)^2, \ldots, (aK)^{r-1}$, the homomorphic image $\phi(A)$ is a cyclic subset of $\phi(G)$. Similar arguments yield that if A is a simulated, a weakly periodic or a distorted cyclic or a distorted periodic subset of G and the elements of A are incongruent modulo K, then $\phi(A)$ is again such a subset of $\phi(G)$.

The next lemma establishes that these subsets possess the P property.

Lemma 1. *Let $G = AB$ be a normed factorization of the finite abelian group G, where A is a cyclic or simulated or weakly periodic or distorted cyclic or distorted periodic subset. Then either A or B is periodic.*

Proof. First assume that A is the cyclic subset $\{e, a, a^2, \ldots, a^{r-1}\}$. The fact that $G = AB$ is a factorization can be recasted in the way that the sets

$$B, Ba, Ba^2, \ldots, Ba^{r-1} \tag{1}$$

form a partition of G. Multiplying the factorization $G = AB$ by a gives the factorization $G = Ga = (Aa)B$ and so the sets

$$Ba, Ba^2, \ldots, Ba^{r-1}, Ba^r$$

also form a partition of G. If $Ba^i \cap Ba^r \neq \emptyset$ for some i, $1 \leq i \leq r-1$, then there is an element g of G such that $g \in Ba^i \cap Ba^r$. Then $ga^{-1} \in Ba^{i-1} \cap Ba^{r-1}$. But by (1) $Ba^{i-1} \cap Ba^{r-1} = \emptyset$. Consequently $Ba^r = B$. From this it follows that either B is periodic or $a^r = e$ in which case A is periodic.

Suppose that A is a simulated subset and let H be the associated subgroup. Let us introduce the notation $H = \{h_1, \ldots, h_s\}$, where $h_1 = e$. We may assume that $A = \{h_1, h_2, \ldots, h_{s-1}, h_s d\}$ since this is only a matter of indexing the elements of H. If $|A| = 2$, then A is a cyclic subset and we are done. If $d = e$, then A is equal to the subgroup H which is clearly periodic. Thus we may assume that $|A| \geq 3$ and $d \neq e$. The factorization $G = AB$ gives that the subsets

$$Bh_1, Bh_2, \ldots, Bh_{s-1}, Bh_s d \tag{2}$$

form a partition of G. We show that in the factorization $G = AB$ the factor A can be replaced by the associated subgroup H, that is, the subsets

$$Bh_1, Bh_2, \ldots, Bh_{s-1}, Bh_s \tag{3}$$

form a partition of G. Now comparing (2) and (3) it follows that $Bh_s = Bh_s d$ and so d is a period of B. The only thing we should verify is that $Bh_s \cap Bh_i = \emptyset$ for each i, $1 \leq i \leq s-1$. Assume the contrary that $x \in Bh_s \cap Bh_i$. If $i \neq 1$, then we have the contradiction $xh_i^{-1} \in Bh_i h_i^{-1} \cap Bh_s h_i^{-1} = B \cap Bh_j$ with some j, $2 \leq j \leq s-1$. If $i = 1$, then since $|H| \geq 3$, there is a $h_j \in H$ with $2 \leq j \leq s-1$. Now we have the contradiction $xh_j \in Bh_1 h_j \cap Bh_s h_j = Bh_j \cap Bh_k$ with some k, $1 \leq j, k \leq s-1$, $k \neq j$.

Assume that A is the weakly periodic subset $C\langle a\rangle \cup b\{e, a, a^2, \ldots, a^{r-1}\}$, where C is a subset, b an element of G, the union is disjoint and the products are direct. We are done if C is the emptyset or the translated cyclic part is missing. We may assume that this is not the case. Comparing the factorizations $G = AB$ and $G = (Aa)B$ we have that $B = Ba^r$. Consequently either B is periodic or $a^r = e$ in which case A is periodic.

Assume that A is the distorted cyclic subset

$$\{e, a, a^2, \ldots, a^{i-1}, a^i d, a^{i+1}, \ldots, a^{r-1}\}.$$

If $r = 2$ or $d = e$, then A is a cyclic subset and in this case either A or B is periodic. Thus we may assume that $r \geq 3$ and $d \neq e$. From the factorizations $G = AB$ and $G = (Aa)B$ it follows that the sets

$$B, Ba, Ba^2, \ldots, Ba^{i-1}, Ba^i d, Ba^{i+1}, \ldots, Ba^{r-1} \tag{4}$$

and

$$Ba, Ba^2, \ldots, Ba^i, Ba^{i+1} d, Ba^{i+2}, \ldots, Ba^r \tag{5}$$

form partitions of G. First we settle the special case when $i = r-1$. If $x \in Ba^{r-1}d \cap Ba^r d$, then $xa^{-2}d^{-1} \in Ba^{r-3} \cap Ba^{r-2}$ which violates (4). Hence $Ba^{r-1}d \cap Ba^r d = \emptyset$. If $x \in Ba^i \cap Ba^r d$, then $xa^{-1} \in Ba^{i-1}d \cap Ba^{r-1}d$ which violates (4). Hence $Ba^i \cap Ba^r d = \emptyset$ for each i, $1 \leq i \leq r-2$. Consequently $Ba^r d = B$. This implies that either B is periodic or $a^r d = e$. We are done if B is periodic so we may assume that $a^r d = e$. By (5), $Ba^i \cap Ba^{r-1} = \emptyset$ for each i, $0 \le i \le r-2$. Consequently $Ba^{r-1} = Ba^{r-1}d$. Thus either B is periodic or $d = e$. As $d \ne e$ we are left with the possibility that B is periodic.

Next we prove the special case when $r = 3$. Now $A = \{e, ad, a^2\}$ or $A = \{e, a, a^2 d\}$. The second case has already been settled. In the first case A can be written in the form $A = \{e, a^2, a^4 d'\}$ which again reduces the problem to the previously settled case. Thus $r \ge 4$ and $1 \le i \le r-2$ may be assumed for the remaining cases. We distinguish two subcases depending on $i = 1$ or $i \ne 1$. Consider first the $i \ne 1$ case. A comparison of (4) and (5) gives that

$$B \cup a^i dB \cup a^{i+1}B = a^i B \cup a^{i+1} dB \cup a^r B.$$

We claim that in this equation $a^i B = a^i dB$ and so d is a period of B. In order to verify this claim note that by (4) $aB \cap a^{i+1}B = \emptyset$ and so $B \cap a^i B = \emptyset$. As $r \ge 4$ again by (4), there is a j, $0 \le j \le r-2$ for which $a^j B \cap a^{j+1}B = \emptyset$ and so $a^i B \cap a^{i+1}B = \emptyset$. This proves the claim that $a^i B = a^i dB$. Finally consider the $i = 1$ case. From the factorization $G = AB$ we get that $G = A^{-1}B$ is also a factorization of G, where $\{e, a^{-1}d^{-1}, a^{-1}, \dots, a^{-(r-1)}\}$. A multiplication by a^{r-1} yields the factorization $G = (a^{r-1}A^{-1})B$. Here $(a^{r-1}A^{-1})$ is a distorted cyclic subset with $i = r-2 \ge 2$ since $r \ge 4$. This reduces the problem to the $i \ne 1$ case.

Assume that A is a distorted periodic subset such that D is the associated periodic subset with period a, that is, $A = \{c\} \cup \big(D \setminus \{d\}\big)$, where $d \in D$ and $c \in G$. If $c \in D \setminus \{d\}$, then A is quasi periodic. Since this case has already been covered, we assume that $c \notin D \setminus \{d\}$. From the factorizations $G = AB$ and $G = (Aa)B$ it follows that $dB \cup acB = adB \cup cB$. If $dB \cap adB \ne \emptyset$, then $B \cap aB \ne \emptyset$ which is a contradiction. If $acB \cap cB \ne \emptyset$, then again $aB \cap B \ne \emptyset$. Thus $dB = cB$. Now either B is periodic or $d = c$ in which case $A = D$, that is, A is periodic.

This completes the proof.

3. Replaceable factors

If A and A' are subsets of G such that for every subset B of G, if $G = AB$ is a factorization of G, then $G = A'B$ is also a factorization of G, then we shall say that A is *replaceable* by A'.

By the fundamental theorem of the finite abelian groups each finite abelian group is a direct product of cyclic groups of prime power orders. If G is the direct product of cyclic groups of the prime power orders $q_1, \dots, q_s$, then we say that G is of *type* $(q_1, \dots, q_s)$.

Lemma 2. *Let G be a finite abelian group whose 2-component is cyclic and let H be a subgroup of G such that $H \ne \{e\}$ and $H \ne G$. Then there are nonsubgroup subsets $A_1, \dots, A_s$ of G such that $G = HA_1 \cdots A_s$ is a factorization of G, each $|A_i|$ is a prime and each A_i is either cyclic or simulated.*

Proof. Set $L_0 = H$ and $L_s = G$ and consider the chain of subgroups

$$L_0 \subset L_1 \subset \cdots \subset L_s,$$

where $|L_i : L_{i-1}| = p_i$ is a prime for each i, $1 \leq i \leq s$. It is sufficient to construct a nonsubgroup complete set of representatives A_i in L_i modulo L_{i-1} for each i, $1 \leq i \leq s$. As $|L_i/L_{i-1}| = p_i$, the order of each element in $L_i \setminus L_{i-1}$ is divisible by p_i. If there is an $a_i \in L_i \setminus L_{i-1}$ for which $a_i^{p_i} \neq e$, then the subset

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

is a complete set of representatives in L_i modulo L_{i-1} and clearly A_i is not a subgroup of G. Thus we may assume that each element in $L_i \setminus L_{i-1}$ is of order p_i. Since $L_i = \langle L_i \setminus L_{i-1} \rangle$, L_i is of type $(p_i, \ldots, p_i)$. Note that L_i is not cyclic since $|L_i| = |L_{i-1}| \cdot |H|$ and $i \geq 1$. As the 2-component of G is cyclic, $p_i = 2$ is not possible. Then choosing an $a_i \in L_i \setminus L_{i-1}$ and a $b_i \in L_{i-1} \setminus \{e\}$ the subset

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

is a complete set of representatives in L_i modulo L_{i-1} and A_i is not a subgroup of G.

This completes the proof.

Let G be a finite abelian group and let A be a subset of G. If g and h are periods of A, then gh is also a period of A whenever $gh \neq e$. All the periods of A together with the identity element form a subgroup H. In fact A is a union of certain cosets modulo H. Thus there is a subset X of G such that $A = XH$ is a factorization.

Lemma 3. *Let $G = AB$ be a normed factorization of the finite abelian group G, where the 2-component of G is cyclic, A is not periodic and possesses the P property. Then A can be replaced by a product of nonsubgroup subsets of prime cardinality such that each factor is either cyclic or simulated.*

Proof. As A has the P property either A or B is periodic. By the hypotheses of the lemma, B is periodic. Hence there is a normed subset Y and a subgroup H of G for which $B = YH$ is a factorization. We assume that H is the maximal possible with this property. If $|Y| = 1$, then $B = H$. By Lemma 2, A can be replaced by a product of nonsubgroup factors of prime cardinality that are either cyclic or simulated.

Assume that $|Y| \geq 2$ and use an induction on $|Y|$. From the factorization $G = AYH$ we get the factorization

$$G/H = (AH)/H \cdot (YH)/H$$

of the factor group G/H. By the P property of $(AH)/H$, either $(AH)/H$ or $(YH)/H$ is periodic. But $(YH)/H$ cannot be periodic by the maximality of H. Hence $(AH)/H$ is periodic. There are normed subsets K and X of G such that $(KH)/H$ is a subgroup of G/H and

$$(AH)/H = (XH)/H \cdot (KH)/H$$

is a factorization. Now $L = KH$ is a subgroup of G. We choose L to be the largest with this property. We also have the factorization

$$G/L = (XL)/L \cdot (YL)/L$$

of the factor group G/L. Here $(XL)/L$ possesses the P property and it is not periodic because of the maximality of L. By Lemma 2, there are nonsubgroup subsets $A_1, \dots, A_s$ of G such that $L = HA_1 \cdots A_s$ is a factorization of L, each $|A_i|$ is a prime and each A_i is either cyclic or simulated. By the inductive assumption there are subsets $D_1, \dots, D_r$ of G such that

$$G/L = (D_1L)/L \cdots (D_rL)/L \cdot (YL)/L$$

is a factorization of G/L. Here each $(D_iL)/L$ consists of a prime number of cosets of L and each of them is either a cyclic or a simulated subset of G/L. Replace the simulated ones by their associated subgroups. As $(D_iL)/L$ consists of a prime number of cosets of L, after the replacements each $(D_iL)/L$ is a cyclic subset of G/L. There are cyclic subsets $C_1, \dots, C_r$ of G such that

$$G/L = (C_1L)/L \cdots (C_rL)/L \cdot (YL)/L \tag{6}$$

is a factorization of G/L. We show that

$$\begin{aligned} G &= C_1 \cdots C_r Y L \\ &= C_1 \cdots C_r Y H A_1 \cdots A_s \\ &= A_1 \cdots A_s C_1 \cdots C_r B \end{aligned}$$

are factorizations of G. In order to verify this claim consider the equation

$$a_1 \cdots a_s c_1 \cdots c_r y h = a'_1 \cdots a'_s c'_1 \cdots c'_r y' h',$$

where $a_i, a'_i \in A_i$, $c_i, c'_i \in C_i$, $y, y' \in B$, $h, h' \in H$. From the factorization (6) it follows that $c_1 = c'_1, \dots, c_r = c'_r$ and $y = y'$. Using this we get $a_1 \cdots a_s h = a'_1 \cdots a'_s y' h'$. Now since $L = A_1 \cdots A_s H$ is a factorization it follows that $a_1 = a'_1, \dots, a_s = a'_s$ and $h = h'$.

Let $C_i = \{e, c_i, c_i^2, \dots, c_i^{p_i - 1}\}$. If C_i is not a subgroup of G, then set $S_i = C_i$. If C_i is a subgroup of G, then set

$$S_i = \{e, c_i, c_i^2, \dots, c_i^{p_i-2}, c_i^{p_i-1} l\}, \tag{7}$$

where $l \in L \setminus \{e\}$. Note that

$$\begin{aligned} G &= S_1 \cdots S_r Y L \\ &= S_1 \cdots S_r Y H A_1 \cdots A_s \\ &= A_1 \cdots A_s S_1 \cdots S_r B \end{aligned}$$

are factorizations of G. Clearly (7) is a nonsubgroup simulated subset of G if $p_i \geq 3$. If $p_i = 2$ and S_i is a subgroup of G, then $|c_i l| = 2$. Since the 2-component of G is cyclic G has only one element of order 2. Hence from the factorization $G = S_1 \cdots S_r Y L$ it follows that $|L|$ cannot be even. Therefore (7) is a nonsubgroup simulated subset of G.

This completes the proof.

4. The result

Now we come to the proof of the main result of the paper.

Theorem 1. *Let G be a finite abelian group whose 2-component is cyclic. If $G = A_1 \cdots A_n$ is a factorization of G, where each A_i possesses the P property, then at least one of the factors must be periodic.*

Proof. Assume the contrary that none of the factors is periodic. Set $A = A_1$ and $B = A_2 \cdots A_n$. Now Lemma 3 is applicable to the factorization $G = AB$ and gives that A_1 can be replaced by a product of nonsubgroup factors of prime cardinality each of which is either cyclic or simulated. Similarly, A_2 can be replaced by a product of nonsubgroup factors of prime cardinality each of which is either cyclic or simulated. Continuing in this way finally we get a factorization $G = B_1 \cdots B_m$, where each $|B_i|$ is a prime and each B_i is either cyclic or simulated and none of the factors is a subgroup of G. By Theorem 2 of [1], it is not possible. This completes the proof.

This work was supported in part by the Hungarian Research Fund Grant number 7441.

References

[1] Corrádi, K.; Sands, A. D.; Szabó, S.: *Simulated factorizations.* J. Algebra **151** (1992), 12–25.

[2] Fuchs, L.: *Abelian groups.* Akadémiai Kiadó, Budapest 1966.

[3] Hajós, G.: *Über einfache und mehrfache Bedeckung des n-dimensionalen Raumes mit einem Würfelgitter.* Math. Zeitschr. **47** (1941), 427–467.

Received June 1, 1996