Mathematica Pannonica
5/2 (1994), 275 – 280

A HAJÓS-TYPE RESULT ON FACTORING FINITE ABELIAN GROUPS BY SUBSETS

Keresztély **Corrádi**

Department of Computer Sciences, Eötvös University Budapest, H–1088 Budapest, Múzeum krt. 6–8, Hungary

Sándor **Szabó**

Department of Mathematics, University of Bahrain, P. O. Box 32038 Isa Town, State of Bahrain

Received July 1994

AMS Subject Classification: 20 K 01, 52 C 22

Keywords: Factorization of finite abelian groups, Hajós–Rédei theory

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. The main result of the paper is an analogous result. Namely, that the same conclusion holds for finite abelian groups of odd order with certain more general type of factors. The proofs mainly rely on characters of finite abelian groups.

1. Introduction

Throughout the paper the word group is used to mean finite abelian group. The groups are written multiplicatively with identity element e. We need the concept of factoring subsets into subsets. Let G be a finite abelian group. If $B, A_1, \ldots, A_n$ are subsets of G such that each b in B is uniquely expressible in the form

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

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

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 if $A_1 \cdots A_n = B$ 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 $\{e, a, a^2, \ldots, a^{r-1}\}$ where a is an element of $G \setminus \{e\}$ and r is a positive integer. We denote this subset of G shortly by $[a, r]$. Loosely speaking the cyclic subset $[a, r]$ 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.

To settle a famous geometric conjecture of H. Minkowski G. Hajós [2] 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.* In order to generalize Hajós' theorem we can try to extend the family of subsets that occur in a factorization of a given finite abelian group. Of course this extended family should contain the cyclic subsets. Beside cyclic subsets we will consider subsets of form $[a, r] \cup g[a, s]$, where the union is disjoint. We would like to show that if a finite abelian group is factored into the above type of subsets, then at least one of the factors must be a subgroup. We are able to verify this fact in the special case when the order of the finite abelian group is odd. This is the main result of this note. On the other hand the result does not extend to abelian groups of even order as the following example shows. Let G be the direct product of two cyclic groups of order four, say $G = \langle x \rangle \times \langle y \rangle$, where $|x| = |y| = 4$. Choose the subsets A and B to be $A = [x, 2] \cup \cup\, y^2[x, 2]$, $B = [y, 2] \cup x^2 y[y, 2]$. Then as it is easy to verify $G = AB$ is a factorization of G and none of the factors A and B is a subgroup of G.

2. Result

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'. Rédei [3] made use of group characters to study replaceable factors. If A is a subset and χ is a character of G, then $\chi(A)$ denotes the sum

$$\sum_{a \in A} \chi(a).$$

Rédei showed that the factor A can be replaced by A' if $|A| = |A'|$ and if from $\chi(A) = 0$ it follows $\chi(A') = 0$ for each character χ of G. The set of characters χ of G for which $\chi(A) = 0$ we call the *annihilator* of the subset A and it is denoted by $\mathrm{Ann}(A)$. Using this concept Rédei's test reads that if $|A| = |A'|$ and $\mathrm{Ann}(A) \subset \mathrm{Ann}(A')$, then the subset A can be replaced by the subset A'.

Lemma 1. *Let G be a finite abelian group of odd order and let A be a subset of G such that $A = [a, r] \cup g[a, s]$, where the union is disjoint and $r + s$ is odd. Then* $\mathrm{Ann}(A) \subset \mathrm{Ann}\big([a, r + s]\big)$.

Proof. Let $B = [a, r + s]$. First note that $\mathrm{Ann}(B)$ consists of each character χ of G for which $\chi(a) \neq 1$ and $\chi(a^{r+s}) = 1$. Indeed, if $\chi(a) = 1$, then $\chi(B) = r + s$ and if $\chi(a) \neq 1$, then

$$\chi(B) = \frac{1 - \chi(a^{r+s})}{1 - \chi(a)}$$

which proves the claim. Thus it is enough to verify that from $\chi(A) = 0$ it follows that (i) $\chi(a) \neq 1$ and (ii) $\chi(a^{r+s}) = 1$.

To prove (i) assume the contrary that χ is a character of G for which $\chi(A) = 0$ and $\chi(a) = 1$. Now $0 = \chi(A) = r + \chi(g)s$ or equivalently $\chi(g) = -(r/s)$. Taking the absolute values of both sides we have $s = r$. Hence $r + s$ is even which is not the case.

To prove (ii) consider a character χ of G with $\chi(A) = 0$. Now $0 = \chi(A)\chi(a) = \chi(Aa)$. From $\chi(A) = \chi(Aa)$ after cancelling we get $\chi(e) + \chi(g) = \chi(a^r) + \chi(ga^s)$. Drawing complex numbers on the plane the reader can verify easily that as the roots of unity occurring are of odd order $\chi(e)$, $\chi(g)$ is a rearrangement of $\chi(a^r)$, $\chi(ga^s)$. Hence $\chi(e)\chi(g) = \chi(a^r)\chi(ga^s)$, which is equivalent to $1 = \chi(a^{r+s})$. $\Diamond$

If $G = AC$ is a factorization of the finite abelian group G, where $A = [a, r] \cup g[a, s]$, then by Lemma 1 A can be replaced by $B = [a, r+s]$ to get factorization $G = BC$. Now B must contain $r + s$ elements and

so $|a| \geq r+s$. Thus when A is a factor of a factorization then $|a| \geq r+s$ holds. We would like to point out that this is not the case in general. Let $G = \langle x \rangle \times \langle y \rangle$, $|x| = 5$, $|y| = 3$ and $A = [x,3] \cup y[x,4]$. Now $|A| = 7$ and $|x| < 7$.

A subset A of G is called *periodic* if there is an element $g \in G \setminus \{e\}$ such that $Ag = A$. The element g is called a *period* of A.

Lemma 2. *Let G be a finite abelian group of odd order and let A be a subset of G such that $A = [a,r] \cup g[a,s]$, where the union is disjoint and $r+s$ is odd. If A is periodic and $|a| \geq r+s$, then $A = \langle a \rangle$.*

Proof. As $|a| \geq r+s$ so it is enough to prove that (i) $a^{r+s} = e$ and (ii) $g = a^r$.

If $\chi(a^{r+s}) = 1$ for each character χ of G, then $a^{r+s} = 1$. So to prove (i) we consider $\overline{C} = \{\chi : \chi(a^{r+s}) = 1\}$ and we show that $\overline{C}$ in fact coincides with the character group $\overline{G}$ of G. Note that $\overline{C}$ is a subgroup of $\overline{G}$ and $\mathrm{Ann}(A) \subset \overline{C}$. Let x be a period of A. By Th. 1 of [4], $\chi(A) = 0$ whenever $\chi(x) \neq 1$. Counting the number of characters χ of G for which $\chi(x) \neq 1$ we get a lower bound for $\big|\mathrm{Ann}(A)\big|$.

$$\big|\mathrm{Ann}(A)\big| \geq |\overline{G}| - \big|G : \langle x \rangle\big| = |G| - \big|G : \langle x \rangle\big| =$$
$$= |G|\big(1 - (1/|x|)\big) \geq |G|\big(1 - (1/p)\big) > |G|(1/2) = (1/2)|\overline{G}|.$$

Here p is the smallest prime divisor of $|G|$. As $\big|\mathrm{Ann}(A)\big| > (1/2)|\overline{G}|$, $\mathrm{Ann}(A)$ generates $\overline{G}$ and consequently $\overline{C} = \overline{G}$.

To prove $g = a^r$ assume the contrary that $g \neq a^r$. Let χ be a character of G for which $\chi(A) = 0$. Applying χ to $g \neq a^r$ we face to two possibilities, (a) $\chi(g) = \chi(a^r)$ and (b) $\chi(g) \neq \chi(a^r)$. We establish an upper bound for $\big|\mathrm{Ann}(A)\big|$. If $\chi(g) = \chi(a^r)$, then $\chi(ga^{-r}) = 1$ and the number of these characters is $\big|G : \langle ga^{-r} \rangle\big| - 1 \leq |G|/p - 1$ since $\chi(A) = |A| \neq 0$ for the principal character χ of G. Turn to the case when $\chi(g) \neq \chi(a^r)$ and let $B = [a,r] \cup a^r[a,s] = [a, r+s]$. By Lemma 1, from $\chi(A) = 0$ it follows that $\chi(B) = 0$ and so

$$0 = \chi(A) - \chi(B) =$$
$$\chi\big([a,r]\big) + \chi(g)\chi\big([a,s]\big) - \chi\big([a,r]\big) - \chi(a^r)\chi\big([a,s]\big) =$$
$$= \chi\big([a,s]\big)\big(\chi(g) - \chi(a^r)\big).$$

Hence $\chi\big([a,s]\big) = 0$ and consequently $\chi\big([a,r]\big) = 0$. Therefore $\chi(a) \neq 1$, $\chi(a^s) = 1$, $\chi(a^r) = 1$. If t is the greatest common divisor of s and

r, then $\chi(a^t) = 1$. The number of these characters is $|G : \langle a^t \rangle| - 1 \leq$ $\leq |G|/p - 1$. We now combine the lower and upper bounds for $|\mathrm{Ann}(A)|$ together.

$$|G|(1 - (1/p)) \leq |\mathrm{Ann}(A)| \leq |G|/p - 1 + |G|/p - 1 < |G|(2/p).$$

Cancelling $|G|$ we get $1 - (1/p) < (2/p)$ or equivalently $p < 3$ which is not the case. $\Diamond$

Theorem 1. *Let G be a finite abelian group of odd order and $A_1, \ldots, A_n$ be subsets of G such that $A_i = [a_i, r_i] \cup g_i[a_i, s_i]$. If $G = A_1 \cdots A_n$ is a factorization of G, then A_i is a subgroup of G for some i, $1 \leq i \leq n$.*

Proof. For $n = 1$ the theorem holds and so we proceed by induction on n. Replace the factor A_i by $B_i = [a_i, r_i + s_i]$ for each i, $1 \leq i \leq n$ in the factorization $G = A_1 \cdots A_n$ to get the factorization $G = B_1 \cdots B_n$. By Lemma 1 this can be done. From the factorization $G = B_1 \cdots B_n$ by Hajós' theorem it follows that at least one of the factors B_i is a subgroup of G. We may assume that $B_1 = H$ is a subgroup of G since this is only a matter of indexing the factors. In the factorization $G = A_1 A_2 \cdots A_n$ replace A_1 by $B_1 = H$ to get the factorization $G = HA_2 \cdots A_n$. From this we get the factorization $G/H = (A_2H)/H \cdots (A_nH)/H$ of the factor group G/H. By the inductive assumption some of the factors $(A_iH)/H$, say $(A_2H)/H$, is a subgroup of G/H, that is, HA_2 is a subgroup of G. Continuing in this way we have that

$$H,\ HA_2,\ HA_2A_3,\ \ldots,\ HA_2 \cdots A_n$$

are subgroups of G. Let $K = HA_2 \cdots A_{n-1}$. If $g_1 \in K$, then $A_1 \subset K$ and so $K = A_1A_2 \cdots A_{n-1}$ is a factorization of K. By the inductive assumption one of the factors is a subgroup of K and so of G.

In the remaining part of the proof we assume that $g_1 \notin K$. Let $b \in A_n$. From the factorizations $G = A_1A_2 \cdots A_n$ and $G = HA_2 \cdots A_n$ by multiplying with b^{-1} we have that $G = A_1A_2 \cdots A_{n-1}(b^{-1}A_n)$ and $G = HA_2 \cdots A_{n-1}(b^{-1}A_n) = K(b^{-1}A_n)$ are also factorizations of G. As $G = K(b^{-1}A_n)$ is a factorization of G, $b^{-1}A_n$ is a complete set of representatives of G modulo K. There is an element t_b in $b^{-1}A_n$ such that $t_b^{-1}K$ contains g_1. Now $g_1t_b \in K$. Let $C_b = [a_1, r_1] \cup$ $\cup\, [a_1, s_1]g_1t_b$. We claim that $K = C_bA_2 \cdots A_{n-1}$ is a factorization of K. Indeed, products coming from $C_bA_2 \cdots A_{n-1}$ occur among the product coming from $A_1A_2 \cdots A_{n-1}(b^{-1}A_n)$. But these latter ones are

distinct as $G = A_1A_2\cdots A_{n-1}(b^{-1}A_n)$ is a factorization of G. From $K = C_bA_2\cdots A_{n-1}$ by the inductive assumption we have that one of the factors is a subgroup of K. If this is not C_b, then we are done. Thus we suppose that C_b is a subgroup of K. Now C_b is periodic and so by Lemma 2, $C_b = \langle a_1\rangle$. Consequently $g_1t_b = a_1^{r_1}$ or equivalently $t_b = g_1^{-1}a_1^{r_1} \in b^{-1}A_n$. If $t_b = e$ for some $b \in A_n$, then $g_1 = a_1^{r_1}$ and $A_1 = \langle a_1\rangle$. If $t_b \neq e$ for each $b \in A_n$, then

$$e \neq t_b = g_1^{-1}a_1^{r_1} \in \bigcap_{b\in A_n} b^{-1}A_n$$

and so by Lemma 4 of [1], A_n is periodic. Now by Lemma 2, $A_n = \langle a_n\rangle$. $\Diamond$

References

[1] CORRÁDI, K. and SZABÓ, S.: An extension for Hajós' theorem, *Journal of Pure and Appl. Alg.* **79** (1992), 217–223.

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

[3] RÉDEI, L.: Die neue Theorie der endlichen Abelschen Gruppen und Verallgemeinerung des Hauptsatzes von Hajós, *Acta Math. Acad. Sci. Hung.* **16** (1965), 329–373.

[4] SANDS, A. D. and SZABÓ, S.: Factorization of periodic subsets, *Acta Math. Hung.* **57** (1991), 159–167.