# FACTORING AN ODD ABELIAN GROUP BY LACUNARY CYCLIC SUBSETS 

SÁndor Szabó<br>Institute of Mathematics and Informatics<br>University of Pécs<br>Ifjúság u. 6<br>7624 Pécs, Hungary<br>e-mail: sszabo7@hotmail.com


#### Abstract

It is a known result that if a finite abelian group of odd order is a direct product of lacunary cyclic subsets, then at least one of the factors must be a subgroup. The paper gives an elementary proof that does not rely on characters.


Key words and phrases: factorization of finite abelian groups, periodic subsets, cyclic subsets, lacunary cyclic subsets, Hajós-Rédei theory.
2000 Mathematics Subject Classification: Primary 20K01; Secondary 05B45, 52C22, 68R05.

## 1. Introduction

In this paper we will use multiplicative notations in connection with abelian groups. Let $G$ be a finite abelian group. The identity element of $G$ will be denoted by $e$. The order of an element $a$ of $G$ is designated by $|a|$. The number of the elements of a subset $A$ of $G$ is denoted by $|A|$.

Let $A_{1}, \ldots, A_{n}$ be subsets of $G$. If the product $A_{1} \cdots A_{n}$ is direct and is equal to $G$, then we say that the equation $G=A_{1} \cdots A_{n}$ is a factorization of $G$. A subset $A$ of $G$ in the form

$$
A=\left\{e, a, a^{2}, \ldots, a^{r-1}\right\}
$$

is called a cyclic subset of $G$. In order to avoid trivial cases we assume that $r \geq 2$ and that $|a| \geq r$. Clearly $A$ is a subgroup of $G$ if and only if $a^{r}=e$. It is a famous result of G. Hajós [2] that if a finite abelian group is factored as a direct product of its cyclic subsets, then at least one of the factors must be a subgroup.

A subset $A$ of $G$ in the form

$$
\begin{equation*}
A=\left\{e, a, a^{2}, \ldots, a^{r-1}\right\} \cup g\left\{e, a, a^{2}, \ldots, a^{s-1}\right\} \tag{1}
\end{equation*}
$$

is called a lacunary cyclic subset. Here we assume that $|a| \geq r$ since otherwise there would be repetition on the list $e, a, a^{2}, \ldots, a^{r-1}$. From similar reason, we assume that $|a| \geq s$. Further we assume that the subsets

$$
\begin{equation*}
\left\{e, a, a^{2}, \ldots, a^{r-1}\right\} \tag{2}
\end{equation*}
$$

and

$$
\begin{equation*}
g\left\{e, a, a^{2}, \ldots, a^{s-1}\right\} \tag{3}
\end{equation*}
$$

are disjoint. Therefore $A$ has $r+s$ elements. We call the cyclic subset

$$
\begin{equation*}
C=\left\{e, a, a^{2}, \ldots, a^{r+s-1}\right\} \tag{4}
\end{equation*}
$$

a cyclic subset associated with the lacunary cyclic subset $A$ relative to the representation (1). Besides the representation (1) the lacunary cyclic subset $A$ may have another representation as a lacunary cyclic subset, say

$$
A=\left\{e, x, x^{2}, \ldots, x^{\alpha-1}\right\} \cup y\left\{e, x, x^{2}, \ldots, x^{\beta-1}\right\} .
$$

We leave the problem of possibility of various representations unresolved. This is why the definition of the cyclic subset associated with a given lacunary cyclic subset contains a reference to the representation.
K. Corrádi and S. Szabó [1] proved that if a finite abelian group of odd order is factored into lacunary cyclic subsets, then at least one of the factors must be a subgroup. The proof heavily relies on the character techniques developed by L. Rédei [3]. Here we give a character free elementary proof.

In 2008 professor A.D. Sands delivered a lecture at the University of Pécs on factoring finite abelian groups. Absorbing his ideas leads us to an elementary character free proof in the case of lacunary cyclic subsets. A part of the lecture has later appeared in printed form [4].

## 2. Replacement

If from the factorization $G=A B$ it follows that $G=C B$ is also a factorization, then we will say that the factor $A$ in the factorization $G=A B$ can be replaced by $C$.

Lemma 1. Let $G$ be a finite abelian group of odd order and let $A$ be a lacunary cyclic subset of $G$ in form (1). If $G=A B$ is a factorization of $G$, then $G=C B$ is also a factorization of $G$.

Proof. If $s=0$, then $A=C$ and there is nothing to prove. So we may assume that $s \geq 1$.

If $s>r$, then multiply the factorization $G=A B$ by $g^{-1}$. We get the factorization $G=g^{-1} G=\left(g^{-1} A\right) B$. Note that

$$
g^{-1} A=g^{-1}\left\{e, a, a^{2}, \ldots, a^{r-1}\right\} \cup\left\{e, a, a^{2}, \ldots, a^{s-1}\right\}
$$

is again a lacunary cyclic subset. Therefore the roles of $r$ and $s$ can be reversed. Thus we may assume that $s \leq r$.

If $r=s$, then $|A|=2 r$. From the factorization $G=A B$ it follows that $|G|=|A||B|$ which implies that $|G|$ is even. This is not the case. Thus we may assume that $1 \leq s<r$.

The factorization $G=A B$ means that the sets

$$
\begin{equation*}
e B, a B, a^{2} B, \ldots, a^{r-1} B, g e B, g a B, g a^{2} B, \ldots, g a^{s-1} B \tag{5}
\end{equation*}
$$

form a partition of $G$. Multiplying the factorization $G=A B$ by $a$ we get
the factorization $G=a G=(a A) B$ of $G$. This means that the sets

$$
\begin{equation*}
a B, a^{2} B, a^{3} B, \ldots, a^{r} B, g a B, g a^{2} B, g a^{3} B, \ldots, g a^{s} B \tag{6}
\end{equation*}
$$

form a partition of $G$. Comparing the two partitions we get

$$
\begin{equation*}
e B \cup g B=a^{r} B \cup g a^{s} B . \tag{7}
\end{equation*}
$$

If $g B \cap g a^{s} B \neq \emptyset$, then $B \cap a^{s} B \neq \emptyset$ which contradicts the partition (5). Thus $g B \cap g a^{s} B=\emptyset$ and from (7) it follows that $g B=a^{r} B$. Plugging this into (5) we get that the sets

$$
e B, a B, a^{2} B, \ldots, a^{r-1} B, a^{r} B, a^{r+1} B, a^{r+2} B, \ldots, g a^{r+s-1} B
$$

form a partition of $G$. Thus $G=C B$ is a factorization of $G$.
This completes the proof.

## 3. Product of non-periodic subsets

We say that a subset $A$ of $G$ is periodic if there is an element $h \in G \backslash\{e\}$ such that $A h=A$. The element $h$ is called a period of $A$.

To a nonempty subset $A$ of a finite abelian group $G$ we assign the subset $L$ defined by

$$
L=\bigcap_{a \in A} A a^{-1} .
$$

It turns out that $L$ is a subgroup of $G$ and further that the elements of $L \backslash\{e\}$ are all the periods of $A$. We will call $L$ the subgroup of periods of $A$. The next result is Lemma 2.8 of [5].

Lemma 2. Let $A$ be a nonempty subset of a finite abelian group $G$. Let $L$ be the subset assigned to $A$.
(i) If $g \in L$, then $g A=A$.
(ii) If $g A=A$ for some $g \in G$, then $g \in L$.
(iii) $L$ is a subgroup of $G$.
(iv) There is a subset $D$ of $A$ such that the product $D L$ is direct and is equal to $A$.

Under certain conditions the product of non-periodic subsets is again a nonperiodic subset. The result below is Theorem 3.1 of [5].

Lemma 3. Let $G$ be a finite abelian group and let $H$ be a subgroup of $G$. Let $A, B$ subsets of $G$ such that $e \in A, e \in B, A \subset H$. Assume that the product $A B$ is direct, $A, B$ are not periodic and the elements of $B$ are pair-wise incongruent modulo $H$. Then the set $A B$ is not periodic.

## 4. Periodic lacunary cyclic subsets

A periodic cyclic subset must be a subgroup. The next result is part of the folklore. Most likely it goes back to G. Hajós.

Lemma 4. Let $G$ be a finite abelian group and let $A=\left\{e, a, a^{2}, \ldots, a^{r-1}\right\}$ be a cyclic subset of $G$. If $A$ is periodic, then $a^{r}=e$.

Under suitable conditions if a lacunary cyclic subset is periodic, then it must be a subgroup.

Lemma 5. Let $G$ be a finite abelian group of odd order and let $A$ be a lacunary cyclic subset of $G$ in form (1) for which $1 \leq s<r$.
(i) $A$ is a subgroup of $G$ if and only if $g=a^{r}$ and $a^{r+s}=e$.
(ii) $A$ is periodic if and only if $A$ is a subgroup of $G$.

Proof. (i) Suppose that $g=a^{r}$ and $a^{r+s}=e$. From $g=a^{r}$, it follows that $A=C$. Then $a^{r+s}=e$ implies that $C$ is a subgroup of $G$.

Next we assume that $A$ is a subgroup of $G$ and show that $g=a^{r}$ and $a^{r+s}=e$ hold. We claim that $g \in\langle a\rangle$. To prove the claim note that as $s \geq 1$, we have $g \in A$ and hence $g^{2} \in A$. Since the sets (2) and (3) are disjoint, it follows that $g \neq e$. As $|G|$ is odd, the order of $g$ cannot be 2 and so $g^{2} \neq e$.

If $g^{2} \in\left\{e, a, a^{2}, \ldots, a^{r-1}\right\}$, then $g^{2} \in\langle a\rangle$ and then $g \in\langle a\rangle$, as we claimed.

If $g^{2} \in g\left\{e, a, a^{2}, \ldots, a^{s-1}\right\}$, then $g \in\langle a\rangle$, as required.
Now $A \subset\langle a\rangle$ and $\langle a\rangle \subset A$ imply $\langle a\rangle=A$. Using $|A|=r+s$,
we get $a^{r+s}=e$, as required. Further $a^{r+s}=e$ gives $A=C$. From

$$
\begin{aligned}
& \left\{e, a, a^{2}, \ldots, a^{r-1}\right\} \cup g\left\{e, a, a^{2}, \ldots, a^{s-1}\right\} \\
& =\left\{e, a, a^{2}, \ldots, a^{r-1}\right\} \cup\left\{a^{r}, a^{r+1}, a^{r+2}, \ldots, a^{r+s-1}\right\}
\end{aligned}
$$

one can see that

$$
g\left\{e, a, a^{2}, \ldots, a^{s-1}\right\}=\left\{a^{r}, a^{r+1}, a^{r+2}, \ldots, a^{r+s-1}\right\} .
$$

If $a^{r} \in g\left\{a, a^{2}, \ldots, a^{s-1}\right\}$, then it follows that $a^{r}=g a^{i}, 1 \leq i \leq s-1$, then $a^{r-i}=g$ which contradicts that the sets (2) and (3) are disjoint. Hence $a^{r}=g$, as required.
(ii) If $A$ is a subgroup of $G$, then since $A \neq\{e\}, A$ is periodic.

Assume that $A$ is periodic and let $h$ be a period of $A$. We claim that $g \in\langle a\rangle$. In order to prove the claim notice that as $e \in A$, it follows that $h \in A$. Hence either

$$
h \in\left\{e, a, a^{2}, \ldots, a^{r-1}\right\}
$$

or

$$
h \in g\left\{e, a, a^{2}, \ldots, a^{s-1}\right\} .
$$

Let us suppose that $h=g a^{i}$ and distinguish two cases depending on either

$$
g h \in\left\{e, a, a^{2}, \ldots, a^{r-1}\right\}
$$

or

$$
g h \in g\left\{e, a, a^{2}, \ldots, a^{s-1}\right\} .
$$

If $g h=a^{j}$, then $g^{2} \in\langle a\rangle$ and so $g \in\langle a\rangle$, as we claimed. If $g h=g a^{j}$, then $g \in\langle a\rangle$, as required.

Let us turn to the $h=a^{i}$ possibility. If $\left(g a^{j}\right) h \in\left\{e, a, a^{2}, \ldots, a^{r-1}\right\}$ for some $j, 0 \leq j \leq s-1$, then we get $g \in\langle a\rangle$. If $\left(g a^{j}\right) h \in g\left\{e, a, a^{2}, \ldots, a^{s-1}\right\}$ for some $j, 0 \leq j \leq s-1$, then $h$ is a period of $g\left\{e, a, a^{2}, \ldots, a^{s-1}\right\}$. As $\left\{e, a, a^{2}, \ldots, a^{s-1}\right\}$ is periodic, by Lemma 4, it follows that $a^{s}=e$.

Since $s<r$ and $|a| \geq r$ we get a contradiction. Thus $g \in\langle a\rangle$ and so $A \subset\langle a\rangle$.
Let $H$ be the subgroup of periods of $A$. Clearly $A$ is a cyclic subgroup and can be written in the form $H=\left\langle a^{t}\right\rangle$. Let $|H|=k$. As $|G|$ is odd, it follows that $k \geq 3$. If $A=\langle a\rangle$, then $A$ is a subgroup of $G$ and we are done. Thus we may assume that there is an $a^{i}$ such that $a^{i} \notin A$. There is an integer $v$ for which

$$
e, a, a^{2}, \ldots, a^{v-1} \in A
$$

and $a^{v} \notin A, v<t$. Set $D=\left\{e, a, a^{2}, \ldots, a^{v-1}\right\}$ and $E=\left\{a^{v}\right\}$. Note that

$$
D, D a^{t}, D a^{2 t}, \ldots, D a^{(k-1) t}
$$

are subsets of $A$ and

$$
E, E a^{t}, E a^{2 t}, \ldots, E a^{(k-1) t}
$$

are not subsets of $A$. It follows that $A$ has at least $k-1$ gaps. But we know that $A$ has at most one gap.

This completes the proof.

## 5. The result

We are in position now to prove the main result of the paper.
Theorem 1. Let $G$ be a finite abelian group of odd order. If $G=A_{1} \cdots A_{n}$ is a factorization of $G$, where each $A_{i}$ is a lacunary cyclic subset, then at least one of the factors must be a subgroup of $G$.

Proof. In the $n=1$ case $G=A_{1}$ and so $A_{1}$ is a subgroup of $G$. We assume that $n \geq 2$ and start an induction on $n$. We consider a factorization $G=A_{1} \cdots A_{n}$ and show that one of the factors is a subgroup of $G$ using the fact that the result holds for each smaller values of $n$. If one of the factors $A_{1}, \ldots, A_{n}$ is periodic, then, by Lemma 5 , one of the factors is a subgroup of $G$ and we are done. Thus we may assume that none of the factors $A_{1}, \ldots, A_{n}$ is periodic.

In the factorization $G=A_{1} \cdots A_{n}$ replace each factor $A_{i}$ by the associated cyclic subset $C_{i}$ relative to $A_{i}$ to get the factorization $G=C_{1} \cdots C_{n}$. By Hajós's theorem, one of the factors $C_{1}, \ldots, C_{n}$ is a subgroup of $G$.

We may assume that $C_{1}=H_{1}$ is a subgroup of $G$ since this is only a matter of indexing the factors $C_{1}, \ldots, C_{n}$.

In the factorization $G=A_{1} \cdots A_{n}$ replace the factor $A_{1}$ by $C_{1}=H_{1}$ to get the factorization $G=H_{1} A_{2} \cdots A_{n}$. Considering the factor group $G / H_{1}$ we get the factorization

$$
G / H_{1}=\left(A_{2} H_{1}\right) / H_{1} \cdots\left(A_{n} H_{1}\right) / H_{1}
$$

of $G / H_{1}$, where

$$
\left(A_{i} H_{1}\right) / H_{1}=\left\{a_{i} H_{1}: a_{i} \in A_{i}\right\}
$$

Note that $\left(a_{i} H_{1}\right) / H_{1}$ is a lacunary cyclic subset of $G / H_{1}$ and so, by the inductive assumption, it follows that one of the factors

$$
\left(A_{2} H_{1}\right) / H_{1}, \ldots,\left(A_{n} H_{1}\right) / H_{1}
$$

is a subgroup of $G / H_{1}$. We may assume that $\left(A_{2} H_{1}\right) / H_{1}$ is a subgroup of $G / H_{1}$. There is a subgroup $H_{2}$ of $G$ such that $H_{1} A_{2}=H_{2}$. Therefore $G=H_{2} A_{3} \cdots A_{n}$ is a factorization of $G$. Considering the factor group $G / H_{2}$ we get the factorization

$$
G / H_{2}=\left(A_{3} H_{2}\right) / H_{2} \cdots\left(A_{n} H_{2}\right) / H_{2}
$$

of $G / H_{2}$. Continuing in this way finally we have that there are subgroups $H_{1}, H_{2}, \ldots, H_{n}$ of $G$ such that $H_{n}=G$ and

$$
H_{1} A_{2}=H_{2}, H_{2} A_{3}=H_{3}, \ldots, H_{n-1} A_{n}=H_{n} .
$$

The factorization $H_{1} A_{2}=H_{2}$ implies that $A_{2} \subset H_{2}$. The factorization $H_{2} A_{3}=H_{3}$ shows that the elements of $A_{3}$ are incongruent modulo $H_{2}$. Thus Lemma 3 is applicable and provides that the product $A_{2} A_{3}$ cannot be periodic.

The factorization $H_{1}\left(A_{2} A_{3}\right)=H_{3}$ implies that $A_{2} A_{3} \subset H_{2}$. From the factorization $H_{3} A_{4}=H_{4}$ on can see that the elements of $A_{4}$ are incongruent modulo $H_{3}$. By Lemma 3, the product $\left(A_{2} A_{3}\right) A_{4}$ is not periodic. Continuing in this way finally we get that the product $\left(A_{2} \cdots A_{n-1}\right) A_{n}$ is not periodic.

Set $B=A_{2} \cdots A_{n}, A=A_{1}, C=C_{1}$ and suppose that $A, C$ are in forms (1), (4), respectively. Now $G=A B$ is a factorization of $G$. From $C=C_{1}=H_{1}$, by Lemma 5, it follows that $a^{r+s}=e$.

In the way we have seen in the proof of Lemma 1, from the factorization $G=A B$ we can conclude that $a^{r} B=g B$. If $a^{r} g^{-1} \neq e$, then $B$ is periodic. This is not the case so $a^{r}=g$ and consequently, by Lemma $5, A=C$. Therefore $A_{1}$ is equal to $H_{1}$.

This completes the proof.
If a finite abelian group cannot be written as a direct product of lacunary cyclic subsets, then Theorem 1 is vacuously true. The next example shows that there are genuine factorizations of finite abelian groups into lacunary cyclic subsets.

Let

$$
\{e\}=H_{0} \subset H_{1} \subset \cdots \subset H_{n-1} \subset H_{n}=G
$$

be subgroups of a finite abelian group $G$ such that the factor groups

$$
H_{1} / H_{0}, H_{2} / H_{1}, \ldots, H_{n} / H_{n-1}
$$

are cyclic. Let

$$
C_{i}=\left\{e, c_{i}, c_{i}^{2}, \ldots, c_{i}^{r(i)+s(i)-1}\right\}
$$

be a complete set of representatives in $H_{i}$ modulo $H_{i-1}$. Choose an $h_{i} \in$ $H_{i-1}$. Note that

$$
A_{i}=\left\{e, c_{i}, c_{i}^{2}, \ldots, c^{r(i)-1}, h_{i} c_{i}^{r(i)}, \ldots, h_{i} c_{i}^{r(i)+s(i)-1}\right\}
$$

is also a complete set of representatives in $H_{i}$ modulo $H_{i-1}$. It follows that

$$
H_{n}=H_{n-1} A_{n}, H_{n-1}=H_{n-2} A_{n-1}, \ldots, H_{1}=H_{0} A_{1}
$$

are factorizations and so

$$
G=A_{1} A_{2} \cdots A_{n}
$$

is a factorization of $G$. Set $g_{i}=h_{i} c_{i}^{r(i)}$. The representation

$$
A_{i}=\left\{e, c_{i}, c_{i}^{2}, \ldots, c_{i}^{r(i)-1}\right\} \cup g_{i}\left\{e, c_{i}, c_{i}^{2}, \ldots, c_{i}^{s(i)-1}\right\}
$$

makes clear that $A_{i}$ is a lacunary cyclic subset of $G$.

## References

[1] K. Corrádi and S. Szabó, A Hajós type result on factoring finite abelian groups by subsets, Mathematica Pannonica 5 (1994), 275-280.
[2] G. Hajós, Über einfache und mehrfache Bedeckung des n-dimensionalen Raumes mit einem Würfelgitter, Math. Zeit. 47 (1942), 427-467. doi:10.1007/BF01180974
[3] L. Rédei, Die neue Theorie der Endlichen Abelschen Gruppen und Verallgemeinerung des Hauptsatzes von Hajós, Acta Math. Acad. Sci. Hungar. 16 (1965), 329-373. doi:10.1007/BF01904843
[4] A.D. Sands, A note on distorted cyclic subsets, Mathematica Pannonica 20 (2009), 123-127.
[5] S. Szabó and A.D. Sands, Factoring Groups into Subsets, Chapman and Hall, CRC, Taylor and Francis Group, Boca Raton 2009.

Received 20 November 2008
Revised 28 January 2010

