International Electronic Journal of Algebra
Volume 14 (2013) 19-31

DIRECT PRODUCT OF GENERALIZED SIMULATED AND DISTORTED CYCLIC SUBSETS

Sándor Szabó

Received: 06 August 2012; Revised: 30 January 2013
Communicated by Arturo Magidin

Abstract. The paper extends three results on vanishing sums of roots of unity originally developed for studying factorizations of finite abelian groups into subsets. Using these tools we will prove a Hajós type factorization theorem.

Mathematics Subject Classification (2010): Primary 20K01; Secondary 05B45, 52C22, 68R05
Keywords: factorization of finite abelian groups, normalized factorizations, periodic, simulated, cyclic, distorted cyclic, lacunary subset, Hajós' theorem, vanishing sums of root of unity

1. Introduction

Let G be a finite abelian group written multiplicatively with identity element e. Let $A_1, \dots, A_n$ be subsets of G. The product of $A_1, \dots, A_n$ is defined to be the set $\{a_1 \cdots a_n : \ a_1 \in A_1, \dots, a_n \in A_n\}$. The product $A_1 \cdots A_n$ is direct if

$$a_1 \cdots a_n = a_1' \cdots a_n', \ a_1, a_1' \in A_1, \dots, a_n, a_n' \in A_n$$

imply $a_1 = a_1', \dots, a_n = a_n'$. If the product $A_1 \cdots A_n$ is direct and it is equal to G, then we say that G is factored into the subsets $A_1, \dots, A_n$ or that the equation $G = A_1 \cdots A_n$ is a factorization of G. A subset A of G is called normalized if $e \in A$. The factorization $G = A_1 \cdots A_n$ is called normalized if the subset A_i is normalized for each i, $1 \le i \le n$.

A subset C of G is called a cyclic subset if it is in the form

$$C = \{e, a, a^2, \dots, a^{m-1}\}, \tag{1}$$

where $a \in G$ and m is a positive integer that divides $|G|$. We assume that $|a| \ge m$. Let $\alpha(1), \dots, \alpha(k)$ be integers such that

$$1 \le \alpha(1) < \cdots < \alpha(k) \le m - 1$$

and let $d_1, \dots, d_k$ be elements of $G \setminus \{e\}$. A subset A of G in the form

$$A = (C \setminus \{a^{\alpha(1)}, \dots, a^{\alpha(k)}\}) \cup \{a^{\alpha(1)} d_1, \dots, a^{\alpha(k)} d_k\} \tag{2}$$

is called a distorted cyclic subset of degree k. Here we assume that the sets

$$C \setminus \{a^{\alpha(1)}, \dots, a^{\alpha(k)}\},\ \{a^{\alpha(1)}d_1, \dots, a^{\alpha(k)}d_k\}$$

are disjoint. This is equivalent to that $|A| = |C|$.

We introduce the bracket notation for cyclic subsets. The cyclic subset (1) will be denoted shortly by $[a, m]$. Let $g_1, \dots, g_k \in G$ such that $g_1 = e$. The subset A in the form

$$A = g_1[a, m_1] \cup \cdots \cup g_t[a, m_k] \tag{3}$$

is called a lacunary cyclic subset of degree t. Here we assume that $m_i \geq 1$ for each i, $1 \leq i \leq k$ and the sets $g_i[a, m_i]$, $g_j[a, m_j]$ are disjoint for each i, j, $1 \leq i < j \leq k$. This is equivalent to that $|A| = m_1 + \cdots + m_k$.

Let H be a subgroup of G. A subset A of G is called a simulated subset of degree k if $|A| = |H|$ and $|A \setminus H| \leq k$.

2. Roots of unity

In this section we present three results on linear combinations of complex roots of unity with integer coefficients. These extend earlier results that are proved in order to analyze factorizations. The results we prove here have the same motivation. The next lemma generalizes a theorem of [4] on page 361.

Lemma 2.1. *Let $a_1, \dots, a_u$ be positive integers and let $\alpha(1), \dots, \alpha(u)$ be nonnegative integers. Let ρ be a primitive n-th root of unity, where $n \geq 2$. If*

$$0 = \sum_{i=1}^{u} a_i \rho^{\alpha(i)}, \tag{4}$$

then $u \geq p$, where p is the least prime divisor of n.

Proof. Clearly, we may assume that $\alpha(i) \leq n - 1$ for each i, $1 \leq i \leq u$. Since $n \geq 2$, it can be written as a product of prime powers. We will proceed by induction on the number of the distinct prime divisors of n.

We settle first the special case $n = p^e$. With the sum on the right hand side on (4) we associate the

$$P(x) = \sum_{i=1}^{u} a_i x^{\alpha(i)}$$

polynomial. As $P(1) = a_1 + \cdots + a_u$, it follows that $P(x)$ is not the zero polynomial. Further the coefficients of $P(x)$ are integers and $\deg[P(x)] \leq p^e - 1$. We need the (p^e)-th cyclotomic polynomial

$$F(x) = 1 + x^{p^{e-1}} + x^{2p^{e-1}} + \cdots + x^{(p-1)p^{e-1}}. \tag{5}$$

It is known that $F(x)$ is irreducible in the ring of polynomial with rational coefficients. Note that ρ is a common root of $P(x)$ and $F(x)$. From this it follows that

there is a polynomial $Q(x)$ with rational coefficients such that $P(x) = F(x)Q(x)$. This gives the following upper estimate for the degree of $Q(x)$.

$$\begin{aligned} \deg[Q(x)] &= \deg[P(x)] - \deg[F(x)] \\ &\leq (p^e - 1) - (p-1)p^{e-1} \\ &= p^{e-1} - 1. \end{aligned}$$

It follows that the nonzero terms of $Q(x)$ appear among the terms of $P(x)$. Let the coefficient of x^λ be c in $Q(x)$ such that $c \neq 0$. Then the coefficients of

$$x^\lambda, x^{\lambda+p^{e-1}}, x^{\lambda+2p^{e-1}}, \ldots, x^{\lambda+(p-1)p^{e-1}} \tag{6}$$

are all equal to c. Therefore u is a multiple of p and so $u \geq p$, as required.

The number n can be represented in the form $n = p^e r$, where r is relatively prime to p. Since the case $r = 1$ is settled for the remaining part of the proof we may assume that $r \geq 2$. We write ρ in the form $\rho = \sigma\tau$, where σ is a primitive (p^e)-th root of unity and τ is a primitive r-th root of unity. Let us define $\beta(i)$ and $\gamma(i)$ by

$$\alpha(i) \equiv \beta(i) \pmod{p^e}, \ \alpha(i) \equiv \gamma(i) \pmod{r}$$

such that $0 \leq \beta(i) \leq p^e - 1$, $0 \leq \gamma(i) \leq r - 1$ for each i, $1 \leq i \leq u$. Note that

$$\rho^{\alpha(i)} = (\sigma\tau)^{\alpha(i)} = \sigma^{\alpha(i)}\tau^{\alpha(i)} = \sigma^{\beta(i)}\tau^{\gamma(i)}. \tag{7}$$

Let $\delta(1), \ldots, \delta(s)$ be all the distinct elements among $\beta(1), \ldots, \beta(u)$. Let A_i be the set of all j for which $\beta(j) = \delta(i)$. The sets $A_1, \ldots, A_s$ form a partition of $\{1, \ldots, u\}$. Using (7) from (4) we get that

$$0 = \sum_{i=1}^{s} b_i \sigma^{\delta(i)}, \tag{8}$$

where

$$b_i = \sum_{j \in A_i} a_j \tau^{\gamma(j)}.$$

Let q be the least prime divisor of r. Since $n = p^e r$, it follows that $q > p$. Suppose that $b_i = 0$ for some i, $1 \leq i \leq s$. By the induction assumption, it follows that $|A_i| \geq q$. Combining $u \geq |A_i|$ and $|A_i| \geq q$ we get $u \geq |A_i| \geq q > p$, as required.

For the rest of the proof we may assume that $b_i \neq 0$ for each i, $1 \leq i \leq s$. With the linear combination of the roots of unity on the right hand side of (8) we associate the polynomial

$$P(x) = \sum_{i=1}^{s} b_i x^{\delta(i)}.$$

The coefficients of $P(x)$ are from the r-th cyclotomic field and $P(x)$ is not the zero polynomial. It is known that the (p^e)-th cyclotomic polynomial (5) is irreducible over the r-th cyclotomic field. Suppose that the coefficient of x^λ is c in $P(x)$ and

$c \neq 0$. An argument, similar to what we used in the first part of the proof, provides that the coefficients of (6) are all equal to c. In particular it follows that $|A_i| \geq 1$ holds for at least p values of i. This shows that $u = |A_1| + \cdots + |A_s| \geq p$, as required. □

The following lemma is an extension of Theorem 4 of [1].

Lemma 2.2. *Let $n \geq 2$ be an integer and let p be the least prime divisor of n. Let $a_1, \ldots, a_u$, $b_1, \ldots, b_v$ be positive integers and let $\alpha(1), \ldots, \alpha(u)$, $\beta(1), \ldots, \beta(v)$ be distinct nonnegative integers. Let ρ be a primitive n-th root of unity. If*

$$\sum_{i=1}^{u} a_i \rho^{\alpha(i)} = \sum_{j=1}^{v} b_j \rho^{\beta(j)}, \tag{9}$$

then $u \geq p$ or $v \geq p$.

Proof. Let us deal with the case $n = p^e$ first. Consider the polynomial

$$P(x) = \sum_{i=1}^{u} a_i x^{\alpha(i)} - \sum_{j=1}^{v} b_j x^{\beta(j)}. \tag{10}$$

We collected the terms of on the left hand side of the equation (9) and then replaced ρ by x. The coefficients of $P(x)$ are integers and $\deg[P(x)] \leq p^e - 1$. Since no $\alpha(i)$ is equal to $\beta(j)$, there are no like terms in the right hand side of the equation (10).

Let c be the coefficient of x^λ in $P(x)$ such that $c \neq 0$. The argument using the p^e-th cyclotomic polynomial gives that the coefficients of (6) are all equal to c. Note that

$$\sum_{i=0}^{p-1} c\rho^{\lambda + ip^{e-1}} = c\rho^\lambda \sum_{i=0}^{p-1} \rho^{ip^{e-1}} = 0.$$

If $c > 0$, then $\lambda \in \{\alpha(1), \ldots, \alpha(u)\}$. In this case we subtract the sum

$$\sum_{i=0}^{p-1} \rho^{ip^{e-1}} \tag{11}$$

from the left hand side of (9). We still will have equal linear combinations of roots of unity. But the quantity $a_1 + \cdots + a_u + b_1 + \cdots + b_v$ decreases. If $c < 0$, then $\lambda \in \{\beta(1), \ldots, \beta(v)\}$. In this case we subtract (11) from the right hand side of (9). We get new equal linear combinations of roots of unity with a smaller value of $a_1 + \cdots + a_u + b_1 + \cdots + b_v$. Continuing in this way finally we get that

$$\sum_{i=1}^{u} a_i \rho^{\alpha(i)} = 0 \text{ and } \sum_{j=1}^{v} b_j \rho^{\beta(j)} = 0.$$

Lemma 2.1 is applicable and gives that $u \geq p$ and $v \geq p$.

Next we assume that n has at least two distinct prime divisors and proceed by induction on the number of the distinct prime divisors of n. We write n in the form

$n = q^f r$, where q is the largest prime divisor of n and r is not a multiple of q. We write ρ in the form $\rho = \sigma\tau$, where σ is a primitive q-th root of unity and τ is a primitive r-th root of unity. We simply set $\sigma = \rho^r$, $\tau = \rho^{q^f}$. We define the numbers $\gamma(i)$, $\delta(i)$, $\varepsilon(j)$, $\mu(j)$ by

$$\alpha(i) \equiv \gamma(i) \pmod{q^f},\ \alpha(i) \equiv \delta(i) \pmod{r},$$

$$\beta(j) \equiv \varepsilon(j) \pmod{q^f},\ \beta(j) \equiv \mu(j) \pmod{r},$$

where

$$0 \le \gamma(i), \varepsilon(j) \le q^f - 1,\ 0 \le \delta(i), \mu(j) \le r - 1.$$

Clearly,

$$\rho^{\alpha(i)} = (\sigma\tau)^{\alpha(i)} = \sigma^{\alpha(i)}\tau^{\alpha(i)} = \sigma^{\gamma(i)}\tau^{\delta(i)},$$
$$\rho^{\beta(j)} = (\sigma\tau)^{\beta(j)} = \sigma^{\beta(j)}\tau^{\beta(j)} = \sigma^{\varepsilon(j)}\tau^{\mu(j)},$$

and so

$$\begin{aligned} 0 &= \sum_{i=1}^{u} a_i \rho^{\alpha(i)} - \sum_{j=1}^{v} b_j \rho^{\beta(j)} \\ &= \sum_{i=1}^{u} a_i \sigma^{\gamma(i)}\tau^{\delta(i)} - \sum_{j=1}^{v} b_j \sigma^{\varepsilon(j)}\tau^{\mu(j)}. \end{aligned}$$

Let $\nu(1), \ldots, \nu(w)$ be all the distinct numbers among $\gamma(1), \ldots, \gamma(u)$, $\varepsilon(1), \ldots, \varepsilon(v)$. Let A_i be the set of all j for which $\nu(i) = \gamma(j)$. Obviously, the sets $A_1, \ldots, A_w$ form a partition of $\{1, \ldots, u\}$. Let B_i be the set of all j for which $\nu(i) = \varepsilon(j)$. The sets $B_1, \ldots, B_w$ form a partition of $\{1, \ldots, v\}$. Using these notations from (9) we have

$$0 = \sum_{i=1}^{w} c_i \sigma^{\nu(i)}, \tag{12}$$

where

$$c_i = \sum_{j \in A_i} a_j \tau^{\delta(j)} - \sum_{j \in B_i} b_j \tau^{\mu(j)}.$$

Consider the polynomial

$$P(x) = \sum_{i=1}^{w} c_i x^{\nu(i)}.$$

We constructed $P(x)$ from the right hand side of the equation (12). Namely, on the right hand side of (12) we replaced σ by x. The coefficients of $P(x)$ are from the r-th cyclotomic field and $\deg[P(x)] \le q^f - 1$.

We assume that $c_i = 0$ and in connection with c_i we distinguish the following three cases.

(i) $A_i = \emptyset$,
(ii) $B_i = \emptyset$,
(iii) $A_i \neq \emptyset$ and $B_i \neq \emptyset$.

If (i) holds, then from

$$0 = \sum_{j \in B_i} b_j \tau^{\mu(j)},$$

by Lemma 2.1, it follows that $|B_i| \geq p$. Combining $v \geq |B_i|$ and $|B_i| \geq p$ we get $v \geq p$, as required. If (ii) holds, then a similar argument gives that $u \geq |A_i| \geq p$, as required.

If (iii) holds, then

$$\sum_{j \in A_i} a_j \tau^{\delta(j)} = \sum_{j \in B_i} b_j \tau^{\mu(j)}. \tag{13}$$

We claim that no $\delta(k)$ is equal to $\mu(l)$ in this equation. In order to verify the claim assume on the contrary that $\delta(k) = \mu(l)$. Now $\sigma^{\nu(i)}\tau^{\delta(k)} = \sigma^{\nu(i)}\tau^{\mu(l)}$. From $k \in A_i$, it follows that $\nu(i) = \gamma(k)$. From $l \in B_i$, it follows that $\nu(i) = \varepsilon(l)$. The computation

$$\begin{aligned} \rho^{\alpha(k)} &= (\sigma\tau)^{\alpha(k)} = \sigma^{\alpha(k)}\tau^{\alpha(k)} \\ &= \sigma^{\gamma(k)}\tau^{\delta(k)} = \sigma^{\nu(i)}\tau^{\delta(k)} \\ &= \sigma^{\nu(i)}\tau^{\mu(l)} = \sigma^{\varepsilon(l)}\tau^{\mu(l)} \\ &= \sigma^{\beta(l)}\tau^{\beta(l)} = (\sigma\tau)^{\beta(l)} = \rho^{\beta(l)} \end{aligned}$$

leads to the $\rho^{\alpha(k)} = \rho^{\beta(l)}$ contradiction. Thus no $\delta(k)$ is equal to $\mu(l)$ in (13).

From (13), by the inductive assumption, it follows that $|A_i| \geq p$ or $|B_i| \geq p$. Therefore $u \geq |A_i| \geq p$ or $v \geq |B_i| \geq p$, as required.

For the rest of the proof we may assume that $c_i \neq 0$ for each i, $1 \leq i \leq w$. In particular, the polynomial $P(x)$ is not the zero polynomial. Let c be the coefficient of x^λ in $P(x)$ such that $c \neq 0$. The argument using the q^f-th cyclotomic polynomial gives that the coefficients of

$$x^\lambda, x^{\lambda+q^{f-1}}, x^{\lambda+2q^{f-1}}, \ldots, x^{\lambda+(q-1)q^{f-1}}$$

are all equal to c. Let $d_j \in \{c_1, \ldots, c_w\}$ be these coefficients, where $0 \leq j \leq q-1$. For the sake of definiteness for a moment suppose $d_j = c_1$. Note that since $c \neq 0$, it follows that $A_1 \cup B_1 \neq \emptyset$ and consequently exactly one of (i), (ii), (iii) holds in connection with d_j.

Suppose that (i) holds for d_0 and d_1. Further suppose that $d_0 = c_k$ and $d_1 = c_l$. The equation $d_0 = d_1$ gives that $c_k = c_l$, that is,

$$\sum_{j \in B_k} b_j \tau^{\mu(j)} = \sum_{j \in B_l} b_j \tau^{\mu(j)}.$$

As before we can verify that no equal roots of unity appear on both sides of the equation. The inductive assumption gives that $|B_k| \geq p$ or $|B_l| \geq p$. Therefore $v \geq |B_k| \geq p$ or $u \geq |B_l| \geq p$, as required. We may assume that (i) hold in connection with at most one d_j. An analogous argument shows that we may assume that (ii) holds in connection with at most one d_j.

Suppose that (iii) holds for d_j for each j, $0 \le j \le q-1$. This guarantees that $|A_i| \ge 1$ for at least q values of i. Using this we get $u = |A_1| + \cdots + |A_w| \ge q > p$, as required. (As a matter of fact $|B_i| \ge 1$ also holds for at least q values of i. Consequently $v = |B_1| + \cdots + |B_w| \ge q > p$, as required.)

If (i) or (iii) holds for d_j for each j, $0 \le j \le q-1$, then $v = |B_1| + \cdots + |B_w| \ge q > p$, as required. Similarly, if (ii) or (iii) holds for d_j for each j, $0 \le j \le q-1$, then $u = |A_1| + \cdots + |A_w| \ge q > p$, as required. We are left with the following situation. Case (i) holds for exactly once for d_j. Case (ii) holds for exactly once for d_j. Further case (iii) holds for exactly $q-2$ times for d_j.

Since n has at least two distinct prime divisors, it follows that $q \ge 3$ and $q-1 \ge p$. Now $|B_i| \ge 1$ holds for exactly $q-1$ values of i. From this we get $v = |B_1| + \cdots + |B_w| \ge q-1 \ge p$, as required. Of course because of symmetry we could draw the $v \ge p$ conclusion too. □

The next result is a generalization of Theorem 4 of [6].

Lemma 2.3. *Let $n \ge 2$ be an integer and let ρ be a primitive n-th root of unity. Suppose that $a_1, \ldots, a_u$ are positive integers and $\alpha(1), \ldots, \alpha(u)$ are distinct non-negative integers less than n. If $1 \le u \le 2p-1$, where p is the least prime divisor of n, then*

$$0 = \sum_{i=1}^{u} a_i \rho^{\alpha(i)} \tag{14}$$

implies that u divides n.

Proof. In the $n = p^e$ case the argument we have seen in the proof of Lemma 2.1 gives that u is a multiple of p. Then from $1 \le u \le 2p-1$ we get $u = p$ and so u divides n, as required.

For the remaining part of the proof we assume that $n = p^e r$, where p does not divide r. Let q be the least prime divisor of r. Clearly $q > p$. We write ρ in the form $\rho = \sigma\tau$, where σ is a primitive p^e-th root of unity and τ is a primitive r-th root of unity. Let us define the numbers $\beta(i)$, $\gamma(i)$ by

$$\alpha(i) \equiv \beta(i) \pmod{p^e}, \ \alpha(i) \equiv \gamma(i) \pmod{r}$$

such that

$$0 \le \beta(i) \le p^e - 1, \ 0 \le \gamma(i) \le r-1$$

for each i, $1 \le i \le u$. Clearly

$$\rho^{\alpha(i)} = (\sigma\tau)^{\alpha(i)} = \sigma^{\alpha(i)}\tau^{\alpha(i)} = \sigma^{\beta(i)}\tau^{\gamma(i)}.$$

Using this equation (14) can be written in the form

$$0 = \sum_{i=1}^{u} a_i \sigma^{\beta(i)} \tau^{\gamma(i)}. \tag{15}$$

Let $\delta(1),\dots,\delta(v)$ be all the distinct numbers among $\beta(1),\dots,\beta(u)$. Let A_i be the set of all j for which $\delta(i)=\beta(j)$. Obviously, the sets $A_1,\dots,A_v$ form a partition of $\{1,\dots,u\}$. Set $t_i=|A_i|$. Now the equation (15) can be represented in the form

$$0=\sum_{i=1}^{v} b_i\sigma^{\delta(i)}, \tag{16}$$

where

$$b_i=\sum_{j\in A_i} a_j\tau^{\gamma(j)}.$$

If $b_i=0$ for each i, $1\le i\le v$, then by Lemma 2.1, $t_i\ge q$ for each i, $1\le i\le v$. From $vq\le t_1+\cdots+t_v=u\le 2p-1<2q-1$, it follows that $v=1$. Then $u=t_1<2q-1$ and so the inductive assumption is applicable to $b_1=0$ implying that $t_1|r$. This means that $u|r$. Then we get $u|p^er$, as required. For the rest of the proof we may assume that $b_i\ne 0$ for some i, $1\le i\le v$. Let us construct the polynomial

$$P(x)=\sum_{i=1}^{v} b_ix^{\delta(i)}.$$

In the way we have seen in the proof of Lemma 2.1 we get that the p^e-th cyclotomic polynomial divides $P(x)$ over the r-th cyclotomic field. Let c be the coefficient of x^λ in $P(x)$ such that $c\ne 0$. It follows that the coefficients of (6) are all equal to c. Let us consider the polynomial

$$Q(x)=P(x)-cx^\lambda F(x),$$

where $F(x)$ is the p^e-th cyclotomic polynomial. Note that $F(x)$ divides $Q(x)$ over the r-th cyclotomic field. The number of the nonzero monomials in $Q(x)$ decreased by p. If $Q(x)$ is not the zero polynomial, then we can repeat this step. Continuing in this way finally we can conclude that the number of the nonzero monomials in $P(x)$ is a multiple of p, that is $p|v$. In particular $p\le v$.

From $p\le v\le u\le 2p-1$, it follows that $v=p$ and therefore

$$P(x)=\sum_{i=1}^{p} b_ix^{\delta(i)}.$$

This implies $b_1=\cdots=b_p$. The inequality $t_1+\cdots+t_p=u\le 2p-1$ together with $t_1\ge 1,\dots,t_p\ge 1$ gives that $1\le t_i\le p$ for each i, $1\le i\le p$.

Suppose that in the equation $b_i=b_j$ not all the roots of unity cancel out for some i, j, $1\le i<j\le p$. Now Lemma 2.2, leads to the contradiction that $t_i\ge q>p$ or $t_j\ge q>p$. Thus in the equation $b_i=b_j$ exactly the same roots of unity appear on the left hand side and on the right hand side for each i, j, $1\le i<j\le p$. Consequently $t_1=\cdots=t_p$. Let t be this common value. This means that $pt=u\le 2p-1$. From this it follows that $t=1$ and then $u=p$. Now plainly u divides $n=p^er$, as required. □

3. Replacement

Let $G = AB$ be a factorization of the finite abelian group G. We say that the factor A can be replaced by the factor A' if $G = A'B$ is also a factorization of G. In [4] L. Rédei developed a test for replacement using characters of G. Let χ be a character of G. The sum of complex numbers

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

is denoted by $\chi(A)$. The set of characters χ of G for which $\chi(A) = 0$ is called the annihilator set of A and is denoted by $\mathrm{Ann}(A)$. Rédei's test now reads as follows. If $|A| = |A'|$ and $\mathrm{Ann}(A) \subseteq \mathrm{Ann}(A')$, then A can be replaced by A'.

The next lemma essentially means that the distorted cyclic subset (2) can be replaced by the cyclic subset $[a, m]$.

Lemma 3.1. *Let G be a finite abelian group and let A be a distorted cyclic subset of G of degree k. Let χ be a character of G such that $\chi(A) = 0$. If $2k+1$ is smaller than the least prime divisor of $|G|$, then $\chi(a) \neq 1$ and $\chi(a^m) = 1$.*

Proof. First we show that $\chi(A) = 0$ implies $\chi(a) \neq 1$. In order to prove the claim assume on the contrary that $\chi(a) = 1$. Let us compute $\chi(A)$.

$$\begin{aligned}\chi(A) &= \sum_{i=0}^{m-1} \chi(a^i) - \sum_{i=1}^{k} \chi(a^{\alpha(i)}) + \sum_{i=1}^{k} \chi(a^{\alpha(i)} d_i) \\ &= m - k + \sum_{i=1}^{k} \chi(d_i).\end{aligned}$$

Using $\chi(A) = 0$, we get that

$$m - k = -\sum_{i=1}^{k} \chi(d_i).$$

Taking absolute values on both sides it follows that

$$m - k = \left| \sum_{i=1}^{k} \chi(d_i) \right| \leq \sum_{i=1}^{k} |\chi(d_i)| = k,$$

that is, $m \leq 2k$.

Let p be the least prime divisor of $|G|$. From $m||G|$ it follows that $p|m$ and so $p \leq m$. Combining $p \leq m$ and $m \leq 2k$ we get $p \leq 2k$. This contradicts the $p > 2k + 1$ assumption. Thus $\chi(a) \neq 1$, as we claimed.

Let us consider $\chi(A)$ again and introduce the $\chi(a^i) = \rho^i$, $\chi(d_i) = \sigma_i$ notations.

$$\chi(A) = \sum_{i=0}^{m-1} \rho^i - \sum_{i=1}^{k} \rho^{\alpha(i)} + \sum_{i=1}^{k} \rho^{\alpha(i)} \sigma_i$$

$$= \frac{1-\rho^m}{1-\rho} - \sum_{i=1}^{k} \rho^{\alpha(i)} + \sum_{i=1}^{k} \rho^{\alpha(i)}\sigma_i.$$

Using $\chi(A) = 0$ and multiplying by $1-\rho$ we get

$$\begin{aligned} 0 &= 1 - \rho^m - \sum_{i=1}^{k} \rho^{\alpha(i)} + \sum_{i=1}^{k} \rho^{\alpha(i)}\sigma_i \\ &\quad + \sum_{i=1}^{k} \rho^{\alpha(i)+1} - \sum_{i=1}^{k} \rho^{\alpha(i)+1}\sigma_i. \end{aligned}$$

Then

$$1 + \sum_{i=1}^{k} \rho^{\alpha(i)}\sigma_i + \sum_{i=1}^{k} \rho^{\alpha(i)+1} = \rho^m + \sum_{i=1}^{k} \rho^{\alpha(i)} + \sum_{i=1}^{k} \rho^{\alpha(i)+1}\sigma_i.$$

The left hand side is a sum of $2k+1$ $|G|$-th roots of unity and so is the right hand side. By the assumption of the lemma, the least prime divisor of $|G|$ is greater than $2k+1$. By Sands' result, the sets

$$\{1, \rho^{\alpha(i)}\sigma_i, \rho^{\alpha(i)+1} : \ 1 \le i \le k\}, \ \{\rho^m, \rho^{\alpha(i)}, \rho^{\alpha(i)+1}\sigma_i : \ 1 \le i \le k\}$$

must be equal. The product of the elements in the first set is equal to the product of the elements in the second set. After cancelling we get $\rho^m = 1$, as required. □

Let A be a lacunary cyclic subset in the form (3). Set $m = m_1 + \cdots + m_k$ and $C = [a, m]$. By the next lemma, A can be replaced by C. This lemma is a variant of an earlier results of [7] and [3].

Lemma 3.2. *Let G be a finite abelian group and let A be a lacunary cyclic subset of G in the form (3). Let χ be a character of G such that $\chi(A) = 0$. If t is less than the least prime divisor of $|G|$, then $\chi(a) \neq 1$ and $\chi(a^m) = 1$.*

Proof. First we verify that $\chi(A) = 0$ implies $\chi(a) \neq 1$. In order to do so we assume on the contrary that $\chi(A) = 0$ and $\chi(a) = 1$. Now

$$0 = \chi(A) = \sum_{i=1}^{k} m_i \chi(g_i). \tag{17}$$

If $\chi(g_1) = \cdots = \chi(g_k) = 1$, then we get the $0 = m_1 + \cdots + m_k = m$ contradiction. Thus there is an integer $n \ge 2$ and a primitive n-th root of unity ρ such that $\chi(g_i) = \rho^{\alpha(i)}$ for each i, $1 \le i \le k$. Clearly, n divides $|G|$ and so the least prime divisor of n cannot be smaller than the least prime divisor of $|G|$. Now (17) contradicts the statement of Lemma 2.1.

In order to prove $\chi(a^m) = 1$ let us consider $\chi(A)$ again.

$$\chi(A) = \sum_{i=1}^{k} \chi(g_i) \Big[\sum_{j=0}^{m_i - 1} \chi(a^j) \Big]$$

$$= \sum_{i=1}^{k} \chi(g_i)\left[\frac{1-\chi(a^{m_i})}{1-\chi(a)}\right].$$

Using $\chi(A) = 0$ and multiplying by $1 - \chi(a)$ we get

$$0 = \sum_{i=1}^{k} \chi(g_i)[1 - \chi(a^{m_i})],$$

that is,

$$\sum_{i=1}^{k} \chi(g_i) = \sum_{i=1}^{k} \chi(g_i)\chi(a^{m_i}).$$

By Sands' result, the sets

$$\{\chi(g_i) : \ 1 \le i \le k\}, \ \{\chi(g_i)\chi(a^{m_i}) : \ 1 \le i \le k\}$$

must be equal. Therefore, the product of the elements in the first set is equal to the product of the elements in the second set. After cancellation we get $1 = \chi(a^{m_1}) \cdots \chi(a^{m_k}) = \chi(a^m)$, as required. □

4. A Hajós type result

In Theorem 5 of [5] A. D. Sands has proved the following result. Let G be a finite abelian group such that p is the least prime divisor of $|G|$. If $G = A_1 \cdots A_n$ is a factorization, where A_i is a simulated subset of degree k and $k \le p - 2$, then at least one of the factors is a subgroup of G. In this section we extend this result.

Theorem 4.1. *Let G be a finite abelian group such that p is the least prime divisor of $|G|$. Let $G = A_1 \cdots A_n$ be a normalized factorization of G, where A_i is either a distorted cyclic subset of degree k with $2k + 1 < p$ or a simulated subset of degree k with $k \le p - 2$ for each i, $1 \le i \le n$. Then A_i is a subgroup of G for some i, $1 \le i \le n$.*

Proof. Assume on the contrary that there is a counter-example, that is, there is a normalized factorization $G = A_1 \cdots A_n$ in which none of the factors is a subgroup of G.

Consider first the case when A_i is a simulated subset for each i, $1 \le i \le n$. By Theorem 2 of [2], from the factorization $G = A_1 \cdots A_n$ it follows that A_i is a subgroup of G for some i, $1 \le i \le n$. This is a contradiction. Thus in a counter-example A_i is a distorted cyclic subset for some i, $1 \le i \le n$. Let t be the number of simulated subsets among the factors $A_1, \ldots, A_n$. We choose a counter-example with a maximal t.

A distorted cyclic subset can be a cyclic subset as an extreme case. Next we consider the situation when each distorted cyclic subset is in fact a cyclic subset. Suppose $A_1, \dots, A_s$ are cyclic subsets and $A_{s+1}, \dots, A_n$ are simulated subsets. (None of the factors is a subgroup of G.) Here $s \geq 1$ and $t = n - s$.

Set $A_1 = [a, m]$. If m is not a prime, say $m = uv$, with $u \geq 2$, $v \geq 2$, then $[a, m] = [a, u][a^u, v]$. If the cyclic subset $[a, u]$ is a subgroup of G, then $a^u = e$ and we get $|a| \leq u$. This contradicts $m \leq |a|$. Thus $[a, u]$ cannot be a subgroup of G. If the cyclic subset $[a^u, v]$ is a subgroup of G, then the cyclic subset $[a, m]$ is a subgroup of G. This is not the case. So $[a^u, v]$ is not a subgroup of G. Therefore the cyclic subset A_1 can be written as a product of non-subgroup cyclic subsets each of which has a prime number of elements. Consequently in the factorization $G = A_1 \cdots A_n$ we can replace A_i by a product of non-subgroup cyclic subsets of prime cardinalities for each i, $1 \leq i \leq s$. Let $G = B_1 \cdots B_r$ be the resulting factorization. By Theorem 2 of [2], B_i is a subgroup of G for some i, $1 \leq i \leq n$. This is an outright contradiction.

Summarizing our considerations we may say that in the counter-example $G = A_1 \cdots A_n$, the factor A_i is a non-cyclic distorted cyclic subset for some i, $1 \leq i \leq n$. For the sake of definiteness may assume that A_1 is a non-cyclic distorted cyclic subset. Let $A_1, \dots, A_s$ be non-cyclic distorted cyclic subsets and let $A_{s+1}, \dots, A_n$ be cyclic subsets or simulated subsets. Of course none of the factors is a subgroup of G. It may happen that a non-cyclic distorted cyclic subset is a simulated subset as well. In this case we treat the subset as a simulated subset. We consider the counter-examples in which t is maximal and among these counter-examples we choose one in which s is minimal.

Let C be the cyclic subset associated with A_1. By Lemma 3.1, in the factorization $G = A_1 A_2 \cdots A_n$ the factor A_1 can be replaced by C to get the factorization $G = C A_2 \cdots A_n$. This factorization contains $s-1$ non-cyclic distorted cyclic subsets and the minimality of s gives that at least one of the factors $C, A_2, \dots, A_n$ is a subgroup of G. Only C can be a subgroup of G. This provides that A_1 is a simulated subset. The number of the simulated subsets increased in the counter-example. The maximality of t gives that A_i is a subgroup of G for some i, $1 \leq i \leq n$. This contradiction completes the proof. □

References

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

[2] K. Corrádi, A. D. Sands and S. Szabó, *Factoring by simulated subsets*, J. Algebra, 175 (1995), 320–331.

[3] K. Corrádi and S. Szabó, *A Hajós type result on factoring finite abelian groups by subsets*, Mathematica Pannonica, 5 (1994), 275–280.

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

[5] A. D. Sands, *Simulated factorizations II*, Aequationes Mathematicae, 44 (1992), 48–59.

[6] A. D. Sands, *A note on distorted cyclic subsets*, Mathematica Pannonica, 20 (2009), 123–127.

[7] S. Szabó, *Products of lacunary subsets of a finite abelian group*, Glasnik Matematički, 29 (1994), 235–238.

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