Mathematica Pannonica
16/1 (2005), 79–94

FACTORING A FINITE ABELIAN GROUP BY PRIME COMPLEXES

Keresztély **Corrádi**

Department of General Computer Technics, Eötvös Loránd University, Pázmány P. sétány 1/C, H–1117 Budapest, Hungary

Sándor **Szabó**

Institute of Mathematics and Informatics, University of Pécs, Ifjúság u. 6, H-7624 Pécs, Hungary

Received: September 2004

MSC 2000: 20 K 01, 52 C 22

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

Abstract: If a finite abelian group is a direct product of its subsets such that each subset (a) has a prime number of elements (b) contains the identity element of the group, then at least one of the factors must be a subgroup. This result is due to L. Rédei. The purpose of this paper is to show that Rédei's theorem can be proved using an earlier result of G. Hajós about certain zero divisors. The remaining part presents an extension and an alternative proof of Rédei's theorem.

1. Introduction

Let G be a finite abelian group written multiplicatively with identity element e. If $A_1, \ldots, A_n$ are subsets of G such that the product $A_1 \cdots A_n$ is direct and gives G, then we say that the equation $G = A_1 \cdots A_n$ is a factorization of G. In the most commonly encountered situation G is represented as a direct product of its cyclic subgroups. In this paper it will not be assumed that $A_1, \ldots, A_n$ are subgroups of G. A subset A of G is called cyclic if it is in the form

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

where r is a integer $r \geq 2$ and $|a| \geq r$. In 1942, in order to prove a famous conjecture of H. Minkowski, G. Hajós [2] proved that if a finite abelian group is factored into cyclic subsets, then at least one of the factors must be a subgroup. Hajós's original proof was not elementary in the sense that it used group rings. Rédei [5] found an elementary proof for Hajós's theorem and later he was able to extend his proof for the case when the appearing factors are not necessarily cyclic subsets.

In this paper we will show that the ideas in Hajós's original proof can be extended to prove Rédei's theorem. Although this proof is not elementary it has a fairly transparent structure.

2. Annihilators

Let A be a subset and let χ be a character of the finite abelian group G. We will denote the sum

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

by $\chi(A)$. We are not going use the $\chi(A)$ notation when A is the empty set. Note that $\chi(A) = |A|$ when χ is the principal (or identity) character of G. The set of characters χ of G for which $\chi(A) = 0$ is called the annihilator of A and we will denote it by $\mathrm{Ann}(A)$. For the sake of a concise notation the cyclic set $\{e, a, a^2, \dots, a^{r-1}\}$ will be denoted by $[a, r]$.

Let $g_1, \dots, g_s$ be all the elements of G and let $\chi_1, \dots, \chi_s$ be all the characters of G. By the standard orthogonality relations the matrix $[\chi_i(g_j)]$ is orthogonal. In particular the columns of the matrix are linearly independent. This gives that if $A, B \subset G$ such that $\chi(A) = \chi(B)$ holds for each character χ of G, then $A = B$.

Consider a factorization $G = AB$ of G. Applying a character χ of G to this factorization gives that $\chi(G) = \chi(AB) = \chi(A)\chi(B)$. For the principal character this equation reduces to $|G| = |A||B|$. For the nonprincipal characters we get $0 = \chi(A)\chi(B)$. Conversely, if $|G| = |A||B|$ and $0 = \chi(A)\chi(B)$ holds for each nonprincipal character χ of G, then $G = AB$ is a factorization of G. Further, if $G = AB$ is a factorization of G and $|A| = |A'|$, $\mathrm{Ann}(A) \subset \mathrm{Ann}(A')$ hold, then $G = A'B$ is a factorization of G. In other words in the factorization $G = AB$ the factor A can be replaced by the subset A'.

We will use the following well known facts.

(i) The (n)th cyclotomic polynomial is irreducible over the (m)th cyclotomic field provided m and n are relatively prime.

(ii) Let n be an integer greater than one and let p be the smallest prime factor of n. Then less than p (n)th roots of unity are linearly independent over the field of rationals. (For a proof see [9].)

Lemma 1. *If $A \subset G$ with $e \in A$ and $|A| = p$ is the smallest prime factor of $|G|$, then $\chi(a_{|p'}) = 1$ for each $\chi \in \mathrm{Ann}(A)$ and $a \in A$.*

Proof. Let $A = \{a_0, a_1, \ldots, a_{p-1}\}$, where $a_0 = e$. Pick a character χ from $\mathrm{Ann}(A)$. Now

$$0 = \chi(A) = \sum_{i=0}^{p-1} \chi(a_i) = \sum_{i=0}^{p-1} \chi(a_{i|p})\chi(a_{i|p'}).$$

There exists a minimal nonnegative integer n such that each $\chi(a_{i|p})$ is a power of the same primitive (p^n)th root of unity, say ρ. If $n = 0$, then

$$0 = \sum_{i=0}^{p-1} \chi(a_{i|p'})$$

which violates the independence of $\big(\chi(a_{i|p'})\big)$s. Thus $n \geq 1$. Let $\chi(a_{i|p}) = \rho^{t_i}$ for $0 \leq i \leq p-1$. We may suppose that

$$t_0 = 0,\ t_1 = 1,\ 0 \leq t_2 \leq \cdots \leq t_{p-1} \leq p^n - 1.$$

Consider the polynomial

$$A(x) = \sum_{i=0}^{p-1} x^{t_i}\chi(a_{i|p'}) = \sum_{i=0}^{s-1} x^{r_i}\lambda_i,$$

where $r_0, \ldots, r_{s-1}$ are all the distinct numbers among $t_0, \ldots, t_{p-1}$. Since λ_i cannot be zero, $A(x)$ is not the zero polynomial. The (p^n)th cyclotomic polynomial

$$F(x) = \sum_{i=0}^{p-1} x^{ip^{n-1}}$$

is irreducible over the (p')th cyclotomic field. Clearly ρ is a common root of $F(x)$ and $A(x)$ and so $F(x)$ divides $A(x)$ over the (p')th cyclotomic field. There is a polynomial $B(x)$ with coefficients from the (p')th cyclotomic field such that $A(x) = F(x)B(x)$. From $0 \leq \deg A(x) \leq p^n - 1$ and $\deg F(x) = (p-1)p^{n-1}$, it follows that $\deg B(x) \leq p^{n-1} - 1$. Consequently, the terms of $B(x)$ occur among the terms of $A(x)$. Let

v be the number of terms in $B(x)$. So $p \geq s = pv$ gives that $s = p$ and $v = 1$. Further

$$1 = t_1 = p^{n-1},\ t_2 = 2p^{n-1}, \ldots, t_{p-1} = (p-1)p^{n-1}$$

and $\lambda_0 = \cdots = \lambda_{p-1}$. Thus $n = 1$ and $\lambda_i = \chi(a_{i|p'})$ and $t_i = i$ for $0 \leq i \leq p-1$. Finally, $\chi(a_{0|p'}) = 1$ provides $\lambda_i = 1$ for $0 \leq i \leq p-1$.

This completes the proof. $\Diamond$

Corollary 1. *Under the conditions of* Lemma 1

(a) $\mathrm{Ann}(A) \subset \mathrm{Ann}(A')$, *where* A' *consists of the* p*-parts of the elements of* A,

(b) $\mathrm{Ann}(A) \subset \mathrm{Ann}\big([a,p]\big)$ *for each* $a \in A \setminus \{e\}$.

Proof. Only part (b) needs proof.

$$0 = \chi(A) = \sum_{i=0}^{p-1} \chi(a_i) = \sum_{i=0}^{p-1} \rho^i = \sum_{i=0}^{p-1} (\rho^j)^i =$$

$$= \sum_{i=0}^{p-1} \chi(a_j^i) = \sum_{i=0}^{p-1} \chi(a_j^i) = \chi\big([a_j,p]\big)$$

for each $1 \leq j \leq p-1$.

This completes the proof. $\Diamond$

Lemma 2. *Let* p *and* q *be distinct primes. Let* $A \subset G$ *with* $e \in A$ *and* $|A| = p$. *If* A *contains only* (p,q)*-elements, then* $\chi(a_{|q}) = 1$ *for each* $\chi \in \mathrm{Ann}(A)$ *and* $a \in A$.

Proof. Let $A = \{a_0, a_1, \ldots, a_{p-1}\}$, where $a_0 = e$ and let $\chi \in \mathrm{Ann}(A)$. There exist minimal nonnegative integers m and n such that

$$\chi(a_{i|p}) = \rho^{u_i},\ 0 \leq u_i \leq p^m - 1,$$

$$\chi(a_{i|q}) = \sigma^{v_i},\ 0 \leq v_i \leq q^n - 1$$

for $0 \leq i \leq p-1$, where ρ and σ are primitive (p^m)th and (q^n)th roots of unity. Consider the polynomial

$$A(x,y) = \sum_{i=0}^{p-1} x^{u_i} y^{v_i}.$$

We claim that $m \geq 1$. In order to prove the claim assume the contrary that $m = 0$. Note that now $n = 0$ is not possible since in the $m = n = 0$ case we get the $0 = \chi(A) = A(\rho,\sigma) = A(1,1) = p$ contradiction. Thus $n \geq 1$. The equation $0 = \chi(A) = A(\rho,\sigma) = A(1,\sigma)$ shows that σ is a common root of the polynomials $A(1,y)$ and the (q^n)th cyclotomic

polynomial $K(y)$. Thus $A(1,y) = K(y)B(y)$. Since $A(1,1) = p$, $A(1,y)$ is not the zero polynomial. Therefore $0 \leq \deg A(1,y) \leq q^n - 1$ and $\deg K(y) = (q-1)q^{n-1}$ implies that $0 \leq \deg B(y) \leq q^{n-1} - 1$. From this it follows that the terms of $B(y)$ occur among the terms of $A(1,y)$ and so $B(y)$ has integer coefficients. Now $p = A(1,1) = K(1)B(1) = qB(1)$ is a contradiction since q does not divide p. Therefore $m \geq 1$.

Next we claim that $A(x,\sigma)$ is not the zero polynomial. To prove the claim assume the contrary that $A(x,\sigma)$ is the zero polynomial. We can write $A(x,y)$ in the following form

$$A(x,y) = \sum_{i=0}^{p-1} x^{u_i} y^{v_i} = \sum_{i=0}^{w-1} x^{t_i} B_i(y),$$

where $t_0, \ldots, t_{w-1}$ are all the distinct numbers among $u_0, \ldots, u_{p-1}$. By the indirect assumption $B_i(\sigma) = 0$ for $0 \leq i \leq w-1$ and consequently $n \geq 1$. From $K(y) \mid B_i(y)$ it follows that $q \mid B_i(1)$. Now

$$p = A(1,1) = \sum_{i=0}^{w-1} B_i(1)$$

leads to the contradiction that $q \mid p$. Thus $A(x,\sigma)$ is not the zero polynomial. By the minimality of m we may assume that

$$u_0 = 0,\ u_1 = 1,\ 0 \leq u_2 \leq \cdots \leq u_{p-1} \leq p^m - 1.$$

From this point the proof follows the proof of Lemma 1.

This completes the proof. $\Diamond$

Corollary 2. *Under the conditions of Lemma 2*

(a) $\mathrm{Ann}(A) \subset \mathrm{Ann}(A')$, *where* A' *consists of the p-parts of the elements of* A,

(b) $\mathrm{Ann}(A) \subset \mathrm{Ann}([a,p])$ *for each* $a \in A \setminus \{e\}$.

3. Zero divisors

We will work in the group ring $\mathbb{Z}(G)$ whose elements are in the form $x_1 g_1 + \cdots + x_s g_s$, where $g_1, \ldots, g_s$ are all the elements of G and $x_1, \ldots, x_s$ are integers. Characters of $\mathbb{Z}(G)$ are linear extensions of the characters of G. We will introduce the following notations. Let $A \in \in \mathbb{Z}(G)$. The set of elements of G having nonzero coefficients in A will be denoted by $\{A\}$. The span (or generatum) of $\{A\}$ will be denoted by $\langle A \rangle$. Finally, the number of the not necessarily distinct prime factors

of $\langle A\rangle$ we will denote by $r(A)$. The next lemma is a generalization of a zero divisor result of G. Hajós. Our proof follows Hajós's proof with some necessary modifications.

Lemma 3. *Let $B, A_1, \dots, A_n \in \mathbb{Z}(G)$ such that each A_i is in one of the following forms*

$$A_i = e - a_i, \tag{1}$$

$$A_i = e + a_i + a_i^2 + \cdots + a_i^{p_i-1}, \tag{2}$$

$$A_i = e + a_{i,1} + \cdots + a_{i,p_i-1}, \tag{3}$$

where p_i is a prime. In the (3) case

$$\mathrm{Ann}(A_i) \subset \mathrm{Ann}(e + a_{i,j} + a_{i,j}^2 + \cdots + a_{i,j}^{p_i-1}) \tag{4}$$

for each $1 \le j \le p_i - 1$. Suppose that no factor A_i can be omitted from the equation

$$BA_1 \cdots A_n = 0 \tag{5}$$

and $n \ge 1$. Then

$$r(B, A_1, \dots, A_n) - r(B) < n. \tag{6}$$

Proof. Note that since no factor A_i can be cancelled from equation (5), it follows that $B \neq 0$ and $A_i \neq ke$, where k is an integer.

Let $n = 1$ and $A_1 = e - a_1$. Now $B(e - a_1) = 0$ gives that $B = Ba_1$. Since $B \neq 0$, there are $b, b' \in \{B\}$ with $b = b'a_1$, that is, $a_1 \in \langle B\rangle$. Therefore $r(B, A_1) - r(B) < 1$.

Let $n = 1$ and

$$A_1 = e + a_1 + a_1^2 + \cdots + a_1^{p_1-1}.$$

The equation

$$B(e + a_1 + a_1^2 + \cdots + a_1^{p_1-1}) = 0 \tag{7}$$

gives that

$$B(a_1 + a_1^2 + \cdots + a_1^{p_1-1}) = -B$$

from which it follows that $a_1^i \in \langle B\rangle$ for some $1 \le i \le p_1 - 1$. If $\{A_1\}$ is a subgroup of G, then $\langle a_1^i\rangle = \{A_1\} \subset \langle B\rangle$ and we are done. If $\{A_1\}$ is not a subgroup, then $a_1^{p_1} \neq e$. Multiplying (7) by $(e - a_1)$ we get $B(e - a_1^{p_1}) = 0$ which gives $a_1^{p_1} \in \langle B\rangle$. Now $a_1^{p_1}, a_1^i \in \langle B\rangle$ implies that $\{A_1\} \subset \langle B\rangle$.

Let $n = 1$ and

$$A_1 = e + a_{1,1} + \cdots + a_{1,p_1-1}.$$

The equation

$$BA_1 = 0 \tag{8}$$

holds if and only if $\chi(BA_1) = 0$ for each character χ of G. By (4) the factor A_1 can be replaced by

$$A_{1,i} = e + a_{1,i} + a_{1,i}^2 + \cdots + a_{1,i}^{p_1-1}$$

for $1 \le i \le p_1 - 1$. So $BA_{1,i} = 0$ and $A_{1,i}$ cannot be cancelled. Thus $a_{1,i} \in \langle B \rangle$ for $1 \le i \le p_1 - 1$ which means that $\{A_1\} \subset \langle B \rangle$.

We proceed by induction on n. From the equation

$$(BA_1 \cdots A_s)A_{s+1} \cdots A_n = 0$$

we have that

$$r(BA_1 \cdots A_s, A_{s+1}, \ldots, A_n) - r(BA_1 \cdots A_s) < n - s \tag{9}$$

for $1 \le s \le n-1$.

If $H \subset K \subset G$ and $L \subset G$, then the index $|\langle K, L\rangle : \langle H, L\rangle|$ divides the index $|\langle K\rangle : \langle H\rangle|$. Thus $r(K, L) - r(H, L) \le r(K) - r(H)$. Applying this observation in the case

$$H = \{BA_1 \cdots A_s\},$$
$$K = \{B\} \cup \{A_1\} \cup \cdots \cup \{A_s\},$$
$$L = \{A_{s+1}\} \cup \cdots \cup \{A_n\}$$

we obtain that

$$r(B, A_1, \ldots, A_n) - r(BA_1 \cdots A_s, A_{s+1}, \ldots, A_n) \le$$
$$\le r(B, A_1, \ldots, A_s) - r(BA_1 \cdots A_s).$$

Adding this to (9) it follows that

$$r(B, A_1, \ldots, A_n) - r(B, A_1, \ldots, A_s) < n - s \tag{10}$$

and similarly

$$r(B, A_1, \ldots, A_n) - r(B, A_n) < n - 1. \tag{11}$$

If there is an A_i with $r(A_i) = 1$, say A_1, then $r(B, A_1) - r(B) \le 1$. Adding this to the $s = 1$ case of (10) we get the desired result. Thus $r(A_i) \ge 2$ may be assumed for each $1 \le i \le n$. The case when each factor is in form (1) or (2) is settled by Hajós. For a fixed n we proceed by induction on $r(A_1) + \cdots + r(A_n) + d$, where d is the number of factors A_i that are not in form (1) or (2).

Consider A_n and distinguish three cases.

Let $A_n = e - a_n$. Multiply (5) by

$$e + a_n + a_n^2 + \cdots + a_n^{p-1},$$

where p is a prime factor of $|a_n|$. We have that

$$BA_1 \cdots A_{n-1} A_n' = 0,$$

where $A_n' = e - a_n^p$. After deleting the superfluous factors and renaming this becomes $BA_1 \cdots A_t A_n' = 0$. Clearly A_n' surely remains. Now $r(A_n') + 1 = r(A_n)$. By the inductive assumption

$$r(B, A_1, \ldots, A_t, A_n') - r(B) < t + 1. \tag{12}$$

If $t \geq 1$, then from (12) it follows that $r(B, A_1, \ldots, A_t) - r(B) \leq t$ and adding this to the $s = t$ case of (10) we are done. If $t = 0$, then $r(B, A_n') - r(B) < 1$ and so $r(B, A_n) - r(B) \leq 1$. Adding this to (11) we have (6).

Let

$$A_n = e + a_n + a_n^2 + \cdots + a_n^{p_n - 1}.$$

Multiplying (5) by $(e - a_n)$ we have

$$BA_1 \cdots A_{n-1} A_n' = 0,$$

where $A_n' = e - a_n^{p_n}$. After canceling the superfluous factors we may assume that

$$BA_1 \cdots A_t A_n' = 0.$$

Now d decreased so by the induction assumption

$$r(B, A_1, \ldots, A_t, A_n') - r(B) < t + 1.$$

Now as in the previous case we get the desired result.

Let

$$A_n = e + a_{n,1} + \cdots + a_{n,p_n - 1}.$$

In (5) A_n can be replaced by

$$A_{n,i} = e + a_{n,i} + a_{n,i}^2 + \cdots + a_{n,i}^{p_n - 1}.$$

After canceling the superfluous factors we may suppose that

$$BA_1 \cdots A_t A_{n,i} = 0$$

since $A_{n,i}$ cannot be cancelled. Now d is decreased so by the inductive assumption

$$r(B, A_1, \ldots, A_t, A_{n,i}) - r(B) < t + 1.$$

If $t \geq 1$ for some i, then adding $r(B, A_1, \ldots, A_t) - r(B) \leq t$ to the $s = t$ case of (10) we are done. Thus we may suppose that $r(B, A_{n,i}) - r(B) \leq 0$ for each $1 \leq i \leq p_n - 1$. But now $a_{n,i} \in \langle B \rangle$ for each

$1 \leq i \leq p_n - 1$, that is, $\{A_n\} \subset \langle B \rangle$ whence $r(B, A_n) - r(B) = 0$. Adding this to (11) we get the desired result.

This completes the proof. $\Diamond$

4. Rédei's theorem

We are now ready to prove Rédei's theorem.

Theorem 1. *Let*

$$G = A_1 \cdots A_n \tag{13}$$

be a factorization of the finite abelian group G, where $e \in A_i$ and $|A_i|$ is a prime for $1 \leq i \leq n$. Then one of the factors A_i is a subgroup of G.

This theorem actually implies a stronger form of itself. Namely, there is a permutation $B_1, \ldots, B_n$ of the factors $A_1, \ldots, A_n$ such that the partial products

$$B_1,\ B_1B_2, \ldots, B_1B_2 \cdots B_n \tag{14}$$

form an ascending chain of subgroups of G. A proof may proceed by induction on n considering a factor group with respect to an existing subgroup factor.

Proof. First we prove the theorem for elementary p-groups. The $|G| = p$ case is trivial. So we assume that $n \geq 2$. By Cor. 1, in factorization (13) the factor A_1 can be replaced by a subgroup H. In chain (14) consider the subgroup $K = HA_1 \cdots A_{n-1}$. In (13) A_n can also be replaced by a subgroup M. Since $G = KM$ is a factorization of G, $K \cap M = \{e\}$. From the factorization $G = A_1 \cdots A_{n-1}M$ it follows that there is an index j such that MA_j is a subgroup of G. If $j \neq 1$, then $K \cap MA_j = A_j$ is a subgroup and we are done. Thus we may assume that $N = MA_1$ is a subgroup. If A_n is not in N, then in (13) A_n can be replaced by a subgroup L such that $L \cap N = \{e\}$. As before we may assume that LA_1 is a subgroup and so $N \cap LA_1 = A_1$ is a subgroup. Thus we left with the $A_n \subset N$ case. Now $N = A_1A_n$ is a factorization. This reduces the problem to the $n = 2$ case for which there are proofs in [3] and [8] respectively.

Next we prove the theorem for p-groups. To do so consider a counter example with minimal $|G|$. We know that G is not an elementary p-group. Consequently, there is a factor, say A_n, such that $a \in A_n$

and $|a| > p$. In (13) the factor A_n can be replaced by $[a, p]$. To a subset A of G we assign an element

$$\overline{A} = \sum_{a \in A} a$$

of $\mathbb{Z}(G)$. To the factorization $G = A_1 \cdots A_{n-1}[a, p]$ we assign the equation

$$\overline{G} = \overline{A}_1 \cdots \overline{A}_{n-1}(e + a + a^2 + \cdots + a^{p-1})$$

in $\mathbb{Z}(G)$. From this by multiplying by $(e - a)$ we get that $0 = \overline{A}_1 \cdots \overline{A}_{n-1}(e - a^p)$. After canceling and relabeling we may suppose that $0 = \overline{A}_1 \cdots \overline{A}_m(e - a^p)$, where $m \geq 1$ since $(e - a^p)$ surely remains and since $e - a^p \neq 0$. Lemma 3 is applicable with the $B = e$ choice and gives that $r(A_1, \ldots, A_m, a^p) < m + 1$. Hence

$$r(A_1, \ldots, A_m) \leq m. \tag{15}$$

Let $T = A_1 \cdots A_m$ and $S = A_{m+1} \cdots A_n$. Restricting the factorization $G = TS$ to $\langle T \rangle$ we get the factorization $\langle T \rangle = G \cap \langle T \rangle = T\big(S \cap \langle T \rangle\big)$. This shows that $|T|$ divides $\big|\langle T \rangle\big|$, that is, $p^m = |T| \leq \big|\langle T \rangle\big| \leq p^m$. It follows that $T = \langle T \rangle$ and so $T = A_1 \cdots A_m$ is a smaller counter example.

In the remaining part of the proof we may assume that G is not a p-group. Call

$$\prod_{i=1}^{n} \prod_{a \in A_i} |a|$$

the height of the factorization (13). Suppose that (13) is a counter example with minimal $|G|$ and with minimal height.

Let p be the smallest prime factor of $|G|$. If each factor of cardinality p has only p-elements, then they form a factorization of the p-component of G. The p-component is a proper subgroup of G so it provides a counter example with smaller order. Thus there is a factor, say A_1 such that $|A_1| = p$ and A_1 contains not only p-elements. Let A_1' be the set of the p-parts of the elements of A_1. In (13) the factor A_1 can be replaced by A_1'. The height of the factorization decreased so by the minimality of the counter example there is a subgroup among the factors. This leads to a contradiction unless A_1' is a subgroup of G. In the chain (14) there is a subgroup

$$K_1 = A_1' A_{1,1} \cdots A_{1,r_1} A_2$$

such that

$$p = |A_1'| = |A_{1,1}| = \cdots = |A_{1,r_1}| \neq |A_2| = q.$$

Note that K_1 is a (p,q)-group. Let A_2' be the set of the q-parts of the elements of A_2. Clearly, A_2' is the q-Sylow subgroup of K_1. In (13) by Cor. 2, the factor A_2 can be replaced by A_2'. In the chain (14) there is a subgroup

$$K_2 = A_2' A_{2,1} \cdots A_{2,r_2} A_3$$

such that

$$q = |A_2'| = |A_{2,1}| = \cdots = |A_{2,r_2}| \neq |A_3|.$$

Repeat this process. In the chain (14) there is a subgroup

$$K_t = A_t' A_{t,1} \cdots A_{t,r_t} A_{t+1}$$

such that

$$|A_t'| = |A_{t,1}| = \cdots = |A_{t,r_t}| \neq |A_{t+1}|$$

and A_{t+1} coincides with one of the factors $A_1, \ldots, A_t$, say with A_1. The orders of the elements make sure that A_{t+1} cannot coincide with a factor $A_{i,j}$. We assume that this is the first instance when such a coincidence occur. Consider the subgroup $H = K_1 \cdots K_t$. The product of the distinct factors occurring among

$$\begin{array}{l} A_1, A_{1,1}, \ldots, A_{1,r_1}, \\ A_2, A_{2,1}, \ldots, A_{2,r_2}, \\ \quad \vdots \quad \vdots \qquad \ddots \quad \vdots \\ A_t, A_{t,1}, \ldots, A_{t,r_t} \end{array}$$

is equal to H. By the minimality of the counter example $H = G$. We can draw the conclusion that A_1 contains only (p,q)-elements. There is an element a in A_1 with $|a| > p$. In (13) A_1 can be replaced by $[a,p]$. From the factorization $G = [a,p]A_2 \cdots A_n$ it follows the $0 = (e - a^p)\overline{A}_2 \cdots \overline{A}_n$ equation in $\mathbb{Z}(G)$. In the way we have seen in the previous part we can get a smaller counter example.

This completes the proof. $\Diamond$

5. Periodic subsets

Let A be a subset of a finite abelian group G. We say that A is periodic if there is a $g \in G$ such that $A = Ag$ and $g \neq e$. We say that A is normalized if $e \in A$. If A is normalized and g is a period of A, then $g \in A$.

Lemma 4. *Let G be a finite abelian group and let $G = AB$ be a factorization of G. Suppose that A is periodic with period g and there is a $b \in B$ such that $bg \notin B$. Set*

$$C = (B \setminus \{b\}) \cup \{bg\}.$$

Then $G = AC$ is a factorization of G.

Proof. It is enough to prove that

$$\chi(G) = \chi(AC) = \chi(A)\chi(C) \tag{16}$$

for each character χ of G. We claim that this holds. In order to prove the claim pick a character χ of G.

If χ is the principal (or identity) character of G, then (16) reduces to

$$|G| = |A||C|. \tag{17}$$

From the factorization $G = AB$ it follows that $|G| = |A||B|$. Using the fact $|B| = |C|$ we get (17) as required. For the remaining part of the proof we may assume that χ is not the principal character of G. Now (16) reduces to

$$0 = \chi(A)\chi(C). \tag{18}$$

If $\chi(A) = 0$, then (18) clearly holds. So we may assume that $\chi(A) \neq 0$. Applying χ to the factorization $G = AB$ gives that $0 = \chi(A)\chi(B)$. As $\chi(A) \neq 0$ it follows that $\chi(B) = 0$. Applying χ to the equation $A = Ag$ gives that $\chi(A)\big(1 - \chi(g)\big) = 0$. As $\chi(A) \neq 0$ it follows that $\chi(g) = 1$. Using $\chi(B) = 0$ and $\chi(g) = 1$ we get $\chi(C) = 0$. This implies (18) as required. $\Diamond$

The next result is an extension of Rédei's theorem.

Theorem 2. *Let G be a finite abelian group and let*

$$G = A_1 \cdots A_n C \tag{19}$$

be a normalized factorization of G. Suppose that each $|A_i|$ is a prime and the subset $A = A_1 \cdots A_n$ is periodic. Then one of the factors $A_1, \ldots, A_n$ is a subgroup of G.

Proof. Assume the contrary that there is a counter example for the theorem. If $C = \{e\}$, then by Rédei's theorem one of the factors $A_1, \ldots, A_n$ is a subgroup of G. Thus we may assume that $C \neq \{e\}$. If $n = 1$, then A_1 is a normalized periodic subset containing a prime number of elements and consequently A_1 is a subgroup of G. Thus we may assume that $n \geq 2$.

Let g be a period of $A = A_1 \cdots A_n$. Choose a $c \in C \setminus \{e\}$ and set $D = \big(C \setminus \{c\}\big) \cup \{cg\}$. We claim that $cg \notin C$. To prove the claim assume the contrary that $cg \in C$, that is, $g \in Cc^{-1}$. Multiplying the factorization $G = AC$ by c^{-1} we get the normalized factorization $G = Gc^{-1} = A(Cc^{-1})$. This leads to the contradiction $g \in A$ and $g \in Cc^{-1}$. Therefore $cg \notin C$ as claimed.

By Lemma 4,

$$G = A_1 \cdots A_n D \tag{20}$$

is a normalized factorization of G. Consider the factor A_i in the factorizations (19) and (20). Suppose that $|A_i| = p$, where p is a prime. By Prop. 3 of [7], A_i can be replaced B_i such that B_i is not a subgroup of G and B_i contains only (p, q)-elements, where q is a prime. We would like to point out that q is not necessarily unique. Further the primes p and q may vary with i.

From factorizations (19), (20) we get the factorizations

$$G = B_1 \cdots B_n C, \tag{21}$$

$$G = B_1 \cdots B_n D. \tag{22}$$

To the factorizations (21), (22) we assign the equations

$$\overline{G} = \overline{B}_1 \cdots \overline{B}_n \overline{C},$$

$$\overline{G} = \overline{B}_1 \cdots \overline{B}_n \overline{D}$$

in the group ring $\mathbb{Z}(G)$. A subtraction gives that

$$0 = \overline{B}_1 \cdots \overline{B}_n (c - cg)$$

and then

$$0 = \overline{B}_1 \cdots \overline{B}_n (e - g). \tag{23}$$

It can happen that the equation holds after canceling some of its factors. Clearly $(e - g)$ cannot be cancelled since $\overline{B}_1 \cdots \overline{B}_n \neq 0$. All of $\overline{B}_1, \ldots, \overline{B}_n$ cannot be cancelled since $(e - g) \neq 0$. Thus we may assume that after all possible cancellation

$$0 = \overline{B}_1 \cdots \overline{B}_m (e - g) \tag{24}$$

since this is only a matter of renaming the factors in (23). Lemma 3 is applicable to (24) and gives that

$$r(B_1, \ldots, B_m, g) < m + 1.$$

It follows that $r(B_1, \ldots, B_m, g) \leq m$ and then $r(B_1, \ldots, B_m) \leq$ $\leq m$, that is, the order of $H = \langle B_1, \ldots, B_m \rangle$ is a product of at most m

(not necessarily distinct) primes.

We claim that $|H|$ is a product of exactly m primes. In order to prove the claim set

$$T = B_1 \cdots B_m, \ S = B_{m+1} \cdots B_n C.$$

Clearly $G = TS$ is a factorization of G. Restricting the factorization $G = TS$ to $\langle T \rangle$ we get that

$$\langle T \rangle = G \cap \langle T \rangle = T\big(S \cap \langle T \rangle\big)$$

is a factorization of $\langle T \rangle$. It follows that $|T|$ divides the order of $\langle T \rangle$. Note that $\langle T \rangle \subset H$. Thus $|H|$ is a product of at least m primes.

Therefore the product $B_1 \cdots B_m$ is a factorization of H. By Rédei's theorem one of the factors $B_1, \ldots, B_m$ is a subgroup of H and so of G. This contradiction completes the proof. $\Diamond$

6. Non-periodic factors

After proving Rédei's theorem for p-groups there are various ways to extend the proof for all finite abelian groups. We will present a proof which based on tactically replacing a product by a non-periodic subset. We need two lemmas. The second lemma first was proved in [6].

Lemma 5. *Let A be a nonempty subset of a finite abelian group G. If for the subset*

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

assigned to A it holds that $U \neq \{e\}$, then A is periodic.

Proof. Let $A = \{a_1, \ldots, a_n\}$. Since A is not empty, $e \in U$. Choose $g \in U \setminus \{e\}$. There are elements $b_1, \ldots, b_n \in A$ such that $g = b_1 a_1^{-1} = \cdots = b_n a_n^{-1}$. Note that $b_1, \ldots, b_n$ are pair-wise distinct elements of A. Clearly $b_1, \ldots, b_n$ are all the elements of A. Consequently,

$$gA = \{ga_1, \ldots, ga_n\} = \{b_1 a_1^{-1} a_1, \ldots, b_n a_n^{-1} a_n\} = \{b_1, \ldots, b_n\} = A.$$

This completes the proof. $\Diamond$

Lemma 6. *Let G be a finite abelian group. Let H be a subgroup of G. Let $A, B \subset G$ such that $A \subset H$, $e \in A \cap B$, the product AB is direct, A, B are not periodic, the elements of B are pair-wise incongruent modulo H. Then the set AB is not periodic.*

Proof. Set $C = AB$ and let $g \in G$ such that $C = Cg$. Let $B = \{b_1, \ldots, b_s\}$. As the product AB is direct the sets $Ab_1, \ldots, Ab_s$ form a partition of C. In particular

$$C = Ab_1 \cup \cdots \cup Ab_s.$$

As $A \subset H$ and $b_1, \ldots, b_s$ are pair-wise incongruent modulo H, it follows that the sets $Ab_1, \ldots, Ab_s$ are in distinct cosets modulo H. Multiplying $Ab_1, \ldots, Ab_s$ by g permutes these sets. For each i, $1 \leq i \leq s$, there is a j, $1 \leq j \leq s$ such that $Ab_ig = Ab_j$. From this we must get $b_ig = b_j$ otherwise A is periodic with period $b_igb_j^{-1}$. Hence $g = b_jb_i^{-1}$ and so

$$g \in \bigcap_{b \in B} Bb^{-1}.$$

From this we must get $g = e$ since otherwise by Lemma 5, B is periodic.

This completes the proof. ◊

Theorem 3. *If Rédei's theorem holds for each finite abelian p-groups, then it holds for each finite abelian group.*

Proof. Assume the contrary that there is a finite abelian group G such that G is not a p-group G has a factorization

$$G = A_1 \cdots A_n, \tag{25}$$

where each A_i is a normalized non-subgroup of G containing a prime number of elements. We may assume that in this counter example n is minimal and among these

$$\prod_{i=1}^{n} \prod_{a \in A_i} |a|$$

the height of the factorization is minimal.

Let p be the smallest prime divisor of $|G|$. There is a factor, say A_1, such that $|A_1| = p$ and A_1 contains an element a whose order is not a power of p. Let A_1' be the set of the p-parts of the elements of A_1. By Cor. 1, in (25) A_1 can be replaced by A_1' to get the factorization

$$G = A_1'A_2 \cdots A_n.$$

The height of this factorization is smaller than the height of (25). By the minimality of the counter example one of the factors $A_1', A_2, \ldots, A_n$ is a subgroup of G. This is a contradiction unless $A_1' = H$ is a subgroup of G. As we have seen earlier there is a permutation $B_2, \ldots, B_n$ of the factors $A_2, \ldots, A_n$ such that

$$K_1 = H,\ K_2 = HB_2, \ldots, K_n = HB_2 \cdots B_n$$

is an ascending chain of subgroups of G. From the factorization $K_3 = = K_2B_3$ it follows that the elements of B_3 are incongruent modulo K_2. Note that $B_2 \subset K_2$. Now Lemma 6 is applicable and gives that B_2B_3 is not periodic.

From the factorization $K_4 = K_3B_4$ it follows that the elements of B_4 are incongruent modulo K_3. We can see that $B_2B_3 \subset K_3$ holds. Lemma 6 shows that $(B_2B_3)B_4$ is not periodic. Continuing in this way finally we get that $(B_2 \cdots B_{n-1})B_n$ is not periodic.

By Cor. 1, in the factorization $G = A_1(B_2 \cdots B_n)$, A_1 can be replaced by $[a, p]$ to get the factorization $G = [a, p]B_2 \cdots B_n$. From this it follows the contradiction that $B_2 \cdots B_n$ is periodic with period a^p.

The proof is complete. $\Diamond$

References

[1] FUCHS, L.: Abelian Groups, Akadémia Kiadó, Budapest 1958.

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

[3] LOVÁSZ, L., SCHRIJVER, A.: Remarks on a theorem of Rédei, *Studia Sci. Math. Hungar.* **16** (1981), 449–454.

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

[5] RÉDEI, L.: Algebra, Pergamon Press, Oxford–London, 1967.

[6] SANDS, A. D.: The factorization of abelian groups II, *Quart. J. Math. Oxford (2)* **13** (1962), 45–54.

[7] SANDS, A. D.: Replacement of factors by subgroups in the factorization of abelian groups, *Bull. London Math. Soc.* **32** (2000), 297–304.

[8] WITTMANN, E.: Einfacher Beweis des Hauptsatzes von Hajós–Rédei für elementare Gruppen von Primzahlquadratordnung, *Acta Math. Acad. Sci. Hungar.* **20** (1969), 227–230.

[9] WITTMANN, E.: Über verschwindete Summen von Einheitswurzeln, *Elemente der Math.* **26** (1971), 42–43.