DEMONSTRATIO MATHEMATICA
Vol. XXXIII No 3 2000

Sandor Szabó

AN EXTENSION OF A RESULT OF A. D. SANDS

Abstract. A. D. Sands showed that if a group of type $(2^2, 2^2)$ is a direct product of its subsets of order 4, then at least one of these subsets must be periodic. In this paper we prove a result about groups of type $(2^\lambda, 2^\lambda)$ that generalizes Sands' theorem.

1. Introduction

In this paper we will use multiplicative notation in connection with finite abelian groups. If A and B are subsets of a finite abelian group G such that the product AB is direct and is equal to G we say that AB is a factorization of G. We also say that the equation $G = AB$ is a factorization of G. In other words the product AB is a factorization of G if each element g in G is uniquely expressible in the form $g = ab$, where $a \in A$ and $b \in B$. In the most commonly encountered situation A and B are subgroups of G. However, in this paper we do not assume that A and B are subgroups of G. A subset A of a finite abelian group G is called periodic if there is an element $g \in G \setminus \{e\}$ such that $A = gA$. (Here e stands for the identity element of G.) Sometimes we express this fact saying that g is a period of A or A is periodic with period g. A subset A of G is called normed if the identity element e of G is contained by A. We call the factorization $G = AB$ normed if the factors A and B are normed.

By the fundemental theorem of finite abelian groups each finite abelian group is a direct product of cyclic groups. If G is a direct product of cyclic groups of orders $q_1, \dots, q_s$ respectively, then we say that G is of type $(q_1, \dots, q_s)$. We would like to point out that a group might be expressed as a direct product of cyclic groups in essentially different ways and so a given group might have different types. This is not going to cause any problem for us since for a given group type there belong to a uniquely determined (up to isomorphism) group and we use group types only to identify groups.

1991 *Mathematics Subject Classification*: Primary 20K01; Secondary 52C22.
Key words and phrases: factorization of finite abelian groups, Hajós-Rédei theory.

For a subset A of G the smallest subgroup of G containing A that is, the span of A in G, will be denoted by $\langle A\rangle$.

A. D. Sands (Theorem 8 of [3]) proved that if G is a group of type $(2^2, 2^2)$ and $G = AB$ is a normed factorization of G such that $|A| = |B| = 4$, then A or B is periodic.

The main result of this paper is the following.

If G is a group of type $(2^\lambda, 2^\lambda)$, $\lambda \geq 2$ and $G = AB$ is a normed factorization of G with $|A| = 4$, $\langle A\rangle = G$, then B is periodic.

In the next lines we will verify that this result implies Sands' theorem and with this Sands' theorem is placed into a wider context.

Let G be of type $(2^2, 2^2)$ and let $G = AB$ be a normed factorization of G with $|A| = |B| = 4$. Set $H = \langle A\rangle$. As $A \subset H$ and $H \subset G$, it follows that $4 \leq |H| \leq 16$. We distinguish three cases depending on $|H| = 4$ or $|H| = 8$ or $|H| = 16$. In the $|H| = 4$ case $A = H$ and so A is clearly periodic. If $|H| = 8$, then restricting the factorization $G = AB$ to H gives the $H = G \cap H = A(B \cap H)$ normed factorization of H. From $|H| = 8$ and $|A| = 4$, it follows that $|B \cap H| = 2$. Let $B \cap H = \{e, b\}$. The factorization $H = A\{e, b\}$ is equivalent to that A and Ab form a partition of H. Note that $Ab \cap Ab^2 = \emptyset$ and so Ab and Ab^2 also form a partition of H. Comparing the two partitions gives $A = Ab^2$. If $b^2 \neq e$, then A is periodic. If $b^2 = e$, then B has an element of order 2. Now Lemma 1 of [3] is applicable to factorization $G = AB$ and gives that A or B is periodic. In the $|H| = 16$ case $\langle A\rangle = G$ and our main result is applicable with the $\lambda = 2$ choice. This gives that B is periodic.

2. Preliminaries

If A is a subset and χ is a character of the finite abelian group G, then the notation $\chi(A)$ stands for the sum $\sum_{a\in A}\chi(a)$. In the $\chi(A) = 0$ case we say that χ annihilates A. The set of all characters of G that annihilate A we call the annihilator set of A or simply the annihilator of A and we will denote it by $\mathrm{Ann}(A)$.

Let $G = AB$ be a factorization and let χ be a character of G. Applying the character to the factorization we get $\chi(G) = \chi(AB) = \chi(A)\chi(B)$. If χ is not the principal character of G, then $\chi(G) = 0$ and from $0 = \chi(A)\chi(B)$ it follows that either $\chi(A) = 0$ or $\chi(B) = 0$.

Characters of G can be used to test if the element g of G is a period of the subset A of G. Namely, by Theorem 1 of [4] g is a period of A if and only if $\mathrm{Ann}(\langle g\rangle) \subset \mathrm{Ann}(A)$. We will use the following variant of this result too. If A is a subset and g, h are elements of G such that

$$\mathrm{Ann}(\langle g\rangle) \cap \mathrm{Ann}(\langle h\rangle) \subset \mathrm{Ann}(A),$$

then it follows that A can be partitioned into two parts that are periodic with periods g and h respectively. In other words there are subsets U, V of G for which

$$A = U\langle g\rangle \cup V\langle h\rangle,$$

where the union is disjoint and the products $U\langle g\rangle$, $V\langle h\rangle$ are direct. This is Theorem 2 of [4].

If for a subset A and for elements g, h of a finite abelian group G the equations $A = Ag$, $A = Ah$ hold, then clearly $A = Agh$ also holds. This has the following consequences. If g is a period of A and g^i is not the identity element of G, then g^i is also a period of A. All the periods of A together with the identity element of G form a subgroup of G. If A is periodic, then it has a period with a prime order.

Let us consider a factorization $G = AB$ of G and let $a \in A$, $b \in B$. Multiplying the factorization by $g = a^{-1}b^{-1}$ we get the factorization $G = Gg = (Aa^{-1})(Bb^{-1})$ of G. Clearly, this factorization is normed. In addition, if A is periodic, then so is (Aa^{-1}) and similarly if B is periodic, then so is (Bb^{-1}). Thus, when we deal with periodic factorizations of G we may assume that the factorization is normed.

By our definition the equation $G = AB$ is a factorization of G if the product AB is direct and is equal to G. This fact can be expressed in many equivalent forms. We will use the following reformulations freely. Each element g of G has a unique representation in the form $g = ab$, where $a \in A$ and $b \in B$. The product AB is equal to G and $|A||B|$ is equal to $|G|$. The product is equal to G and $AA^{-1} \cap BB^{-1} = \{e\}$. Here A^{-1} is a short hand notation for the set $\{a^{-1} : a \in A\}$.

3. The result

With the tools and terminology are available from the previous section we can turn to the proof of the main result of the paper.

THEOREM 1. *Let G be a group of type $(2^\lambda, 2^\lambda)$, with $\lambda \geq 2$. If $G = AB$ is a normed factorization of G and $|A| = 4$, $\langle A\rangle = G$, then B is periodic.*

Proof. We divide the proof into 4 steps.

(1) We claim that there are elements x, y in A such that x, y form a basis for G.

In order to prove the claim note that because of its type G has a basis u, v with $|u| = |v| = 2^\lambda$. The elements of G whose order is less than or equal to $2^{\lambda-1}$ span the subgroup $\langle u^{2^{\lambda-1}}, v^{2^{\lambda-1}}\rangle$ of G. If A does not contain any element of order 2^λ, then $\langle A\rangle \subset \langle u^{2^{\lambda-1}}, v^{2^{\lambda-1}}\rangle \neq G$ which is a contradiction. Thus there is an element x of A with $|x| = 2^\lambda$. In the basis representation $x = u^\alpha v^\beta$, $0 \leq \alpha, \beta \leq 2^\lambda - 1$ of x at least one of α and β is odd. For the sake of definiteness we assume that α is odd. Now $\langle x\rangle \cap \langle v\rangle = \{e\}$ and consequently x, v is a basis for G. If $A \setminus \langle x\rangle = \emptyset$, then $\langle A\rangle \subset \langle x\rangle \neq G$. So $A \setminus \langle x\rangle \neq \emptyset$. Let $y = x^\gamma v^\delta$, $0 \leq \gamma, \delta \leq 2^\lambda - 1$ be an element of $A \setminus \langle x\rangle$. If for each choice of y the exponent δ is even, then $\langle A\rangle \subset \langle x, v^2\rangle \neq G$. Therefore there is a y with odd δ. In this case $\langle x\rangle \cap \langle y\rangle = \{e\}$ and so x, y is a basis for G.

(2) By step (1) A can be written in the form $A = \{e, x, y, x^\alpha y^\beta\}$, $0 \leq \alpha, \beta \leq 2^\lambda - 1$, where x, y is a basis for G. We claim that if (α, β) is not one of $(1,1)$, $(1, 2^\lambda - 1)$, $(2^\lambda - 1, 1)$, then B is periodic.

By Theorem 1 of [4] B is periodic with period g if and only if $\mathrm{Ann}(\langle g\rangle) \subset \mathrm{Ann}(B)$. Clearly, $\mathrm{Ann}(\langle g\rangle)$ consists of all characters χ of G that is not principal on $\langle g\rangle$. In other words, $\chi(\langle g\rangle) = 0$ if and only if $\langle g\rangle \not\subset \mathrm{Ker}\chi$. In the special case when $|g|$ is a prime g is a period of B if and only if $\chi(g) \neq 1$ implies $\chi(B) = 0$. We will use this condition in the form that $\chi(B) \neq 0$ implies $\chi(g) = 1$. For the principal character this obviously holds. If χ is not the principal character of G, then from the factorization $G = AB$ it follows that $0 = \chi(G) = \chi(AB) = \chi(A)\chi(B)$ and so if $\chi(B) \neq 0$, then $\chi(A) = 0$. Thus if $\chi(A) = 0$ implies $\chi(g) = 1$, then B is periodic with period g. Or equivalently, if $\chi(g) \neq 1$ implies $\chi(A) \neq 0$, then B is periodic with period g.

If B is periodic with period g, then we may assume that $|g| = 2$. The possible choices for g are $x^{2^{\lambda-1}}$, $y^{2^{\lambda-1}}$, $x^{2^{\lambda-1}}y^{2^{\lambda-1}}$.

In the $g = x^{2^{\lambda-1}}$ case $\chi(g) \neq 1$ holds for characters χ of G with $\chi(x) = \rho$, $\chi(y) = \rho^m$, where ρ is a primitive (2^λ)th root of unity and m is an integer $0 \leq m \leq 2^\lambda - 1$. Now $\chi(A) = 0$ must hold for some such character χ of G otherwise B is periodic with period g. This puts some restriction on the possible values of (α, β). Namely, (α, β) must belong to $Q_1 \cup Q_2$, where

$$Q_1 = \{(\alpha, \beta) : \alpha \equiv 2^{\lambda-1}\beta + 2^{\lambda-1} + 1 \pmod{2^\lambda},\quad 0 \leq \alpha, \beta \leq 2^\lambda - 1\},$$

$$Q_2 = \{(\alpha, \beta) : \alpha \equiv (2^{\lambda-1} - 1)\beta + 2^{\lambda-1} \pmod{2^\lambda},\quad 0 \leq \alpha, \beta \leq 2^\lambda - 1\}.$$

To prove this claim note that from

$$0 = \chi(A) = \rho^0 + \rho^1 + \rho^m + \rho^{\alpha + m\beta}$$

it follows that $0, 1, m, \alpha + m\beta$ is a rearrangement of $0, 1, 2^{\lambda-1}, 2^{\lambda-1} + 1$. This leads to the following two possibilities

$$m \equiv 2^{\lambda-1} \pmod{2^\lambda}, \quad \text{and} \quad \alpha + m\beta \equiv 2^{\lambda-1} + 1 \pmod{2^\lambda}$$

or

$$m \equiv 2^{\lambda-1} + 1 \pmod{2^\lambda}, \quad \text{and} \quad \alpha + m\beta \equiv 2^{\lambda-1} \pmod{2^\lambda}$$

which are equivalent to

$$\alpha \equiv 2^{\lambda-1}\beta + 2^{\lambda-1} + 1 \pmod{2^\lambda} \quad \text{or} \quad \alpha \equiv (2^{\lambda-1} - 1)\beta + 2^{\lambda-1} \pmod{2^\lambda}$$

respectively.

In the $g = y^{2^{\lambda-1}}$ case $\chi(g) \neq 1$ holds for characters χ of G with $\chi(x) = \rho^m$, $\chi(y) = \rho$, where ρ is a primitive (2^λ)th root of unity and m is an integer $0 \leq m \leq 2^\lambda - 1$. Now $\chi(A) = 0$ must hold for some such character χ of G otherwise B is periodic with period g. This places some restriction on the possible values of (α, β). Namely, (α, β) must belong to $Q_3 \cup Q_4$, where

$$Q_3 = \{(\alpha,\beta) : \beta \equiv 2^{\lambda-1}\alpha + 2^{\lambda-1} + 1 \pmod{2^\lambda}, \quad 0 \leq \alpha, \beta \leq 2^\lambda - 1\},$$
$$Q_4 = \{(\alpha,\beta) : \alpha \equiv (2^{\lambda-1} - 1)\beta + 2^{\lambda-1} \pmod{2^\lambda}, \quad 0 \leq \alpha, \beta \leq 2^\lambda - 1\}.$$

To prove this assertion note that from

$$0 = \chi(A) = \rho^0 + \rho^m + \rho^1 + \rho^{m\alpha+\beta}$$

it follows that $0, m, 1, m\alpha+\beta$ is a rearrangement of $0, 1, 2^{\lambda-1}, 2^{\lambda-1}+1$. This leads to the following two possibilities

$$m \equiv 2^{\lambda-1} \pmod{2^\lambda}, \quad \text{and} \quad m\alpha + \beta \equiv 2^{\lambda-1} + 1 \pmod{2^\lambda}$$

or

$$m \equiv 2^{\lambda-1} + 1 \pmod{2^\lambda}, \quad \text{and} \quad m\alpha + \beta \equiv 2^{\lambda-1} \pmod{2^\lambda}$$

which are equivalent to

$$\beta \equiv 2^{\lambda-1}\alpha + 2^{\lambda-1} + 1 \pmod{2^\lambda} \quad \text{or} \quad \alpha \equiv (2^{\lambda-1} - 1)\beta + 2^{\lambda-1} \pmod{2^\lambda}$$

respectively.

In the $g = x^{2^{\lambda-1}} y^{2^{\lambda-1}}$ case $\chi(g) \neq 1$ holds for characters χ of G with $\chi(x) = \rho^m$, $\chi(xy) = \rho$, where ρ is a primitive (2^λ)th root of unity and m is an integer $0 \leq m \leq 2^\lambda - 1$. Obviously, $\chi(y) = \rho^{1-m}$. Now $\chi(A) = 0$ must hold for some such character χ of G otherwise B is periodic with period g. This restricts the possible values of (α, β). Namely, (α, β) must belong to $Q_5 \cup Q_6$, where

$$Q_5 = \{(\alpha,\beta) : \beta \equiv 2^{\lambda-1}\alpha + 2^{\lambda-1} + 1 \pmod{2^\lambda}, \quad 0 \leq \alpha, \beta \leq 2^\lambda - 1\},$$
$$Q_6 = \{(\alpha,\beta) : \alpha \equiv 2^{\lambda-1}\beta + 2^{\lambda-1} + 1 \pmod{2^\lambda}, \quad 0 \leq \alpha, \beta \leq 2^\lambda - 1\}.$$

To verify this claim note that from

$$0 = \chi(A) = \rho^0 + \rho^m + \rho^{1-m} + \rho^{m\alpha+(1-m)\beta}$$

it follows that there is an integer l such that $0, m, 1-m, m\alpha + (1-m)\beta$ is a rearrangement of $0, 2^{\lambda-1}, l, l + 2^{\lambda-1} + 1$. We face to the following three possibilities

$$m \equiv 2^{\lambda-1} \pmod{2^\lambda}, \quad \text{and} \quad 1 - m + 2^{\lambda-1} \equiv m\alpha + (1-m)\beta \pmod{2^\lambda}$$

or

$$m - 1 \equiv 2^{\lambda-1} \pmod{2^\lambda}, \quad \text{and} \quad m + 2^{\lambda-1} \equiv m\alpha + (1-m)\beta \pmod{2^\lambda}$$

or

$$m\alpha + (1-m)\beta \equiv 2^{\lambda-1} \pmod{2^\lambda}, \quad \text{and} \quad m + 2^{\lambda-1} \equiv 1-m \pmod{2^\lambda}.$$

The last congruence leads to $2m + 2^{\lambda-1} \equiv 1 \pmod{2^\lambda}$ then to the contradiction $0 \equiv 1 \pmod 2$. This sorts out the third case. The first two cases are equivalent to

$$\beta \equiv 2^{\lambda-1}\alpha + 2^{\lambda-1} + 1 \pmod{2^\lambda} \quad \text{or} \quad \alpha \equiv 2^{\lambda-1}\beta + 2^{\lambda-1} + 1 \pmod{2^\lambda}$$

respectively.

Summing up our argument we can say that B has a chance not to be periodic only if (α, β) is an element of

$$(Q_1 \cup Q_2) \cap (Q_3 \cup Q_4) \cap (Q_5 \cup Q_6).$$

We will show that this set is equal to $\{(1,1),(1,2^\lambda-1),(2^\lambda-1,1)\}$. To do this note that $Q_4 = Q_2$, $Q_5 = Q_3$, $Q_6 = Q_1$ and $(Q_1 \cup Q_2) \cap (Q_3 \cup Q_2) = (Q_1 \cap Q_3) \cup Q_2 = \{(1,1)\} \cup Q_2$ as $Q_1 \cap Q_3 = \{(1,1)\}$. The rest follows from that $Q_2 \cap Q_1 = \{(1,2^\lambda-1)\}$ and $Q_2 \cap Q_3 = \{(2^\lambda-1,1)\}$.

(3) Let $A = \{e, x, y, x^\alpha y^\beta\}$, where x, y is a basis for G and (α, β) is one of $(1,1)$, $(1,2^\lambda-1)$, $(2^\lambda-1,1)$. We claim that the normed factorization $G = AB$ implies that either B is periodic or $\langle B \rangle \neq G$.

In the $(\alpha,\beta) = (1,1)$ case $A = \{e,x\}\{e,y\}$ and from the normed factorization $G = B\{e,x\}\{e,y\}$ by Lemma 4 of [1] it follows that $B \subset \langle x^2, y\rangle$ or $B \subset \langle x, y^2\rangle$. Therefore $\langle B \rangle \neq G$.

The $(\alpha,\beta) = (1,2^\lambda-1)$ and $(\alpha,\beta) = (2^\lambda-1,1)$ cases can be settled in a similar manner. So for the sake of definiteness we deal with the $(\alpha,\beta) = (1,2^\lambda-1)$ case. Now $A = \{e,x,y,xy^{-1}\}$. Note that y and xy^{-1} span G and their product is x. This reduces the problem to the previous case.

This completes the proof.

4. Open problems

We close with five open problems. Does Theorem 1 holds in a more general setting? Namely, does Theorem 1 hold for groups that are direct products of two cyclic groups but the orders of the groups are not necessarily equal? We spell out this question more formally.

Problem 1. Let G be a group of type $(2^\lambda, 2^\mu)$ and let $G = AB$ be a normed factorization with $|A| = 4$, $\langle A \rangle = G$. Does it follow that B is periodic?

In the next problem we ask if the condition that $|A| = 4$ is essential?

Problem 2. Let G be a group of type $(2^\lambda, 2^\mu)$ and let $G = AB$ be a normed factorization of G. Does it follow that either A or B does not span the whole G?

Is it true in more general replacing 2 by a prime p?

Problem 3. Let G be a group of type (p^λ, p^μ) and let $G = AB$ be a normed factorization of G. Does it follow that either A or B does not span the whole G?

In Sands' theorem both of the two factors have four elements. Can we extend Sands' theorem for more than two factors?

Problem 4. Let G be a finite abelian 2-group and let $G = A_1 \cdots A_n$ be a normed factorization of G such that each $|A_i|$ is either 2 or 4. Does it follow that at least one of the factors is periodic?

In Sands' theorem the group is a direct product of two cyclic groups of order four. Can we extend Sands' theorem for groups that are direct products of more than two cyclic groups of order four?

Problem 5. Let G be a group of type $(2^{\lambda_1}, \dots, 2^{\lambda_s})$, where $1 \leq \lambda_1, \dots, \lambda_s \leq 2$ and let $G = A_1 \cdots A_n$ be a normed factorization of G, where each $|A_i| = 4$ or $|A_i| = 2$. Does it follow that at least one of the factors is periodic?

References

[1] K. Corrádi and S. Szabó, *On the algebraic form of Keller's conjecture*, Beiträge Algebra Geometrie 30 (1990), 17–34.

[2] A. D. Sands, *On the factorization of finite abelian groups*, Acta Math. Hungar. 8 (1957), 65–86.

[3] A. D. Sands, *The factorization of abelian groups*, Quart. J. Math. Oxford 10 (1959), 81–91.

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

DEPARTMENT OF GENERAL SCIENCES AND MATHEMATICS
COLLEGE OF HEALTH SCIENCES
P. O. BOX 12
MANAMA, STATE OF BAHRAIN

Received August 9, 1999.