Mathematica Pannonica
20/1 (2009), 1–5

A NOTE ON DISTORTED CYCLIC SUBSETS

A. D. **Sands**

Department of Mathematics, Dundee University, Dundee DD1 4HN, Scotland

Received: February 2009??

MSC 2000: 20 K 01

Keywords: Finite abelian groups, factorizations, cyclic subsets.

Abstract: In their paper [1] Corrádi and Szabó show how certain results on cyclic subsets may be extended to distorted cyclic subsets. In this note a shorter proof of one of their results is given and it is shown that a distorted cyclic factor must be a subgroup. It is then shown that distorted cyclic factors may be added to the types of factors called admissible in [2] and still obtain the result given there.

1. Introduction

We shall use the definitions and notations of [1]. We recall that a cyclic subset of an abelian group is a subset of the form $\{e, a, \dots, a^{r-1}\}$, where the order of a is at least equal to r. If $r > 2$ and one element of the cyclic subset, other than e, is replaced by an element of the group not already present then the new subset is called a distortion of the original cyclic subset. We note that when $r = 2$ every replacement would already be cyclic and so we simply use the original cyclic subset. In Lemma 1 of [1] it is shown that in any factorization of the finite abelian group involving a distorted cyclic subset this set may be replaced by the associated cyclic subset, where $r > 3$. In one case in this proof a rather complicated use

E-mail address: adsands@maths.dundee.ac.uk

of group characters is made but the remaining cases are dealt with in a more straight forward manner. We shall show that a straight forward proof can also be given in this exceptional case. Later in Th. 1 of [1] it is shown that given certain conditions involving distorted cyclic factors one factor must be periodic. In the cyclic case it is known that such a factor is a subgroup. We shall see that this also holds in the distorted cyclic case.

2. Results

The multiplicative notation is used. The product of subsets $A_1, A_2, \ldots, A_r$ of an abelian group G is the subset of all elements of the form $\prod_{i=1}^{r} a_i$, where $a_i \in A_i$ for each i. The product is said to be direct if each such element has a unique expression in this form. If the direct product of these subsets equals G we call this a factorization of the group G. The notation gA is used to denote the set of all elements $\{ga : a \in A\}$ and this subset is called a translate of A. In a factorization each subset A_i may be replaced by $g_i A_i$ for any elements $g_i \in G$. Hence we may and do assume that $e \in A_i$ for each factor A_i. The order of the subset A of G is denoted by $|A|$. In order to avoid trivial cases we assume that $|A_i| > 1$ for each factor A_i of G. The order of an element a is denoted by $|a|$. The subgroup generated by a subset A of G is denoted by $\langle A \rangle$.

A subset A of a group G is said to be cyclic if $A = \{e, a, \ldots, a^{r-1}\}$ where $|a| \geq r$. Clearly A is a subgroup if and only if $|a| = r$. a^r is called the successor element of A. We shall denote this cyclic set by $[a]_r$. If $r = st$ then $[a]_r = [a]_s[a^s]_t$. $[a]_r$ is a subgroup if and only if $[a^s]_t$ is a subgroup. By continuing this procedure we may replace a cyclic subset by a product of cyclic subsets of prime order and the original cyclic subset is a subgroup if and only if one of these subsets of prime order is a subgroup.

A subset A of a group G is said to be periodic if there exists $g \in G$ such that $gA = A$, where $g \neq e$. It is well known and easy to see that a cyclic periodic set is a subgroup and that a periodic set of prime order is a subgroup. We denote the cyclic group of order n by $Z(n)$.

Lemma 1. *If $A = \{e, a, \ldots, a^{r-2}, a^{r-1}d\}$ is a direct factor of a finite abelian group G then it may be replaced by the associated cyclic subset obtained by replacing $a^{r-1}d$ by a^{r-1} in any such factorization, where $r > 2$.*

Proof. Let $G = AB$ be a factorization. Then it suffices to show that $dB = B$. We have $aAB = aG = G$. Since the products are direct upon comparing this with $AB = G$ we obtain that

$$a^{r-1}B \cup a^r dB = B \cup a^{r-1}dB.$$

Since $r > 2$ it follows that $B \cap aB = \emptyset$. Hence we have that $a^{r-1}dB \cap a^r dB = \emptyset$. Therefore from consideration of order we see that $a^{r-1}dB = a^{r-1}B$, as required.

In the case $r = 3$ we have the distorted cyclic set $\{e, a, b\}$. By the above this may be replaced by either of the cyclic sets $A_1 = \{e, a, a^2\}$ or $A_2 = \{e, b, b^2\}$. These need not be the only cyclic sets associated with A. Let $G = Z(12) = \langle c\rangle$. Let $A = \{e, c^2, c^{10}\}$. Then as well as the two cyclic subsets given above we can also use the sets $A_3 = \{e, c, c^2\}$ and $A_4 = \{e, c^5, c^{10}\}$ as cyclic subsets associated with A. If we choose $B = \{e, c\}\{e, c^6\}$ then we see that we have the factorizations $G = AB = = A_1B = A_2B$, but that the products A_3B and A_4B are not direct. Thus Lemma 1 of [1] does not extend to the case $r = 3$ but only to the weaker result that there exists a cyclic subset associated with A which can be used as a replacement for A.

We turn to the case of periodic distorted cyclic factors. It should be noted that periodic distorted cyclic subsets need not be subgroups. For example if $G = Z(6) = \langle a\rangle$ then $A = \{e, a, a^3, a^4\}$ is a distorted cyclic subset with period a^3 but is clearly not a subgroup. Since $|A| = 4$ and $|G| = 6$ it is clear that A is not a factor of G.

Theorem 1. *If G is a finite abelian group and A is a periodic distorted cyclic factor of G then A is a subgroup of G.*

Proof. Let $A = \{e, a, \dots, a^{k-1}, a^k d, a^{k+1}, \dots, a^{r-1}\}$. Since periodic sets of prime order are subgroups we may assume that $r > 3$. Let $A_1 = = \{e, a, \dots, a^{k-1}\}$ and let $A_2 = \{a^{k+1}, \dots, a^{r-1}\}$. Let g be a period of A. Since $r > 3$ there exist u, v such that $ga^u = a^v$. Hence $g \in \langle a\rangle$. Since $ga^k d \in A\{a^k d\}$ it follows that $a^k d \in \langle a\rangle$. Let $a^k d = a^m$ and let $|a| = n$. Then we have that $r \le m \le n - 1$. If $(r + 1) \le m \le (n - 2)$ then either A_1 or A_2 must have order 1 and g must be a period of the other set A_i. However A_1 is a cyclic set which is clearly not a subgroup. Hence A_1 cannot be periodic. A similar argument applies to $a^{-(k+1)}A_2$ and so to A_2. Thus we must have either $a^k d = a^r$ or $a^k d = a^{-1}$. In the first case we must have $gA_1 = A_2 \cup a^r$ and so $g = a^{k+1}$. We must also have $g^2 = e$ as A_1 is not periodic. In the second case we have similar results for the set aA with $g = a^{k+2}$. We note that the combined case with $r = m = n - 1$ cannot occur as A is then a translate of a cyclic set of order $n - 1$, which would give rise to a factor of order $n - 1$ in a group of order n.

In the first case we have that $|A_1| = |A_2| + 1 = k$. Hence $|A| = 2k$ and $|a| = |\langle a\rangle| = 2k + 2$. Now as A is a factor of G we have a subset B of G such that $G = AB$ is a factorization. Since $A \subset \langle a\rangle$ it follows that $\langle a\rangle = A(\langle a\rangle \cap B)$. This implies that $2k$ divides $2k + 2$. This is false. In the second case we have that $|A_1| = |A_2| - 1 = k$. Hence $|A| = 2k+2$ and $|a| = |\langle a\rangle| = 2k + 4$. This gives that $2k + 2$ divides $2k + 4$ which is false. So while these sets are periodic distorted cyclic subsets they cannot be factors of G. The only possibility is that A is cyclic and so is a subgroup of G.

In [2] the concept of an admissible subset is introduced. A factor A of a finite abelian group is said to be admissible if it belongs to one or more of the following types.

Type 1: A has prime order;

Type 2: A is k-simulated, where $k \leq p - 2$, and p is the least prime divisor of $|A|$;

Type 3: A is k-simulated, where $k \leq p - 1, p$ is the least prime divisor of $|A|$ and G_p is cyclic;

Type 4: A is simulated and A has even order.

A is k-simulated means that there is a subgroup H such that $|A| = |H| \leq |A \cap H| + k$. In the case where $k = 1$ the set is said to be simulated. We should note that by implication cyclic factors are covered here as they can be expressed as a product of factors of prime order such that the cyclic set is a subgroup if and only if one of these factors of prime order is a subgroup. In [2, Th. 2] it is shown that if a finite abelian group is a product of admissible factors then one of the factors must be a subgroup. We now show that we can add distorted cyclic subsets to the type of factors allowed and still obtain this result.

Theorem 2. *If a finite abelian group is factorized as a product of admissible subsets and distorted cyclic subsets then one of these factors must be a subgroup.*

Proof. Let G have such a factorization. We proceed by induction on the number of factors which are not admissible. If every factor is admissible then the result is just Th. 2 of [2]. Now suppose that the result holds when fewer than m factors are not admissible. Suppose that in the above factorization m factors are not admissible and so these factors must be distorted cyclic factors. By Lemma 1 of [1] each of these factors may be replaced by a corresponding cyclic subset. We note that we do not have to consider factors of order 2 or 3 as they are of Type 1 and so are admissible. When we have made these m replacements we may express each cyclic factor as a product of cyclic factors of prime order. We now have a factorization in which all the factors are admissible. By Th. 2 of [2] one of these factors is a subgroup. If one of the new subsets of prime order is a subgroup then the cyclic subgroup of which it is a factor here is also a subgroup. This implies that the original factor associated with this cyclic subgroup is simulated and so is admissible. This would leave only $m-1$ non-admissible factors and so by the inductive assumption the required result would hold. The only other alternative is that one of the original admissible factors is a subgroup.

References

[1] CORRÁDI, K. and SZABÓ, S.: Direct products of subsets in a finite abelian group.

[2] CORRÁDI, K., SANDS A. D. and SZABÓ, S.: Factoring by simulated subsets II, *Communications in Algebra* **27** (1999), 5367–5376.