International Electronic Journal of Algebra
Volume 3 (2008) 83-95

A GENERALIZATION OF HAJÓS' THEOREM

A.D. Sands

Received: 13 April 2007; Revised: 15 June 2007
Communicated by Abdullah Harmancı

Abstract. Hajós' Theorem states that if a finite abelian group is expressed as a direct product of cyclic subsets, then one of these subsets must be a subgroup. Here factorizations are considered in which one of the factors is not assumed to be cyclic but has certain restrictions on its order placed upon it.

Mathematics Subject Classification (2000): 20K01
Keywords: factorization, abelian group, cyclic subset

1. Introduction

Hajós [4] solved a classical problem of Minkowski by very surprisingly reducing it to a problem involving the factorization of a finite abelian group into a product of cyclic subsets and then showing that one of these subsets must be a subgroup. Any cyclic subset can be expressed as a product of cyclic subsets of prime order. Rédei [5] generalized Hajós' Theorem by showing that the desired result holds if one assumes only that the factors have prime order and that they need not be assumed to be cyclic. Examples of de Bruijn [1] show that in Rédei's Theorem it is not possible in general to weaken this condition even for just one factor. Szabó [9] has asked whether this might be done in relation to Hajós' Theorem. The examples of de Bruijn show that this is not possible if the exceptional factor has order divisible by pqr where p, q, r are primes which need not be distinct. This leaves open the case where the exceptional factor has order pq. In this paper this question is considered but it is assumed that the primes p and q are distinct. There is one unsolved case involving factors of order 2, but a positive answer is obtained in all other cases.

In the proofs the concept of a simulated subset also arises. So these subsets are also considered along with cyclic subsets and the positive results are obtained for the two types of subset taken together modulo the above exception. Positive results have been given in all cases for simulated sets considered on their own in [7] . The case $p = q$ is also covered in these cases. Finally examples are given of some families of finite abelian groups where in the case of cyclic subsets no restriction is needed on the order of the exceptional factor. It is shown that these families contain all the groups with this property.

2. Preliminaries

Throughout the paper the word 'group' will be used to mean 'finite abelian group'. The multiplicative notation is used. The product of subsets $A_1, A_2, \ldots, A_r$ of a 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 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 proceedure we may replace a cyclic subset by a product of cyclic subsets of prime order.

A subset A of a group G is said to be simulated by a subgroup H of G if $|A| = |H| \leq |A \cap H| + 1$ and $|A| > 2$. Equivalently either $A = H$ or A and H differ in one element only. In this latter case there exists $h \in H$ and $g \in G, g \notin H$ such that $A = (H \setminus \{h\}) \cup \{gh\}$. g is called the distorsion element of A with respect to H. If $|A| > 4$ then the simulating subgroup must be unique as two such subgroups of order n would intersect in a subgroup of order $n-2$, but for $n = 3$ or 4 more than one simulating subgroup may exist.

A subset A of a group G is said to be periodic if there exists a non-identity element g of G such that $gA = A$. The set H of these periods, together with e, forms a subgroup of G. Clearly A is a union of cosets of H. Equivalently there exists a subset D such that $A = HD$, where D is non-periodic. A cyclic subset is periodic if and only if it is a subgroup. A simulated subset is periodic if and only if it is equal to its simulating subgroup, which in this case must be unique.

If $G = A_1 A_2 \cdots A_r$ is a factorization in which $A_1 = HD_1$ then we obtain a factorization of the quotient group G/H. If, again, one factor is periodic this process may be continued. In [6] formulae are given to obtain all such factorizations whenever this process continues at each stage, except in the case of elementary 2-groups.

The cyclic group of order n is denoted by $Z(n)$. If $n = p_1^{e_1} \cdots p_k^{e_k}$, where $p_1, \ldots, p_k$ are distinct primes, then we define $e(n) = \sum e_i$. If p is a prime then G_p denotes the p-component of G and $G_{p'}$ denotes the complementary subgroup to G_p in G. If $a \in G$ then $(a)_p$ denotes the G_p component of a and $(a)_{p'}$ denotes the complementary component in $G_{p'}$.

When dealing with these problems Rédei [5] introduced the use of group characters. If χ is a character of a group G and A is a subset of G then $\chi(A)$ is defined to be the complex number $\sum_{a \in A} \chi(a)$. If $G = A_1 \cdots A_r$ is a factorization of G then it is easily seen that $\chi(G) = \chi(A_1) \cdots \chi(A_r)$. If χ is not the unity character then $\chi(G) = 0$ and so there exists i such that $\chi(A_i) = 0$.

Rédei used these group characters to introduce the notion of replaceability of factors. A factor A of a group G is said to be replaceable by a subset D if whenever $G = AB$ is a factorization so also is $G = DB$. He showed that if $|A| = |D|$ and for each character χ of G, $\chi(A) = 0$ implies $\chi(D) = 0$ then A is replaceable by D. The following replacement results are known. A cyclic factor $[a]_p$, where p is prime, may be replaced by its p-component $[(a)_p]_p$. If this replacement is not a subgroup we shall refer to the original factor as a cyclic subset of the first kind. If the p-component of a cyclic factor of order p is a subgroup we shall refer to the original factor as a cyclic subset of the second kind. In this case if the original factor is not contained in G_p it is known [2, Lemma 2] that it may be replaced by a simulated subset which is not a subgroup provided that its order is at least equal to 3. It may also be assumed that the distorsion element has prime order q where $q \neq p$. A simulated factor may be replaced by its simulating subgroup.

The following results on periodicity are known. If $[a]_r\, B = G$ is a factorization then $a^r B = B$. This follows by comparing this factorization with $a[a]_r B = aG = G$. So the successor element of a cyclic factor which is not a subgroup is a period of the other factor B. If $AB = G$ is a factorization and A is simulated with simulating subgroup H and distorsion element g then $gB = B$. This follows by comparing the original factorization with $G = HB$. So if A is simulated but is not a subgroup then B is periodic.

We present the next result formally, since we shall need only this special case of a previous result.

Lemma 1. *If a group G is factorized as $G = A_1 \cdots A_n$, where each factor is either a simulated subset or is a subset of prime order then one of the factors is a subgroup of G.*

Proof. This is a special case of Theorem 2 of [3]. □

Lemma 2. *If B and D are subsets of a group G with empty intersection and if the direct products $[a]_p B$ and $[a]_p D$ are equal, where $a \in G$ and p is prime, then $a^p B = B$ and $a^p D = D$.*

Proof. In the integer group ring $Z(G)$ from $[a]_p B = [a]_p D$ we obtain that

$$(e + a + \cdots + a^{p-1}) \sum_{b \in B} b = (e + a + \cdots + a^{p-1}) \sum_{d \in D} d.$$

Upon multiplying by $e - a$ and rearranging we obtain that

$$\sum_{b \in B} b + a^p \sum_{d \in D} d = \sum_{d \in D} d + a^p \sum_{b \in B} b.$$

Since $B \cap D = \emptyset$ it follows that $a^p B = B$ and that $a^p D = D$. □

3. General Results

Theorem 1. *Let $A_1, \ldots, A_m$ be subsets of a group G each of which is either cyclic or simulated but not equal to a subgroup of G. Suppose that the product $A = A_1 \cdots A_m$ is direct and is a direct factor of G of prime index. Then there is precisely one factor B of G such that $G = AB$ and B is a subgroup of G generated either by the successor element of one of the cyclic factors or by the distorsion element of one of the simulated factors.*

Proof. We may assume that the cyclic subsets have prime order. It follows from Lemma 1 that such a factor B must be periodic and so, as B has prime order, it must be a subgroup. If $m = 1$ then the result is already known. So we may proceed by induction on m. For each i let f_i denote either the successor element of the cyclic factor A_i or the distorsion element of the simulated factor A_i. From the factorization $G = BA_1 \cdots A_m$ we obtain the factorization

$$G/B = (A_1 B/B) \cdots (A_m B/B).$$

Here again one factor must be periodic and so, as it is cyclic or simulated, it must be a subgroup. We may then repeat this process and eventually by renumbering the factors, if necessary, we obtain an ascending chain of subgroups

$$B, BA_1, \ldots, BA_1 \cdots A_{m-1} = L, G.$$

Since BA_1 is a subgroup it follows as above that $B = \langle f_1 \rangle$. Since $A_i \subset L, 1 \leq i \leq m-1$ and L is a subgroup it follows that $f_i \in L$. $LA_m = G$ implies that f_m is a period of L and so that $f_m \in L$.

Now let us suppose, for some subgroup H of G, that $G = AH$ is a factorization. As above it follows that $H = \langle f_k \rangle$ for some k. From this it follows that $H \subset L$. Then the product $HA_1 \cdots A_{m-1}$ is direct and is contained in L,. Since $|H| = |B|$ it follows that this product equals L. By the inductive assumption it follows that $H = B$. □

We should note that the simulating subgroup and distorsion element need not be uniquely determined for certain subsets of small order. This result implies that in the above circumstance the subgroup generated by the distorsion element is unique.

Theorem 2. *Let $A_1, ..., A_m$ be cyclic subsets of a group G which are not subgroups of G. Suppose that the product $A = A_1 \cdots A_m$ is direct and that there is a factorization $G = AH$ where H is a subgroup of G. Then if B and D are subsets of G such that $AB = AD$, where these products are direct, and $|B|$ is less than the least prime factor of $|G|$ it follows that $B = D$.*

Proof. From $G = HA_1 \cdots A_m$ we obtain as before in a renumbering an ascending chain of subgroups $H, HA_1, ..., HA_1 \cdots A_m$. Let $A_r = [a_r]_{m_r}$. Since A_r gives rise to a subgroup in $HA_1 \cdots A_r/HA_1 \cdots A_{r-1}$ it follows that $a_r^{m_r} \in HA_1 \cdots A_{r-1}$.

First let us suppose that $m = 1$. Let the subsets X, Y be the complements of $B \cap D$ in B and D respectively. Then $A_1X = A_1Y$. By Lemma 2 it follows that $a_1^{m_1}$ is a period of X. Since A_1 is not a subgroup it follows that X, if non-empty, has order at least equal to the order of $a_1^{m_1}$. This contradicts the definition of B. Hence X and also Y are empty and so $B = D$.

We proceed by induction on m.

Now let X and Y denote the complements of $A_2 \cdots A_mB \cap A_2 \cdots A_mD$ in $A_2 \cdots A_mB$ and $A_2 \cdots A_mD$ respectively. Then $A_1X = A_1Y$. By Lemma 2 it follows that $a_1^{m_1}$ is a period of X. Let this period have order k. Then $a_1^{m_1r}$ is a period of X for $r < k$. For each $x \in X$ we can express $a_1^{m_1r}x$ as $a_{2,r} \cdots a_{m,r}b_r$ where $a_{i,r} \in A_i$ and $b_r \in B$. Suppose for $r < s$ that $b_r = b_s$. Then

$$a_{2,s} \cdots a_{m,s} = a_1^{m_1(s-r)}a_{2,r} \cdots a_{m,r}.$$

Now $a_1^{m_1} \in H$ and the product $HA_2 \cdots A_m$ is direct. This implies that $a_1^{m_1(s-r)} = e$, which is false. It follows that the elements b_r, $0 \leq r < k$ are distinct and so that $k \leq |B|$. This contradicts the definition of B. Hence X and also Y are empty sets and so $A_2 \cdots A_mB = A_2 \cdots A_mD$. Now HA_1 is a subgroup which has all the requisite properties with respect to the above products. By the inductive assumption it follows that $B = D$. $\square$

Theorem 3. *Let a group G be a direct product of cyclic subsets of the first kind and of a subset D of order pq, where p and q are distinct primes. Then the subset D is periodic.*

Proof. We may assume that the generator of each cyclic subset of the first kind has order equal to a power of r, where r is prime and is the order of the subset. If such a cyclic subset exists for which r is different from p and from q then by consideration of the orders involved it follows that the product of all the cyclic subsets of order r is equal to G_r. Hajós Theorem then applies to this situation and shows that one of these cyclic subsets is a subgroup and so is not of the first kind. Thus we may suppose that $|G| = p^s q^t$ and that $G = A_1 \cdots A_{s-1} B_1 \cdots B_{t-1} D$, where each A_i has order p and each B_j has order q. By replacement results we may also assume that each A_i is contained in G_p and that each B_j is contained in G_q.

Let $A = A_1 \cdots A_{s-1}$ and $B = B_1 \cdots B_{t-1}$. Since $A \subset G_p$ it follows, for each $f \in G_q$, that $A(BD \cap G_p f) = G_p f$ and so that $A(BDf^{-1} \cap G_p) = G_p$. Now $(BDf^{-1} \cap G_p)$ need not contain e but there exists $g_f \in G_p$ such that $(BDf^{-1} \cap G_p)g_f$ does contain e. By Theorem 1 it follows that there exists a subgroup H of G_p, which is independent of f, such that $(BDf^{-1} \cap G_p)g_f = H$. Since $BD = \bigcup_{f \in G_q}(BD \cap G_p f)$ it follows that H is a group of periods of BD. H has order p and so has a generator h.

Let $d_1, \ldots, d_r$ be the set of all elements in D such that $(d_i)_p \in A$. Since h^k is a period of BD it follows that $h^k D \subseteq BD$. Thus $h^k d_i = bd$ for some $b \in B, d \in D$. Then we have that $(d)_p = h^k (d_i)_p \in h^k A$. Since the converse holds on multiplication by h^{-k} it follows that there are exactly r elements in D whose p-components belong to $h^k A$, $0 \leq k < p$. Hence $pq = |D| = pr$ and so $r = q$.

We consider first the case where the elements $d_1, \ldots, d_q$ all have the same p-component. So let $(d_i)_p = a, 1 \leq i \leq q$. Then there are exactly q elements in D whese p-components are equal to $h^k a$, for each k. Let this set of elements be $h^k f_i, 1 \leq i \leq q$, where $f_i \in G_q$. Since the product BD is direct it follows that the product $B\{f_1, \ldots, f_q\}$ is direct and, from consideration of order, it must equal G_q. By Theorem 1 there is a subgroup K which is independent of k such that $\{f_1, \ldots, f_q\}$ is a translate of K. Since D is the union of the subsets $h^k a\{f_1, \ldots, f_q\}$ it follows that K is a group of periods of D.

We now consider the other case where the number of elements d_i with equal p-components is less than q. By renumbering we may assume that $(d_1)_p = \cdots = (d_m)_p = a \in A$, where $m < q$. As above, for each k there are exactly m elements of D with p-component equal to $h^k a$. Let $d_i = af_i$. Then $f_i \in G_q$. Since $h^k af_i \in BD$ there exist elements $b_i \in B, 1 \le i \le m$, such that $h^k af_i(b_i)^{-1} \in D$. As $B \subseteq G_q$ the only elements in BD with p-component equal to $h^k a$ are exactly those in the subset $h^k a\{f_1(b_1)^{-1}, \ldots, f_m(b_m)^{-1}\}B$. Since h^k is a period of BD it follows that the elements of the subset $h^k a\{f_1, \ldots, f_m\}B$ are in BD and have p-component $h^k a$. It follows that

$$\{f_1(b_1)^{-1}, \ldots, f_m(b_m)^{-1}\}B = \{f_1, \ldots, f_m\}B.$$

Since $B(AD \cap G_q) = G_q$ and, by Theorem 1, $AD \cap G_q$ is a subgroup of G_q the conditions of Theorem 2 are satisfied. It follows that

$$\{f_1(b_1)^{-1}, \ldots, f_m(b_m)^{-1}\} = \{f_1, \ldots, f_m\}.$$

Suppose that $f_i = f_j(b_j)^{-1}$ and hence that $af_ib_j = af_j$. Now b_j is in B and af_i and af_j are in D. It follows that $i = j$ and that $b_j = e$.

Thus the elements $h^k af_i$ belong to D for $0 \le k < p$. Thus this subset of elements of D has H as a group of periods. Since $m < q$ implies that D is a union of such subsets it follows that H is a group of periods of D. □

Theorem 4. *If a group G is a direct product of cyclic subsets of the first kind, of simulated subsets and a subset of order pq, where p and q are distinct primes, then one of the factors is periodic.*

Proof. The cyclic subsets may be assumed to belong to the primary component of G corresponding to their order. Let $G = A_1 \cdots A_m D$, where D has order pq and the other sets are either cyclic of the first kind or simulated. If no simulated subset occurs then the result follows by Theorem 3. So we may assume that A_1 is simulated with simulating subgroup H_1 and distorsion element g_1.

The result is known to be true if $m = 1$. So we may proceed by induction on m.

We may replace A_1 by H_1 and so obtain a factorization

$$G/H_1 = (A_2H_1/H_1) \cdots (A_mH_1/H_1)(DH_1/H_1)$$

of the quotient group. By the inductive assumption it follows that either some subset A_iH_1/H_1 is a subgroup or that DH_1/H_1 is periodic. In the first case A_iH_1 is a subgroup of G. In the second case there is a subgroup D_1H_1/H_1 and a subset D_2H_1/H_1 such that $DH_1/H_1 = (D_1H_1/H_1)(D_2H_1/H_1)$. The subsets D_1 and

D_2 of G are not uniquely determined but we may suppose that $|D_1| = p, |D_2| = q$ and that they have been chosen to be subsets of D. As before this process may be repeated to obtain an ascending chain of subgroups

$$H_1, H_1A_2, \ \ldots \ , H_1A_2 \cdots A_{r-1}, H_1A_2 \cdots A_{r-1}D_1, \ldots$$

until a subgroup L is reached such that $LX = G$ where either $X = A_m$ or $X = D_2$.

There are now four cases to be considered depending on whether $X = A_m$ or $X = D_2$ and on whether or not $g_1 \in L$.

Firstly let us suppose that $X = A_m$ and that $g_1 \in L$. Then we have that $A_1 \subseteq L$ and as D_1, D_2 are contained in L we have that $D \subseteq L$. Then the product $A_1 \cdots A_{m-1}D$ is direct, is contained in L and has order equal to that of L. Hence it is equal to L and the result follows by the inductive assumption.

Secondly let us suppose that $X = D_2$ and that $g_1 \in L$. Then for each $f \in D_2$ it follows from $A_1 \subseteq L$ that $A_1 \cdots A_m(D \cap Lf) = Lf$. Again by Theorem 1 it follows that there is a subgroup K which is independent of f such that $D \cap Lf$ is a translate of K. Since $D = \bigcup_{f \in D_2}(D \cap Lf)$ it follows that K is a group of periods of D.

Now we turn to the cases in which $g_1 \notin L$. From $LX = G$ it follows that $LXx^{-1} = G$ for each $x \in X$. Hence there exists $b_x \in X$ such that $(g_1)^{-1} \in Lb_xx^{-1}$. If $g_1b_x = x$ for all $x \in X$ then X is periodic. In this case we may assume that $X = D_2$. D_2 has prime order and so must be a subgroup and contain its period g_1. If this is so we can use D_2 rather than D_1 at the stage where $H_1A_1 \cdots A_{r-1}D$ was being considered. This would lead to a new subgroup L' instead of L with $g_1 \in L'$. Now the arguments from one of the first two cases apply and achieve the desired result.

Thus we may assume that there exists $f \in X$ such that $g_1b_f \neq f$. Now we form a set B_f from A_1 by replacing the distorsion element g_1 by $g_1b_ff^{-1}$ but making no other changes. Then B_f is also simulated by H_1 and, since $|H_1| \geq 3$, B_f cannot be a subgroup. We note also that $B_f \subseteq L$.

The third case to be considered is that in which $X = A_m$ and $g_1 \notin L$. We claim that the product $B_fA_2 \cdots A_{m-1}D$ is direct. Since the product obtained by replacing B_f here by H_1 is direct we need consider only the case where $ha_2 \cdots a_{m-1}d = h_1g_1b_ff^{-1}a'_2 \cdots a'_{m-1}d'$, where $h \in H_1 \cap A_1,\ a_i, a'_i \in A_i, d, d' \in D$. This leads to $ha_2 \cdots a_{m-1}fd = h_1g_1a'_1 \cdots a'_{m-1}b_fd'$. Since each side belongs to $A_1 \cdots A_mD$ we have the contradiction $h = h_1g_1$. Thus the above product is direct. Since each term is contained in L it follows by consideration of order that $B_fA_2 \cdots A_{m-1}D = L$. The desired result follows by the inductive assumption.

Finally we consider the fourth case in which $g_1 \notin L$ and $X = D_2$. For each $x \in D_2$ we claim that the product $B_f A_2 \cdots A_m(D \cap Lx)$ is direct. Since the product $A_1 A_2 \cdots A_m D$ is direct we need only consider the case

$$ha_2 \cdots a_m lx = h_1 g_1 b_f f^{-1} a_2' \cdots a_m' l' x$$

where $h \in A_1 \cap H_1, a_i, a_i' \in A_i, l, l' \in L$. This leads to

$$ha_2 \cdots a_m lf = h_1 g_1 a_2' \cdots a_m' l' b_f.$$

Since the product LD_2 is direct this implies that $f = b_f$, which is false. Hence the above product is direct.

We may assume that $|D_1| = p, |D_2| = q$. From $B_f A_2 \cdots A_m(D \cap Lx)x^{-1} \subseteq L$ it follows that $|D \cap Lx| \leq p$ for each $x \in D_2$. Since $D = \bigcup_{x \in D_2}(D \cap Lx)$ it follows that $pq = |D| = \Sigma_{x \in D_2}|D \cap Lx|$. Hence $|D \cap Lx| = p$ and so $B_f A_2 \cdots A_m(D \cap Lx)x^{-1} = L$. By the inductive assumption and by Theorem 1 there is a subgroup M, which is independent of x, such that $D \cap Lx$ is a translate of M. As before it follows that M is a group of periods of D. □

When we consider cyclic subsets of the second kind no problem arises if the order is at least three. These cyclic subsets can be replaced by simulated subsets. However a problem arises for any cyclic subsets of the second kind which are of order two. Let A_1 be such a subset, where $A_1 = \{e, ag\}$ with $|a| = 2$ and $|g|$ odd. Then as a cyclic subset A_1 can be replaced by $H_1 = \{e, a\}$ and g^2 and hence g is a period of the product of the remaining factors. The problem arises when B_f is constructed in the third and fourth cases of Theorem 4. We cannot now assert that B_f is not periodic. It could be another subgroup of order 2 and so the inductive argument breaks down.

So for general cyclic subsets we have the following result.

Theorem 5. *If $G = A_1 \cdots A_m D$ is a factorization of the group G where each subset A_i is either cyclic or simulated and $|D| = pq$, where p, q are distinct primes then one of these factors is periodic provided that no cyclic factor of the second kind of order 2 arises when the cyclic factors are expressed as products of cyclic factors of prime order.*

Let $[a]_n$ be a cyclic factor where $n = 2^k m$ with $k > 0$ and m odd. Then if $|a| = 2^r s$ with s odd every factor of order 2 which arises in the expression as a product of cyclic factors of prime order will have 2-component of order at least 4 if $r > k$ but if $r = k$ the final factor of order 2 which arises will be of the second kind.

It is clear that the conclusion of Theorem 5 must hold if G has odd order. It is also true that the conclusion holds if the 2-component of G is cyclic. In this case G cannot have two distinct subgroups A_1 and B_f of order 2 and the proof of Theorem 4 goes through without change.

4. Special Results

We now consider those groups where no restriction on the order of the exceptional factor is needed but we restrict our attention to cyclic subsets for the other factors.

Definition. *Let $\mathcal{C}$ denote the set of all groups with the property that in any factorization into a product of cyclic subsets together with one other subset at least one factor must be periodic.*

As usual we may assume that the cyclic subsets have prime order. For each prime p it is clear that elementary p-groups belong to $\mathcal{C}$ since any cyclic subset of order p is a subgroup.

Theorem 6. *If G is a group such that $e(|G|) \leq 4$ then G belongs to $\mathcal{C}$.*

Proof. If $e(|G|) = 1$ then there is nothing to prove.

If $e(|G|) = 2$ then only one cyclic factor can arise and the result is known.

If $e(|G|) = 3$ then either there is only one cyclic factor or every factor has prime order. In each case the result is known.

Let $e(|G|) = 4$. If there is only one cyclic factor or if there are three cyclic factors the result follows as in the previous case. So we may suppose that $G = A_1A_2D$ where the first two factors are cyclic of prime order and $e(|D|) = 2$. Let $A_1 = [a]_p$ and $A_2 = [b]_q$. Let $H = \langle a^p \rangle$, $K = \langle b^q \rangle$ and $L = \langle a, b \rangle$. We may assume that neither H nor K equals $\{e\}$ and thus that $e(|L|)| > 2$.

Suppose first that $e(|L|) = 3$. Let B be a complete set of coset representatives for G modulo L. Then, for each $b \in B$, $A_1A_2(D \cap Lb) = Lb$. As before this implies by Theorem 1 that there exists a subgroup M of G which is independent of b such that $D \cap Lb$ is a translate of M. This implies that M is a group of periods of D.

Now we may suppose that $L = G$. Let χ be a character of G such that $\chi(A_1) = 0$. Then from $\Sigma_{0 \leq i \leq p-1} \chi(a)^i = 0$ it follows upon multiplication by $1 - \chi(a)$ that $\chi(a^p) = 1$ and so that $\chi(H) \neq 0$. Hence $\chi(H) = 0$ implies that $\chi(A_1) \neq 0$. Similarly we have that $\chi(K) = 0$ implies $\chi(A_2) \neq 0$. It follows that $\chi(H) = \chi(K) = 0$ implies that $\chi(D) = 0$. By [8, Theorem 2] there exist subsets X, Y of G such that $D = HX \cup KY$, where the products are direct and the union is disjoint. Then from $A_1A_2D = G$ and $A_1H = \langle a\rangle, A_2K = \langle b\rangle$ it follows that $G = \langle a\rangle A_2X \cup A_1\langle b\rangle Y$. Suppose that X and Y are both non-empty and that $a^rb^s \in X, a^ub^v \in Y$. Then $a^ub^s = a^{u-r}a^rb^s = b^{v-s}a^ub^v$. This contradicts the fact that the union is disjoint. Hence either X or Y is the empty set and so either K or H is a group of periods of D. $\square$

We now observe that [1, Theorem 1] implies that many groups do not belong to $\mathcal{C}$. If g is a generator of $Z(mn)$ then $A\langle a^m\rangle = \langle g\rangle$ where $A = \{e, a, \ldots, a^{m-1}\}$. Now the construction of de Bruijn shows that if a group G contains a proper subgroup H which is a direct product of subgroups H_1 and H_2 and each of these has a factorization into a product of a subgroup and a non-periodic set then there is a factorization of G into the product of these two non-periodic subsets and a third non-periodic factor. From the remark above if H_1 and H_2 are cyclic subgroups of composite order then the first two non-periodic subsets may be chosen to be cyclic. Thus, in this case, the group G will not belong to $\mathcal{C}$.

Let $e(|G|) > 4$. If $|G|$ is divisible by four distinct primes then G must have a proper subgroup H of type $Z(pq) \otimes Z(rs)$ and so G does not belong to $\mathcal{C}$. If $|G|$ is divisible by three distinct primes then G has either a proper subgroup of the form $Z(p^2) \otimes Z(qr)$ or of the form $Z(pq) \otimes Z(pr)$ and so does not belong to $\mathcal{C}$. If $|G|$ is divisible by two distinct primes p and q then if G contains either a subgroup of the form $Z(p^2) \otimes Z(q^2)$, a subgroup of the form $Z(pq) \otimes Z(pq)$ or a subgroup of the form $Z(p^2) \otimes Z(pq)$ then G does not belong to $\mathcal{C}$. Finally if $|G|$ is a p-group and contains a subgroup of the form $Z(p^2) \otimes Z(p^2)$ then G does not belong to $\mathcal{C}$.

In the case of two prime factors of $|G|$ this leaves groups of type $H \otimes K$, where H is a cyclic p-group and K is an elementary q-group. In the case of G being a p-group this leaves only groups of this form, but with $p = q$. We shall now show that all groups of these types do belong to $\mathcal{C}$ and so complete the classification of the groups in $\mathcal{C}$.

Theorem 7. *Let p be a prime and let G be a group of type $Z(p^e) \otimes H$, where H is an elementary p-group. Then G belongs to $\mathcal{C}$.*

Proof. If $e = 1$ then G is an elementary p-group and the result is known. So we may suppose that $e > 1$. Let a be an element in G of order p^e. Then $G = \langle a\rangle \otimes H$. Let $G = A_1 \cdots A_mD$ be a factorization in which each factor A_i is cyclic of order p. Let $A_i = [a^{m_i}h_i]_p$, where $h_i \in H$. If p^{e-1} divides m_i then A_i is a subgroup. So we may suppose that this is not the case.

Let $K = \langle a^{p^{e-1}} \rangle$. Let χ be any character of G such that $\chi(K) = 0$. Then $\chi(a)$ must be a primitive root of unity of order p^e. Then $\chi(A_i) = \Sigma_{0 \le k \le p-1} (\chi(a))^{m_i} \chi(h_i)$. Then as $\chi(h_i)^p = 1$ it follows that $(1 - ((\chi(a))^{m_i} \chi(h_i))\chi(A_i) = 1 - (\chi(a))^{pm_i}$. Since p^e does not divide pm_i it follows that $\chi(A_i) \neq 0$. Hence $\chi(K) = 0$ implies that $\chi(D) = 0$. By [8] it follows that K is a group of periods of D. $\square$

Theorem 8. *Let p and q be distinct primes and let a group G be a direct sum of a cyclic p-group and an elementary q-group. Then G belongs to $\mathcal{C}$.*

Proof. Let $G = L \otimes H$, where $L = Z(p^e)$ and H is an elementary q-group. Let $G = A_1 \cdots A_k B_1 \cdots B_m D$ be a factorization in which each factor A_i is cyclic of order p and each factor B_j is cyclic of order q. Let a be an element of order p^e and let $K = \langle a^{p^{e-1}} \rangle$ be the unique subgroup of G of order p. Let $A_i = [a_i f_i]_p$, where $a_i \in G_p$, $f_i \in G_q$. Let $B_j = [b_j h_j]_q$, where $b_j \in G_p$, $h_j \in G_q$.

Let χ be a character of G such that $\chi(K) = 0$. Then $\chi(a)$ must be a primitive root of unity of order p^e and so the restriction of χ to G_p is bijective. If $\chi(B_j) = 0$ then $\chi(b_j h_j)$ is a primitive root of unity of order q. Hence $\chi(b_j) = 1$ and so $b_j = e$. Thus B_j is a subgroup. Therefore we may assume that $\chi(B_j) \neq 0$.

If for all characters χ of G such that $\chi(K) = 0$ it follows that $\chi(D) = 0$ then by [8] K is a group of periods of D. Thus we may assume that there exists such a character χ_1 and an integer k such that $\chi_1(A_k) = 0$. Then this implies that $\chi_1(a_k)$ has order p and that $\chi_1(f_k) = 1$. Hence $(A_k)_p = K$ and $\chi_1(\langle f_k \rangle) \neq 0$. Each factor A_i may be replaced by $(A_i)_p$. Since the product is still direct it follows that $(A_i)_p \neq K$ for $i \neq k$ and so that $\chi(A_i) \neq 0$ for any character χ with $\chi(K) = 0$. On the assumption that $A_k \neq K$ we obtain that $\chi(K) = 0, \chi(\langle f_k \rangle) = 0$ implies that $\chi(D) = 0$. We may again apply [8] to obtain the existence of subsets X and Y such that $D = KX \cup \langle f_k \rangle Y$, where the products are direct and the union is disjoint. Now we may replace A_k by $(A_k)_p$, which equals K . Since the product $(A_k)_p D$ is direct it follows that $X = \emptyset$. Hence $\langle f_k \rangle$ is a group of periods of D.

This completes the proof and so also the classification of the groups in $\mathcal{C}$. $\square$

Acknowledgment. I should like to thank Professor K. Corrádi for many helpful discussions concerning the problems considered in this paper.

References

[1] N.G. Brujin, *On the factorization of finite abelian groups*, Indag. Math. 15 (1953), 258–264.

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

[3] K. Corrádi, A.D. Sands and S. Szabó, *Factoring by simulated subsets II*, Comm. Algebra, 27 (1999), 5367–5376.

[4] G. Hajós, *Über einfache und mehrfache Bedeckung des n-dimensionalen Raumes mit einem Würfelgitter*, Math. Zeitschrift, 47 (1942), 427–467.

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

[6] A.D. Sands, *Factorization of cyclic groups*, Proc. Coll. Abelian Groups (Tihany), (1964), 139–146.

[7] A.D. Sands, *Factorizations of abelian groups involving simulated factors and one other factor*, Acta Sci. Math. to appear.

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

[9] S. Szabó, *Factoring by cyclic and simulated subsets*, Acta Math. Hungar. 85 (1999), 123–133.

A.D. Sands
Department of Mathematics
Dundee University
Dundee DD1 4HN Scotland
E-mail: adsands@maths.dundee.ac.uk