Mathematica Pannonica
7/2 (1996), 197 – 207

FACTORING ABELIAN GROUPS OF ORDER p^4

Sándor **Szabó**

Department of Mathematics, University of Bahrain, P. O. Box 32038 Isa Town, State of Bahrain

Khalid **Amin**

Department of Mathematics, University of Bahrain, P. O. Box 32038 Isa Town, State of Bahrain

Received: July 1995

MSC 1991: 20 K 01, 52 C 22

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

Abstract: Let G be a finite abelian group of order p^4, where p is a prime. If G is a direct product of three of its subsets A, B, C, where B and C are nonsubgroup cyclic or simulated subsets, then A is a direct product of a subset and a nontrivial subgroup of G.

1. Introduction

Let G be a finite abelian group. We will use multiplicative notation in connection with abelian groups. We denote the identity element by e. Let $A_1, \dots, A_n$ be subsets of G. If the product $A_1 \dots A_n$ is direct and gives G, then we say that the product $A_1 \dots A_n$ is a *factorization* of G. We also call the equation $G = A_1 \dots A_n$ a factorization of G. The above definition is clearly equivalent to the following. Each g in G is uniquely expressible in form

$$g = a_1 \dots a_n, \quad a_1 \in A_1, \dots, a_n \in A_n.$$

Sometimes another equivalent formulation is useful. The product $A_1 \dots$ $\dots A_n$ gives G and in addition $|G| = |A_1| \dots |A_n|$ holds. Here $|A|$ denotes the cardinality of the subset A of G. We also use the notation $|a|$ to denote the order of the element a of G.

The subset A of G is defined to be *periodic* if there is an element $g \in G \setminus \{e\}$ such that $gA = A$. Such an element g is called a *period* of A. All the periods of A together with the identity element e form a subgroup H of G. In fact A is a union of cosets modulo H. Therefore A is a direct product HD, where D is a set of representatives of A modulo H. Clearly D is not necessarily defined uniquely.

Beside periodic subsets two other types of subsets play a role in the paper. The subset A of G is called *cyclic* if it consists of the elements $e, a, a^2, \ldots, a^{r-1}$. In order to avoid trivial cases we will assume that $r \geq$ ≥ 2 and $|a| \geq r$. If $|a| = r$, then the cyclic subset A is equal to the cyclic subgroup $\langle a \rangle$. If $|a| > r$, then A consists of the "first" r elements of $\langle a \rangle$. Let $a \in G$ such that $|a| = r$. The subset A of G is called *simulated* if it consists of the elements $e, a, a^2, \ldots, a^{r-2}, a^{r-1}u$. If $u = e$, then the simulated subset A is equal to the subgroup $\langle a \rangle$. If $u \neq e$, then A differs from the subgroup $\langle a \rangle$ in one element $a^{r-1}u$.

It is proved in [3] that if a finite abelian group is a direct product of cyclic subsets, then at least one of the factors must be periodic. By [1] a similar result holds if the factors are simulated instead of being cyclic. Rédei [4] proved that if a finite abelian group is a direct product of normed subsets of prime cardinality, then at least one of the factors must be a subgroup.

These theorems suggest the following problem. Let $G = AB_1 \ldots B_n$ be a factorization of the finite abelian group G, where each B_i is either cyclic or simulated and $|A|$ is a product of two (not necessarily distinct) primes. Does it follow that at least one of the factors $A, B_1, \ldots, B_n$ is periodic? The main result of this paper gives an answer in the affirmative in a particular case. Namely, let G be a group of order p^4, where p is a prime. If $G = ABC$ is factorization of G, where B and C may be cyclic or simulated, then at least one of the factors A, B, C must be periodic. The emphasis is on that $|A|$ is not a prime and nothing is assumed about the structure of A.

2. Preliminaries

If A and A' are subsets of G such that for every subset B of G, if $G = AB$ is a factorization of G, then $G = A'B$ is also a factorization

G, then we shall say that A is *replaceable* by A'.

We will need the next three lemmas on replaceable factors. They can be proved using the ideas of the proofs of Lemma 1 and 2 in [2].

Lemma 1. *Let G be a finite abelian group and let $A = \{e, a, a^2, \ldots, a^{r-1}\}$ be a cyclic subset of G. Then A can be replaced by $A' = \{e, a^i, a^{2i}, \ldots, a^{(r-1)i}\}$ for each i, whenever i is prime to r.*

Lemma 2. *The simulated subset $A = \{e, a, a^2, \ldots, a^{r-2}, a^{r-1}u\}$ of a finite abelian group can be replaced by $A' = \{e, a, a^2, \ldots, a^{r-2}, a^{r-1}u^i\}$ for each integer i.*

Lemma 3. *The simulated subset $A = \{e, a, a^2, \ldots, a^{r-2}, a^{r-1}u\}$ of a finite abelian group can be replaced by $A' = \{e, a, a^2, \ldots, a^{i-1}, a^i u, a^{i+1}, \ldots, a^{r-1}\}$ for each i, $1 \leq i \leq r-1$.*

At some instances it will be convenient to work in the group ring $\mathbb{Z}(G)$. If G is a finite abelian group, then $\mathbb{Z}(G)$ consists of all the elements $\sum_{g \in G} \lambda_g g$, where λ_g is an integer. Addition and multiplication are defined between such sums in the same fashion as between polynomials. To the subset A of G we assign the element $\overline{A} = \sum_{a \in A} a$ of $\mathbb{Z}(G)$. We will use the next argument several times. Let $G = ABC$ be a factorization of G, where

$$B = \{e, b, b^2, \ldots, b^{r-1}\}, \quad C = \{e, c, c^2, \ldots, c^{s-2}, c^{s-1}v\}.$$

Replace C by $\langle c \rangle$ in the factorization $G = ABC$ to get the factorization $G = AB\langle c \rangle$. This can be done by Lemma 2 with the choice of $i = 0$. The factorizations $G = ABC$ and $G = AB\langle c \rangle$ correspond to the equations $\overline{G} = \overline{ABC}$ and $\overline{G} = \overline{AB\langle c \rangle}$ respectively in the group ring $\mathbb{Z}(G)$. Subtracting the first from the second we get $0 = \overline{AB}(c^{s-1} - c^{s-1}v)$ and so $0 = \overline{AB}(e - v)$. From this by multiplying by $e - b$ we get the equation $0 = \overline{A}(e - b^r)(e - v)$. Now using the ideas in the proof of Th. 2 of [6] we can conclude that there are subsets U, V of G such that $A = U\langle b^r \rangle \cup V\langle v \rangle$, where the union is disjoint and the products are direct. Analogous results hold when both B and C are cyclic or both are simulated. For easier reference we state them as a lemma.

Lemma 4. *Let $G = ABC$ be a factorization of the finite abelian group G, where the factors B and C are one of the following*

$$B = \{e, b, b^2, \ldots, b^{r-1}\}, \qquad C = \{e, c, c^2, \ldots, c^{s-1}\},$$

$$B = \{e, b, b^2, \ldots, b^{r-2}, b^{r-1}u\}, \quad C = \{e, c, c^2, \ldots, c^{s-2}, c^{s-1}v\},$$

$$B = \{e, b, b^2, \ldots, b^{r-1}\}, \qquad C = \{e, c, c^2, \ldots, c^{s-2}, c^{s-1}v\}.$$

Then there are subsets U, V of G such that A can be represented in the following forms respectively

$$A = U\langle b^r\rangle \cup V\langle c^s\rangle, \quad A = U\langle u\rangle \cup V\langle v\rangle, \quad A = U\langle b^r\rangle \cup V\langle v\rangle,$$

where the unions are disjoint and the products are direct.

3. Result

Now we are ready to prove the main result of the paper. By the fundamental theorem of the finite abelian groups each finite abelian group is a direct product of cyclic groups of prime power order. If G is the direct product of cyclic groups of prime power order $t_1, \dots, t_n$ respectively, then we say that G is of *type* $(t_1, \dots, t_n)$.

Theorem 1. *Let p be a prime and G be an abelian group of order p^4. Let $G = ABC$ be a factorization of G, where $|A| = p^2$, $|B| = |C| = p$. Further the factors B and C are cyclic or simulated. Then one of A, B, C is periodic.*

Proof. The type of G be can be

$$(p^4), \quad (p^3, p), \quad (p^2, p^2), \quad (p^2, p, p), \quad (p, p, p, p).$$

We distinguish 5 cases depending on the type of G. Then we distinguish 3 subcases depending on both B and C are cyclic; both B and C are simulated; B is cyclic and C is simulated.

CASE 1. G is of type (p^4). This case is settled by Th. 1 of [5]. If G is a finite cyclic group and $G = A_1 \dots A_n$ is a factorization of G, where each $|A_i|$ is a prime power, then one of the factors is periodic.

CASE 2. G is of type (p^3, p). Let $G = \langle x\rangle \times \langle y\rangle$, where $|x| = p^3$, $|y| = p$.

Subcase 2(a). Both B and C are cyclic, that is,

$$B = \{e, b, b^2, \dots, b^{p-1}\}, \quad C = \{e, c, c^2, \dots, c^{p-1}\}.$$

If $b^p = e$ or $c^p = e$, then we are done and so we assume that $|b| \geq p^2$, $|c| \geq p^2$. By Lemma 4, $A = U\langle b^p\rangle \cup V\langle c^p\rangle$. Let $b = x^\alpha y^\beta$ and $c = x^\gamma y^\delta$ be the basis representations of b and c. Now $b^p = x^{p\alpha}$ and $c^p = x^{p\gamma}$. The subgroups of $\langle x^p\rangle$ form a chain. Hence $\langle x^{p^2}\rangle \subset \langle x^{p\alpha}\rangle \cap \langle x^{p\gamma}\rangle = \langle b^p\rangle \cap \langle c^p\rangle$. Thus x^{p^2} is a period of A.

Subcase 2(b). Both B and C are simulated, that is,

$$B = \{e, b, b^2, \dots, b^{p-2}, b^{p-1}u\}, \quad C = \{e, c, c^2, \dots, c^{p-2}, c^{p-1}v\}.$$

Here $|b| = |c| = p$. If $u = e$ or $v = e$, then we are done and so we assume that $|u| \geq p$, $|v| \geq p$. By Lemma 2 we may assume that $|u| = |v| = p$. The elements of G of order p generate the subgroup $K = \langle x^{p^2}, y\rangle$ of order p^2. Now $K = BC$ is a factorization of K. By Rédei's theorem one of the factors B and C is a subgroup of K.

Subcase 2(c). B is cyclic and C is simulated, that is,

$$B = \{e, b, b^2, \ldots, b^{p-1}\}, \quad C = \{e, c, c^2, \ldots, c^{p-2}, c^{p-1}v\}.$$

Here we may assume that $|b| \geq p^2$ and $|c| = |v| = p$. By Lemma 4, $A = U\langle b^p\rangle \cup V\langle v\rangle$. If $U = \emptyset$ or $V = \emptyset$, then A is periodic and so we assume that $U \neq \emptyset$ and $V \neq \emptyset$. If $|b| = p^3$, then $|U||\langle b^p\rangle| \geq p^2$ and hence $V = \emptyset$. We assume that $|b| = p^2$. Therefore $\langle b^p\rangle = \langle x^{p^2}\rangle$. If $v \in \langle x^{p^2}\rangle$, then $\langle v\rangle = \langle x^{p^2}\rangle$ and so A is periodic. Thus we assume that $v \notin \langle x^{p^2}\rangle$.

Replace C by $\langle c\rangle$ in the factorization $G = ABC$ to get the factorization $G = AB\langle c\rangle$. Let us compute $A\langle c\rangle$.

$$A\langle c\rangle = \Big(U\langle x^{p^2}\rangle \cup V\langle v\rangle\Big)\langle c\rangle = U\langle x^{p^2}\rangle\langle c\rangle \cup V\langle v\rangle\langle c\rangle.$$

The product $AB\langle c\rangle$ is direct so the products $\langle x^{p^2}\rangle\langle c\rangle$ and $\langle v\rangle\langle c\rangle$ must be direct. They both must be equal to K. Note that x^{p^2}, v form a basis for K. By Lemma 3 in C c can be replaced by c^i for each i, $1 \leq i \leq p-1$, so we have $p-1$ choices for c. Namely, c may be $x^{p^2}v^i$, $1 \leq i \leq p-1$. Now

$$C = \{e, x^{p^2}v^i, x^{2p^2}v^{2i}, \ldots, x^{(p-2)p^2}v^{(p-2)i}, x^{(p-1)p^2}v^{(p-1)i+1}\}.$$

There is a j such that $1 \leq j \leq p-2$ and $ji \equiv (p-1)i + 1 \pmod{p}$ since $(j+1)i \equiv 1 \pmod{p}$ is solvable. Let $t \in U$. The product $t\langle x^{p^2}\rangle C$ is direct since it is part of ABC. Compute $\langle x^{p^2}\rangle C$. Note that the sets

$$\langle x^{p^2}\rangle x^{jp^2}v^{ji} = \langle x^{p^2}\rangle v^{ij} \text{ and } cl\langle x^{p^2}\rangle x^{(p-1)p^2}v^{(p-1)i+1} = \langle x^{p^2}\rangle v^{(p-1)i+1}$$

are parts of $\langle x^{p^2}\rangle C$ and they have the same elements. This is a contradiction.

CASE 3. G is of type (p^2, p^2). Let $G = \langle x\rangle \times \langle y\rangle$, where $|x| = p^2$, $|y| = p^2$.

Subcase 3(a). Both B and C are cyclic, that is,

$$B = \{e, b, b^2, \ldots, b^{p-1}\}, \quad C = \{e, c, c^2, \ldots, c^{p-1}\}.$$

If $b^p = e$ or $c^p = e$, then we are done and so we assume that $|b| = p^2$, $|c| = p^2$. Let $L = \langle b\rangle$. If $c \in L$, then $L = BC$ is a factorization of L and so by Rédei's theorem one of the factors is a subgroup of L. Thus we may assume that $c \notin L$. We may choose x, y to be b, c respectively. Now

$$B = \{e, x, x^2, \ldots, x^{p-1}\}, \quad C = \{e, y, y^2, \ldots, y^{p-1}\}.$$

We show that if $G = ABC$ is a normed factorization, then

$$A \subset \langle x^p, y\rangle \quad \text{or} \quad A \subset \langle x, y^p\rangle.$$

To show this let $a', a \in A$ and $a'a^{-1} = x^\alpha y^\beta$. If $p \nmid \alpha$ and $p \nmid \beta$, then

$a' = ax^\alpha y^\beta$ contradicts the factorization $G = AB'C'$ what we get from the factorization $G = ABC$ by replacing B, C by B', C', where

$$B' = \{e, x^\alpha, x^{2\alpha}, \dots, x^{(p-1)\alpha}\}, \quad C' = \{e, y^\beta, y^{2\beta}, \dots, y^{(p-1)\beta}\}.$$

This replacement is possible by Lemma 1. Let $a = x^\alpha y^\beta \in A$. The previous argument with $a' = e$ gives that $p|\alpha$ or $p|\beta$. If $p|\alpha$ for each $a \in \in A$, then $A \subset \langle x^p, y\rangle$. Similarly if $p|\beta$ for each $a \in A$, then $A \subset \langle x, y^p\rangle$. Thus we may assume that there are $a = x^\alpha y^\beta, a' = x^{\alpha'} y^{\beta'} \in A$ such that $p|\alpha$, $p \nmid \beta$ and $p \nmid \alpha'$, $p|\beta'$, then $p \nmid (\alpha' - \alpha)$, $p \nmid (\beta' - \beta)$. So $a'a^{-1} = x^{\alpha'-\alpha} y^{\beta'-\beta}$ leads to a contradiction.

Let $M = \langle x^p, y\rangle$ and $N = \langle x, y^p\rangle$. If $A \subset \langle x^p, y\rangle = M$, then $M = = AC$ is a factorization and so $\overline{A}(e - y^p) = 0$ shows that y^p is a period of A. Similarly if $A \subset \langle x, y^p\rangle = N$, then $N = AB$ is a factorization and so $\overline{A}(e - x^p) = 0$ shows that x^p is a period of A.

Subcase 3(b). Both B and C are simulated, that is,

$$B = \{e, b, b^2, \dots, b^{p-2}, b^{p-1}u\}, \quad C = \{e, c, c^2, \dots, c^{p-2}, c^{p-1}v\}.$$

Here $|b| = |c| = p$ and we may assume that $|u| = p$, $|v| = p$. The elements of G of order p generate the subgroup $K = \langle x^p, y^p\rangle$ of order p^2. Now $K = BC$ is a factorization of K. By Rédei's theorem one of the factors B and C is a subgroup of K.

Subcase 3(c). B is cyclic and C is simulated, that is,

$$B = \{e, b, b^2, \dots, b^{p-1}\}, \quad C = \{e, c, c^2, \dots, c^{p-2}, c^{p-1}v\}.$$

Here we may assume that $|b| \geq p^2$ and $|c| = |v| = p$. By Lemma 4, $A = U\langle b^p\rangle \cup V\langle v\rangle$. If $U = \emptyset$ or $V = \emptyset$, then A is periodic and so we assume that $U \neq \emptyset$ and $V \neq \emptyset$. If $v \in \langle b^p\rangle$, then $\langle v\rangle = \langle b^p\rangle$ and so A is periodic. Thus we assume that $v \notin \langle b^p\rangle$. Now b^p, v form a basis for $K = \langle x^p, y^p\rangle$.

In the factorization $G = ABC$ replace C by $\langle c\rangle$ to obtain the factorization $G = AB\langle c\rangle$. Compute $A\langle c\rangle$.

$$A\langle c\rangle = \Big(U\langle b^p\rangle \cup V\langle v\rangle\Big)\langle c\rangle = U\langle b^p\rangle\langle c\rangle \cup V\langle v\rangle\langle c\rangle.$$

Both $\langle b^p\rangle\langle c\rangle$ and $\langle v\rangle\langle c\rangle$ must be direct and equal to K. Note that b^p, v form a basis for K. By Lemma 3 in C c can be replaced by c^i for each i, $1 \leq i \leq p-1$, so we have $p-1$ choices for c. Namely, c may be $b^p v^i$, $1 \leq i \leq p-1$. Now

$$C = \{e, b^p v^i, b^{2p} v^{2i}, \dots, b^{(p-2)p} v^{(p-2)i}, b^{(p-1)p} v^{(p-1)i+1}\}.$$

There is a j such that $1 \leq j \leq p-2$ and $ji \equiv (p-1)i + 1 \pmod p$ since $(j+1)i \equiv 1 \pmod p$ is solvable. Let $t \in U$. The product $t\langle b^p\rangle C$ is direct since it is part of ABC. Compute $\langle b^p\rangle C$. Note that the sets

$$\langle b^p\rangle b^{jp}v^{ji} = \langle b^p\rangle v^{jp} \quad \text{and} \quad \langle b^p\rangle b^{(p-1)p}v^{(p-1)i+1} = \langle b^p\rangle v^{(p-1)i+1}$$

are parts of $\langle b^p\rangle C$ and they have the same elements. This is a contradiction.

CASE 4. G is of type (p^2, p, p). Let $G = \langle x\rangle \times \langle y\rangle \times \langle z\rangle$, where $|x| = p^2$, $|y| = |z| = p$.

Subcase 4(a). Both B and C are cyclic, that is,

$$B = \{e, b, b^2, \dots, b^{p-1}\}, \quad C = \{e, c, c^2, \dots, c^{p-1}\}.$$

Here we may assume that $|b| = p^2$, $|c| = p^2$. By Lemma 4, $A = U\langle b^p\rangle \cup \cup V\langle c^p\rangle$. Let $b = x^\alpha y^\beta z^\gamma$ and $c = x^\delta y^\epsilon z^\mu$ be the basis representations of b and c. Now $b^p = x^{p\alpha}$ and $c^p = x^{p\delta}$. The subgroups of $\langle x^p\rangle$ form a chain. So $\langle x^p\rangle = \langle b^p\rangle = \langle c^p\rangle$. Thus x^p is a period of A.

Subcase 4(b). Both B and C are simulated, that is,

$$B = \{e, b, b^2, \dots, b^{p-2}, b^{p-1}u\}, \quad C = \{e, c, c^2, \dots, c^{p-2}, c^{p-1}v\}.$$

Here $|b| = |c| = p$ and by Lemma 2 we may assume that $|u| = p$, $|v| = = p$. Replace B, C by $\langle b\rangle, \langle c\rangle$ in the factorization $G = ABC$ to get the factorization $G = A\langle b\rangle\langle c\rangle$. This gives that the product $\langle b\rangle\langle c\rangle$ is direct.

If $u, v \in \langle b, c\rangle$, then $BC = \langle b, c\rangle$ is a factorization and so by Rédei's theorem we are done. We assume that $u \notin \langle b, c\rangle$ and $v \in \langle b, c, u\rangle$, that is, $v = b^\alpha c^\beta u^\gamma$ Now

$$B = \{e, b, b^2, \dots, b^{p-2}, b^{p-1}u\}, \quad C = \{e, c, c^2, \dots, c^{p-2}, c^{p-1}b^\alpha c^\beta u^\gamma\},$$

$$A = U\langle u\rangle \cup V\langle b^\alpha c^\beta u^\gamma\rangle.$$

Here we assume that $U \neq \emptyset$ and $V \neq \emptyset$ since otherwise A is periodic.

Assume first that $\beta = 0$. If $\gamma = 0$, then $\alpha \neq 0$. By Lemma 2 we may assume that $\alpha = 1$. Let $t \in V$. The product $t\langle b\rangle B$ is direct since the product ABC is direct. On the other hand $b \in \langle b\rangle$ and $b \in B$. This is a contradiction.

If $\gamma \neq 0$, then by Lemma 2 we may assume that $\gamma = 1$. If $\alpha = 0$, then u is a period of A. Thus we assume that $\alpha \neq 0$. Let $t \in V$. The product $t\langle b^\alpha u\rangle B$ is direct. The elements $b^{(p-1)\alpha+p-1}, e, b, b^2, \dots, p^{p-2}$ belong to $\langle b^\alpha u\rangle B$. So $(p-1)\alpha + p - 1 \not\equiv 0, 1, 2, \dots, p-2 \pmod{p}$ and hence $(p-1)\alpha + p - 1 \equiv p - 1 \pmod{p}$. Thus $\alpha = 0$. But we know this is not the case.

Secondly assume that $\beta \neq 0$. By Lemma 2 we may assume that $\beta = 1$. Now

$$C = \{e, c, c^2, \dots, c^{p-2}, c^{p-1}b^\alpha c u^\gamma\} = \{e, c, c^2, \dots, c^{p-2}, b^\alpha u^\gamma\}$$

Let $t \in U$. The product $t\langle u\rangle BC$ is direct. Clearly $\langle u\rangle BC = \langle b, u\rangle C$. But this a contradiction since $b^\alpha u^\gamma \in \langle b, u\rangle$ and $b^\alpha u^\gamma \in C$.

Subcase 4(c). B is cyclic and C is simulated, that is,

$$B = \{e, b, b^2, \dots, b^{p-1}\}, \quad C = \{e, c, c^2, \dots, c^{p-2}, c^{p-1}v\}.$$

We may assume that $|b| = p^2$ and $|c| = |v| = p$. By Lemma 4, $A = U\langle b^p\rangle \cup V\langle v\rangle$. We assume that $U \neq \emptyset$ and $V \neq \emptyset$ since otherwise A is periodic.

Let $t \in U$. The product $t\langle b^p\rangle C$ is direct since it is part of the product ABC. If $c \in \langle b^p\rangle$, then $c = b^{pi}$ for some i, $1 \leq i \leq p-1$. This leads to the contradiction $c \in \langle b^p\rangle$ and $c \in C$. Thus we assume that $c \notin \langle b^p\rangle$. We distinguish two cases depending on $v \in \langle b^p, c\rangle$ or $v \notin \langle b^p, c\rangle$.

If $v \in \langle b^p, c\rangle$, then $v = b^{p\alpha}c^\beta$. If $\beta = 0$, then A is periodic by b^p. If $\beta \neq 0$, then by Lemma 2 we may assume that $\beta = 1$. Now

$$C = \{e, c, c^2, \dots, c^{p-2}, c^{p-1}b^{p\alpha}c\} = \{e, c, c^2, \dots, c^{p-2}, b^{p\alpha}\}.$$

Let $t \in U$. The product $t\langle b^p\rangle C$ is direct since it is part of the product ABC. But $b^{p\alpha} \in \langle b^p\rangle$ and $b^{p\alpha} \in C$ is a contradiction.

Turn to the case when $\langle b^p, c, v\rangle$ is of type (p,p,p). From the factorization $G = ABC$ it follows that $0 = \overline{AC}(e - b^p)$ and so AC is periodic by b^p. Consequently $V\langle v\rangle C$ is periodic by b^p. Note that $\langle v\rangle C = \langle c, v\rangle$. If $t \in V$, then $e \in t^{-1}V\langle v\rangle C = t^{-1}V\langle c, v\rangle$. Now $\langle b^p\rangle \subset t^{-1}V\langle c, v\rangle$. As $t^{-1}V\langle c, v\rangle$ is a union cosets modulo $\langle c, v\rangle$ and the elements of $\langle b^p\rangle$ are incongruent modulo $\langle c, v\rangle$, it follows that $p^3 = \left|\langle b^p\rangle\langle c, v\rangle\right| \leq \left|t^{-1}V\langle c, v\rangle\right| = |V|p^2$. This gives that $|V| \geq p$ and so we get the contradiction that $U = \emptyset$.

CASE 5. G is of type (p,p,p,p). Each element of $G \setminus \{e\}$ is of order p and so a cyclic subset of G is a subgroup of G. Thus the only case we should consider is when both B and C are simulated, that is,

$$B = \{e, b, b^2, \dots, b^{p-2}, b^{p-1}u\}, \quad C = \{e, c, c^2, \dots, c^{p-2}, c^{p-1}v\}.$$

Here $|b| = |c| = p$ and we may assume that $|u| = p$, $|v| = p$. Replace B, C by $\langle b\rangle, \langle c\rangle$ in the factorization $G = ABC$ to get the factorization $G = A\langle b\rangle\langle c\rangle$. This gives that the product $\langle b\rangle\langle c\rangle$ is direct. So the group $\langle b, c, u, v\rangle$ is one of the types (p,p), (p,p,p), (p,p,p,p).

Turn first to the case when $\langle b, c, u, v\rangle$ is of type (p,p). Now $u, v \in \langle b, c\rangle$. Further $BC = \langle b, c\rangle$ is a factorization and so by Rédei's theorem we are done.

Secondly consider the case when $\langle b, c, u, v\rangle$ is of type (p,p,p). We assume that $u \notin \langle b, c\rangle$ and $v \in \langle b, c, u\rangle$, that is, $v = b^\alpha c^\beta u^\gamma$ Now

$$B = \{e, b, b^2, \dots, b^{p-2}, b^{p-1}u\}, \quad C = \{e, c, c^2, \dots, c^{p-2}, c^{p-1}b^\alpha c^\beta u^\gamma\},$$

$$A = U\langle u\rangle \cup V\langle b^{\alpha}c^{\beta}u^{\gamma}\rangle.$$

Here we assume that $U \neq \emptyset$ and $V \neq \emptyset$ otherwise A is periodic.

Assume first that $\beta = 0$. If $\gamma = 0$, then $\alpha \neq 0$. By Lemma 2 we may assume that $\alpha = 1$. Let $t \in V$. The product $t\langle b\rangle B$ is direct since the product ABC is direct. On the other hand $b \in \langle b\rangle$ and $b \in B$. This is a contradiction.

If $\gamma \neq 0$, then by Lemma 2 we may assume that $\gamma = 1$. If $\alpha = 0$, then u is a period of A. Thus we assume that $\alpha \neq 0$. Let $t \in V$. The product $t\langle b^{\alpha}u\rangle B$ is direct. The elements $b^{(p-1)\alpha+p-1}, e, b, b^2, \ldots, p^{p-2}$ belong to $\langle b^{\alpha}u\rangle B$. So $(p-1)\alpha + p - 1 \not\equiv 0, 1, 2, \ldots, p-2 \pmod{p}$ and hence $(p-1)\alpha + p - 1 \equiv p - 1 \pmod{p}$. Thus $\alpha = 0$. But we know this is not the case.

Secondly assume that $\beta \neq 0$. By Lemma 2 we may assume that $\beta = 1$. Now

$$C = \{e, c, c^2, \ldots, c^{p-2}, c^{p-1}b^{\alpha}cu^{\gamma}\} = \{e, c, c^2, \ldots, c^{p-2}, b^{\alpha}u^{\gamma}\}$$

Let $t \in U$. The product $t\langle u\rangle BC$ is direct. Clearly $\langle u\rangle BC = \langle b, u\rangle C$. But this a contradiction since $b^{\alpha}u^{\gamma} \in \langle b, u\rangle$ and $b^{\alpha}u^{\gamma} \in C$.

Finally turn to the case when $\langle b, c, u, v\rangle$ is of type (p, p, p, p). From the factorization $G = A\langle b\rangle\langle c\rangle$ it follows that A is a complete set of representatives modulo $\langle b, c\rangle$ and so

$$A = \{u^i v^j a_{ij} : 0 \leq i, j \leq p-1, a_{ij} \in \langle b, c\rangle\}.$$

We may assume that $e \in A$, that is, $a_{00} = e$. We also know that $A = U\langle u\rangle \cup V\langle v\rangle$.

Here we assume that $U \neq \emptyset$ and $V \neq \emptyset$ since otherwise A is periodic. As the roles of u and v are symmetric, we may assume that $e \in U$. Then $\langle u\rangle \subset A$. This means that $a_{i0} = e$ for each i, $0 \leq i \leq p-1$. Let $u^i v^j a_{ij} \in V\langle v\rangle$. Now $u^i v^j a_{ij}\langle v\rangle \subset A$. This gives that a_{ij}'s are equal for each j, $0 \leq j \leq p-1$. As $a_{i0} = e$, we have $a_{ij} = e$ for each j, $0 \leq j \leq p-1$. Then $u^i v^j a_{ij}\langle v\rangle = u^i\langle v\rangle$. Therefore $u^i \in V\langle v\rangle$. On the other hand $u^i \in U\langle u\rangle$. This is a contradiction since $V\langle v\rangle$ and $U\langle u\rangle$ are disjoint.

This completes the proof. ◊

4. Examples

In this section we exhibit examples to show that the conditions of the problem proposed in the introduction cannot be relaxed in general.

Let $G = \prod_{i=1}^{5}\langle x_i\rangle$, where $|x_i| = r_i \geq 3$. Set

$$T_0 = \{e, x_3, x_3^2, \dots, x_3^{r_3-2}, x_3^{r_3-1}x_4\},$$
$$T_1 = \{e, x_2, x_2^2, \dots, x_2^{r_2-2}, x_2^{r_2-1}x_5\},$$
$$T_2 = \dots = T_{r_1-1} = \langle x_2 \rangle.$$

Now we define A, B, C by

$$A = T_0\langle x_2\rangle \cup x_1T_1\langle x_3\rangle \cup x_1^2T_2\langle x_3\rangle \cup \dots \cup x_1^{r_1-1}T_{r_1-1}\langle x_3\rangle,$$
$$B = \{e, x_4, x_4^2, \dots, x_4^{r_4-2}, x_4^{r_4-1}x_2\},$$
$$C = \{e, x_5, x_5^2, \dots, x_5^{r_5-2}, x_5^{r_5-1}x_3\}.$$

We claim that $G = ABC$ is a factorization of G. In order to verify this first we show that

$$T_0\langle x_2\rangle BC = T_1\langle x_3\rangle BC = \dots = T_{r_1-1}\langle x_3\rangle BC = \langle x_2, x_3, x_4, x_5\rangle.$$

Indeed,

$$T_0\langle x_2\rangle BC = T_0\langle x_2, x_4\rangle C = \langle x_2, x_3, x_4\rangle C = \langle x_2, x_3, x_4, x_5\rangle,$$

and

$$T_1\langle x_3\rangle CB = T_1\langle x_3, x_5\rangle B = \langle x_2, x_3, x_5\rangle B = \langle x_2, x_3, x_4, x_5\rangle.$$

The remaining cases can be verified in a similar way. Now

$$ABC = \left(T_0\langle x_2\rangle \cup x_1T_1\langle x_3\rangle \cup x_1^2T_2\langle x_3\rangle \cup \dots \cup x_1^{r_1-1}T_{r_1-1}\langle x_3\rangle\right)BC =$$
$$= T_0\langle x_2\rangle BC \cup x_1T_1\langle x_3\rangle BC \cup x_1^2T_2\langle x_3\rangle BC \cup \dots \cup x_1^{r_1-1}T_{r_1-1}\langle x_3\rangle BC =$$
$$= \{e, x_1, x_1^2, \dots, x_1^{r_1-1}\}\langle x_2, x_3, x_4, x_5\rangle = \langle x_1, x_2, x_3, x_4, x_5\rangle = G.$$

It is clear that B, C are not periodic. The subset A is not periodic since it is a disjoint union of periodic subsets which have no period in common. To make the example more concrete let us choose $r_1, \dots, r_5$ to be 3. In this case G is of type $(3,3,3,3,3)$, B, C are simulated subsets $|A| = 3^3$ and none of the factors is periodic. In the special case when $r_1, \dots, r_5$ are pairwise relatively primes G is a cyclic group.

In the next example the factors B and C are cyclic. Let $G = \langle x\rangle \times \times \langle y\rangle$, where $|x| = rst$, $|y| = uv$, and $r, s, t, u, v \geq 2$. Set

$$T_0 = \{e, y^u, y^{2u}, \dots, y^{(v-2)u}, y^{(v-1)u}x^r\},$$
$$T_1 = \{e, x^{rs}, x^{2rs}, \dots, x^{(t-2)rs}, x^{(t-1)rs}y\},$$
$$T_2 = \dots = T_{r-1} = \langle x^{rs}\rangle.$$

Now define A, B, C by

$$A = T_0\langle x^{rs}\rangle \cup xT_1\langle y^u\rangle \cup x^2T_2\langle y^u\rangle \cup \dots \cup x^{r-1}T_{r-1}\langle y^u\rangle,$$
$$B = \{e, x^r, x^{2r}, \dots, x^{(s-1)r}\}, \quad C = \{e, y, y^2, \dots, y^{u-1}\}.$$

Clearly B, C are not periodic and A is not periodic since it is a disjoint union of periodic subsets without common period. We claim that $G = = ABC$ is a factoring of G. In order to verify this claim we first show that

$T_0\langle x^{rs}\rangle BC = T_1\langle y^u\rangle BC = T_2\langle y^u\rangle BC = \cdots = T_{r-1}\langle y^u\rangle BC = \langle x^r, y\rangle$.
Indeed,
$T_0\langle x^{rs}\rangle BC = T_0\langle x^r\rangle C = \langle x^r, y\rangle$, and $T_1\langle y^u\rangle CB = T_1\langle y\rangle B = \langle x^r, y\rangle$.
The remaining cases can be verified in a similar way. Using these facts

$$ABC = \big(T_0\langle x^{rs}\rangle \cup xT_1\langle y^u\rangle \cup x^2T_2\langle y^u\rangle \cup \ldots \cup x^{r-1}T_{r-1}\langle y^u\rangle\big)BC =$$
$$= T_0\langle x^{rs}\rangle BC \cup xT_1\langle y^u\rangle BC \cup x^2T_2\langle y^u\rangle BC \cup \ldots \cup x^{r-1}T_{r-1}\langle y^u\rangle BC =$$
$$= \{e, x, x^2, \ldots, x^{r-1}\}\langle x^r, y\rangle = \langle x, y\rangle = G.$$

If we choose r, s, t, u, v to be 2, then G is of type $(2^3, 2^2)$, $|A| = 2^3$, $|B| = |C| = 2$. If rst, and uv are relatively primes, then G is a cyclic group.

References

[1] CORRÁDI, K. and SANDS, A. U. and SZABÓ, S.: Simulated factorizations, *Journal of Alg.*, **151** (1992), 12–25.

[2] CORRÁDI, K. and SZABÓ, S: Solution to a problem of A. D. Sands, *Communications in Algebra*, **23** (1995), 1503–1510.

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

[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] SANDS, A. D.: Factorization of cyclic groups, *Colloquium on abelian groups*, Tihany, Hungary, Sept. 1963, 139–146.

[6] SANDS, A. D. and SZABÓ, S.: Factorization of periodic subsets, *Acta Math. Hungar.* **57** (1991), 159–167.