Circulant Matrices and Factorizations of $\mathbb{Z}_p \times \mathbb{Z}_q$

Vladimir Božović

Department of Science and Mathematics, University of Montenegro

Abstract. We say that a collection of subsets $\alpha = [B_1, \dots, B_k]$ of a group G is a *factorization* if $G = B_1 \cdots B_k$ and each element of G is expressed in a unique way in this product. We examine a special case, factorizations of a group $\mathbb{Z}_p \times \mathbb{Z}_q$, where p and q are different prime numbers, using the new approach based on circulant matrices. An interesting number theoretic implication of Rédei's theorem for the group $\mathbb{Z}_p \times \mathbb{Z}_q$ is given.

1. INTRODUCTION

The factorization of abelian groups deals with decomposing an abelian group into a direct sum of its subsets. The nature of these problems are partly algebraic and partly combinatorial. However, the origin of the theory of abelian group factorizations is related to one famous geometric problem. Namely, about 1900, H. Minkowski conjectured:

Every lattice of a tiling of $\mathbb{R}^n$ by unit cubes contains two cubes that meet in an $n-1$ dimensional face.

In 1938, in his PhD thesis, G. Hajós reformulated Minkowski's conjecture in terms of finite abelian groups. That was the beginning of the theory of factorization of abelian groups in the sense it exists now. The fact that every abelian group is isomorphic to a factor group of an integral lattice with respect to an integral sub-lattice, connects the vast field of tilings and abelian groups. In general, factorization questions are relevant to the theory of numbers, tilings, variable length codes, graph theory, packings, covering problems, just to mention a few. For a comprehensive introduction to factorizations of abelian groups we refer the reader to book by Szabó [6].

Definition 1.1. *We say that a list of $k \geq 2$ subsets $\alpha = [B_1, B_2, \dots, B_k]$ of a group G is a factorization of $C \subseteq G$ if $C = B_1 B_2 \dots B_k$ and every $c \in C$ has a unique representation as a product $c = b_1 b_2 \dots b_k$, $b_i \in B_i$, $1 \leq i \leq k$. We call the subsets B_i, the blocks of the factorization α and each block a factor. The factorization is called normalized if each block B_i contains the identity element (as does C itself). When C is finite we say that the type of α is $(r_1, r_2, \dots, r_k)$, where $|B_i| = r_i$ for $1 \leq i \leq k$.*

A factorization $\alpha = [B_1, B_2, \dots, B_k]$ of a group G is said to be *proper* if $|B_i| \neq 1$ and $B_i \neq G$, for every i, $1 \leq i \leq k$.

Theorem 1.1. *Let A, B, C be finite subsets of a group G with $AB \subseteq C$. Then any two of the following implies the third. Furthermore, the three conditions are equivalent to $[A, B]$*

being a factorization of C.

(a) $AB \supseteq C$;
(b) $(A^{-1}A) \cap (BB^{-1}) = \{e\}$;
(c) $|A||B| = |C|$;

Proof. Let P be the set of ordered pairs $A \times B$ and consider the product map $f : P \to C$ given by $f : (a,b) \mapsto ab$. Then $[A,B]$ is a factorization of C exactly when the map f is a bijection from P to C. It remains only to note that the three conditions are

(a) f maps P onto C;
(b) f is one-to-one;
(c) $|P| = |C|$;

For (b) observe that $a_1b_1 = a_2b_2$ exactly if $a_2^{-1}a_1 = b_2b_1^{-1}$. □

The following, well known lemma gives an algorithmic procedure for constructing a factorization of given group G.

Lemma 1.1. *Let $\{e\} = G_0 \leq G_1 \leq \cdots \leq G_s = G$ be a chain of subgroups and let B_i be a complete set of right coset representatives of G_{i-1} in G_i, for $1 \leq i \leq s$. Then, $\alpha = [B_1,\ldots,B_s]$ is a factorization of G.*

Proof. Let $g \in G$ be an arbitrary element. There exists a unique $b_s \in B_s$ such that $g \in G_{s-1}b_s$. Then $gb_s^{-1} \in G_{s-1}$. Similarly, there exists a unique $b_{s-1} \in B_{s-1}$ such that $gb_s^{-1} \in G_{s-2}b_{s-1}$ and consequently $gb_s^{-1}b_{s-1}^{-1} \in G_{s-2}$. Continuing this way, we obtain a sequence $b_1, b_2, \ldots, b_s$, unique for a given $g \in G$ such that $gb_s^{-1}b_{s-1}^{-1} \cdots b_1^{-1} \in G_0$. Therefore, $g = b_1 \cdots b_s$ and $b_i \in B_i$ for $1 \leq i \leq s$. Thus, α is a factorization of G. □

This specific type of group factorization $\alpha = [B_1,\ldots,B_s]$ of a group G, derived from the chain of groups

$$\{e\} = G_0 \leq G_1 \leq \cdots \leq G_s = G$$

where B_i is a set of complete representatives of G_{i-1} in G_i is called a *transversal factorization*. Note that whenever a group G has a proper subgroup, there exists a proper factorization.

Example 1.1. *In particular, let G be a permutation group acting on the set $\Omega = \{1,2,\ldots,n\}$. Consider the sequence of subgroups G_i, such that G_i fixes pointwise the letters from the set $\{1,2,\ldots,i\}$. Then*

$$G \geq G_1 \geq G_2 \geq \cdots \geq G_n \geq \{e\}.$$

Therefore, every permutation group has a transversal factorization.

We mention one of the milestones in the theory of factorizations of abelian groups, Rédei's theorem [6].

Theorem 1.2. *[Rédei] Let $\alpha = [B_1, B_2, \ldots, B_k]$ be a normalized factorization of the finite abelian group G such that $|B_i| = p_i$ is a prime for each i, $1 \leq i \leq k$. Then at least one of the blocks $B_1, B_2, \ldots, B_k$ is a subgroup of G.*

2. FREE MAPPINGS AND FACTORIZATIONS OF $A \times B$

In this section, A and B will denote finite groups. By introducing a certain class of so-called free mappings [3] between A and B and by giving an effective way for their construction, we obtain factorizations of $A \times B$. Although this could be applied to nonabelian groups A and B, this approach has greater significance for abelian groups.

For the rest of the paper, the term factorization will be reserved for proper factorization.

Definition 2.1. *Let $f : A \to B$ and $g : B \to A$ be mappings between groups A and B. Two pairs (a_1,b_1), (a_2,b_2), where $a_1,a_2 \in A$, $b_1,b_2 \in B$, are said to be a clip of pair (f, g) if it holds*

$$f(a_1)^{-1}f(a_2) = b_2b_1^{-1}$$

$$g(b_2)g(b_1)^{-1} = a_1^{-1}a_2.$$

We say that a clip (a_1,b_1), (a_2,b_2) is strong if $a_1 \neq a_2$ or $b_1 \neq b_2$. In fact, it is clear that if (a_1,b_1), (a_2,b_2) is a strong clip, then $a_1 \neq a_2$ and $b_1 \neq b_2$. A pair of mappings (f,g) is chained if there exists a strong clip of (f, g), otherwise we say that it is free.

The following theorem provides a way for constructing a factorization of $A \times B$ for given pair of free mappings (f, g).

Theorem 2.1. *Let $f : A \to B$ and $g : B \to A$ be mappings where A, B are finite groups. Let $S = \{(a, f(a)) \mid a \in A\}$ and $T = \{(g(b), b) \mid b \in B\}$. Then, $\alpha = [S,T]$ is a factorization of $A \times B$ if and only if (f, g) is a pair of free mappings.*

Proof. Suppose that α is a factorization of $A \times B$. Let $a_1,a_2 \in A$ and $b_1,b_2 \in B$ be such that

$$f(a_1)^{-1}f(a_2) = b_2b_1^{-1}$$

$$g(b_2)g(b_1)^{-1} = a_1^{-1}a_2.$$

Equivalently, we have that

$$(a_1, f(a_1))(g(b_2),b_2) = (a_2, f(a_2))(g(b_1),b_1).$$

Hence, $(a_1, f(a_1)) = (a_2, f(a_2))$ and $(g(b_2),b_2) = (g(b_1),b_1)$. We conclude that $a_1 = a_2$ and $b_1 = b_2$, so (f,g) is free.

Conversely, suppose that a pair (f, g) is free. It is easy to see that $(S^{-1}S) \cap (TT^{-1}) = \{(e,e)\}$. Since A and B are finite groups, it follows that $|ST| = |S||T| = |A||B| = |A \times B|$. Therefore, $ST = A \times B$ and according to Theorem 1.1, α is a factorization of $A \times B$. □

Let A and B be groups and H be a subgroup of A. We say that $f : A \to B$ is constant on the left cosets of H if $|f(aH)| = 1$ for every $a \in A$. In the following lemma, we give a technique for constructing free mappings.

Lemma 2.1. *Let A and B be groups and H be a subgroup of A. Let $f : A \to B$ be constant on the left cosets of H and $g : B \to A$ such that $Im(g) \subseteq H$. Then the pair (f, g) is free.*

Proof. Suppose that there exists a strong clip (a_1,b_1), (a_2,b_2) of (f,g). Then, $a_1^{-1}a_2 = g(b_2)g(b_1)^{-1} \in H$. This means that a_1,a_2 are in the same left coset of H. Hence, $f(a_1)^{-1}f(a_2) = e$ and $b_2b_1^{-1} = e$, implying $b_1 = b_2$. Consequently, we have $a_1 = a_2$ which contradicts the assumption that (a_1,b_1), (a_2,b_2) is a strong clip of (f, g). □

Clearly, the previous result holds if we take right instead of left cosets. Note that if $H = \{e\}$ then $\mathrm{Im}(g) = \{e\}$. Hence, f could be any mapping from A to B. In order to construct a proper factorization using the previous lemma, either A or B must have a nontrivial subgroup. Previous construction could be generalized [2], so that it's possible to factorize much broader class of groups than direct products.

The following example is a simple illustration of how to use free mappings to obtain a factorization of $A \times B$.

Example 2.1. *Consider the group*

$$G = \langle a,b,c \mid a^2 = b^3 = c^3 = e,\ b^a = b,\ c^a = c^{-1},\ bc = cb \rangle.$$

This is a nonabelian group of order 18 and has a permutation representation on 6 points. Denote by $\mathrm{Sym}(n)$ *symmetric group on n elements. We can identify* $a = (4\,5)$*,* $b = (1\,2\,3)$ *and* $c = (4\,5\,6)$*. Let A, B be the pointwise stabilizers [1] of the letters* $\{1,2,3\}$*,* $\{4,5,6\}$ *respectively. It is easy to see that* $A \cong \mathrm{Sym}(3)$ *while* $B \cong \mathbb{Z}_3$*. Since A and B are both normal in G and* $A \cap B = \{e\}$ *it follows that* $G \cong \mathrm{Sym}(3) \times \mathbb{Z}_3$*. Therefore, we can identify elements of G as ordered pairs.*

First, we apply the technique given in Lemma 2.1 in order to find a pair of free mappings. We choose a subgroup H of $\mathrm{Sym}(3)$*, say* $H = \{\mathrm{id}, (1\ 2\ 3), (1\ 3\ 2)\}$*. Then, considering the cosets H and* $H(1\ 2)$*, we can construct a pair of free mappings* f,g *in the following way:*

$$f : \mathrm{Sym}(3) \to \mathbb{Z}_3\ ,\ \ f(x) = \begin{cases} 0, & \text{if } x \in H; \\ 2, & \text{if } x \in H(1\ 2). \end{cases}$$

$$g : \mathbb{Z}_3 \to \mathrm{Sym}(3)\ ,\ \ g(0) = \mathrm{id}\ ,\ g(1) = (1\ 3\ 2),\ g(2) = (1\ 3\ 2).$$

The pair of free mappings f,g *provides a factorization* $\mathrm{Sym}(3) \times \mathbb{Z}_3 = B_1 \cdot B_2$*, where*

$B_1 = \{(id,0), ((1\,2\,3),0), ((1\,3\,2),0), ((1\,2),2), ((1\,3),2), ((2\,3),2)\}$,

$B_2 = \{(id,0), ((1\,3\,2),1)), ((1\,3\,2),2)\}$. *Note that this is a nontrivial factorization where the blocks* B_1, B_2 *are neither groups nor cosets of groups.*

3. FACTORIZATION OF $\mathbb{Z}_{PQ}$

The particular relevance of free mappings appears in the factorizations of $\mathbb{Z}_{pq}$. Further on, p and q will be different prime numbers. It will be shown that every factorization of $\mathbb{Z}_{pq}$ induces a pair of free mappings between $\mathbb{Z}_p$ and $\mathbb{Z}_q$. We will present an interesting application of circulant matrices [4] in the factorization of abelian groups. We will show that under certain conditions each pair of mappings $f : \mathbb{Z}_p \to \mathbb{Z}_q$ and $g : \mathbb{Z}_q \to \mathbb{Z}_p$ must be chained.

Definition 3.1. *A set of integers that includes one and only one member of each number class modulo n is called a complete residue system modulo n.*

Example 3.1. *Set* $\{-8,-1,0,1,7\}$ *is a complete residue system modulo* 5.

Theorem 3.1. *Let p be a prime number and $c_p, c_{p-1}, \ldots, c_1$ integers. Let*

$$\mathbf{V} = \begin{pmatrix} c_p & c_{p-1} & \ldots & c_1 \\ c_1 & c_p & \ldots & c_2 \\ \vdots & \vdots & \vdots & \vdots \\ c_{p-1} & c_{p-2} & \ldots & c_p \end{pmatrix}$$

be a circulant matrix, denoted by $V = \operatorname{circ}(c_p, c_{p-1}, \ldots, c_1)$. *Then* $\det(V) = 0$ *if and only if either* $\sum_{i=1}^{p} c_i = 0$ *or all the* c_i *are equal.*

Proof. If all c_i are equal then clearly $\det(V) = 0$. If $\sum_{i=1}^{p} c_i = 0$, then by adding all rows of V together, the zero row is obtained and therefore $\det(V) = 0$.

Conversely, suppose that $\det(V) = 0$. We know that at least one of the eigenvalues of a circulant matrix is equal to zero. The eigenvalues of the circulant matrix V are

$$\lambda_l = P(e^{\frac{2\pi i}{p} l}), \quad l = 0, 1, \ldots, p-1$$

where

$$P(x) = \sum_{i=0}^{p-1} c_i x^i.$$

So, there exists l such that $e^{\frac{2\pi i}{p} l}$ is a root of the polynomial $P(x)$. Consider two cases. If $l = 0$ then

$$\sum_{i=0}^{p-1} c_i = 0.$$

If $l \neq 0$ then $e^{\frac{2\pi i}{p} l}$ is a primitive p-th root of unity. In this case, the minimal polynomial of $e^{\frac{2\pi i}{p} l}$ over the integers is the cyclotomic polynomial

$$Q(x) = \sum_{i=0}^{p-1} x^i.$$

Therefore $P(x)$ is a constant multiple of $Q(x)$. Consequently, all c_i's are equal. □

Definition 3.2. *Let U and W be multisets that belong to a common additive group G. We define $U + W$ to be the multiset that contains all elements of the form $u + w$ where $u \in U$ and $w \in W$.*

The following result is interesting by itself, disregarding any implications on factorizations of abelian groups. Namely, it provides a condition under which the sum of two multisets of integers, where one of them has prime size p, is uniformly distributed among the residue classes modulo p.

Lemma 3.1. *Let U and W be two multisets of positive integers. Let $|U| = p$ and $|W| = n$, where p is a prime number and $\gcd(p,n) = 1$. Then, the multiset $U+W$ contains exactly n numbers from each class modulo p if and only if U is a complete residue system modulo p.*

Proof. Let us suppose that $U+W$ contains n elements from each residue class modulo p. Let c_i, b_i represents the number of elements from U, W that are congruent to i modulo p respectively, where $1 \leq i \leq p$. Note that

$$\sum_{i=1}^{p} c_i = p \text{ and } \sum_{i=1}^{p} b_i = n.$$

Consider the multiset $U+W$. Let m_i denotes the number of elements of $U+W$ that are congruent to i modulo p. Clearly,

$$\begin{array}{rcccccccc} m_1 = & b_1c_p & + & b_2c_{p-1} & + & \dots & + & b_pc_1 \\ m_2 = & b_1c_1 & + & b_2c_p & + & \dots & + & b_pc_2 \\ \vdots & \vdots & & \vdots & & & & \vdots \\ m_p = & b_1c_{p-1} & + & b_2c_{p-2} & + & \dots & + & b_pc_p. \end{array}$$

If $m_1 = m_2 = \cdots = m_p = n$ then the previous system can be written in the matrix form

$$\begin{pmatrix} c_p & c_{p-1} & \dots & c_1 \\ c_1 & c_p & \dots & c_2 \\ \vdots & \vdots & \vdots & \vdots \\ c_{p-1} & c_{p-2} & \dots & c_p \end{pmatrix} \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_p \end{pmatrix} = \begin{pmatrix} n \\ n \\ \vdots \\ n \end{pmatrix}$$

If $C = \operatorname{circ}(c_p, c_{p-1}, \dots, c_1)$, $b = (b_1, b_2, \dots, b_p)^t$ and $d = (n, n, \dots, n)^t$, then the previous system is

$$Cb = d.$$

Let us suppose that $\det(C) \neq 0$. Then, the system has a unique solution, given by

$$b_1 = b_2 = \cdots = b_p = \frac{n}{p}.$$

Since b_i are positive integers and $\gcd(p,n) = 1$, this case is not possible. Therefore, it must be that $\det(C) = 0$. According to Theorem 3.1, it holds

$$c_1 = c_2 = \cdots = c_p = 1.$$

Thus, U is a complete system of residue classes modulo p.

Conversely, let us suppose that U is a complete system of residue classes modulo p. Consider $U+w$ for $w \in W$. It follows that $U+w$ is a complete residue system modulo p as well. Therefore, the multiset $U+W$ contains every residue class modulo p exactly $|W| = n$ times. □

Although the following result is a very special case of Theorem 1. in [5], the proof presented here is based on a new method, using circulant matrices and cyclotomic polynomials.

Lemma 3.2. *Let $\alpha = [B_1,\, B_2]$ be a factorization of $\mathbb{Z}_{pn}$. Let $|B_1| = p$ and $|B_2| = n$, where p is a prime number such that $\gcd(p,n) = 1$. Then B_1 is a complete system of residue classes modulo p.*

Proof. Let $m = pn$. Since $\gcd(p,n) = 1$, there is the natural isomorphism π between $\mathbb{Z}_m$ and the group of ordered pairs

$$\mathbb{Z}_p \times \mathbb{Z}_n = \{(a,b)|\; 0 \leq a \leq p-1,\; 0 \leq b \leq n-1\}$$

given by

$$\pi(x) = (x \bmod p,\; x \bmod n).$$

Therefore, α is a factorization of $\mathbb{Z}_m$ if and only if $\beta = [\pi(B_1),\, \pi(B_2)]$ is a factorization of $\mathbb{Z}_p \times \mathbb{Z}_n$. Note that there are exactly n pairs from $\mathbb{Z}_p \times \mathbb{Z}_n$ that have a particular a on the first coordinate, and there are exactly p pairs having a particular b on the second coordinate.

Let U, W be a multiset of the first coordinates of the set $\pi(B_1)$, $\pi(B_2)$ respectively. Note that elements in U and W are from $\mathbb{Z}_p$, where $|U| = p$ and $|W| = n$. Consider the multiset $U + W$. If β is a factorization of $\mathbb{Z}_p \times \mathbb{Z}_n$, then $U + W$ must contain every residue class modulo p exactly n times.

According to Lemma 3.1, U must contain all residue classes modulo p. Therefore, B_1 is a complete system of residue classes modulo p. □

Corollary 3.1. *Let $\alpha = [B_1,\, B_2]$ be a factorization of $\mathbb{Z}_{pq}$ where p and q are two different prime numbers. Let $|B_1| = p$ and $|B_2| = q$. Then B_1, B_2 are complete residue systems modulo p, q respectively.*

According to the previous corollary, it is clear that every factorization of $\mathbb{Z}_p \times \mathbb{Z}_q$ must be of the form $\alpha = [B_1, B_2]$ where $B_1 = \{(a, f(a))|\; 0 \leq a \leq p-1\}$ and $B_2 = \{(g(b), b)|\; 0 \leq b \leq q-1\}$. Consequently, using Theorem 2.1 we have the following result.

Corollary 3.2. *$\alpha = [B_1,\, B_2]$ is a factorization of $\mathbb{Z}_p \times \mathbb{Z}_q$ if and only if*

$$B_1 = \{(a, f(a))|\; 0 \leq a \leq p-1\},\; B_2 = \{(g(b), b)|\; 0 \leq b \leq q-1\},$$

p and q different primes and $(f,\, g)$ is a pair of free mappings.

Clearly, every factorization can be normalized, simply by a translation by an appropriate element. According to the previous corollary and Rédei's theorem, one block of a normalized factorization of $\mathbb{Z}_p \times \mathbb{Z}_q$, say B_1 must be of the form $B_1 = \{(a, 0))|\; 0 \leq a \leq p-1\}$. This means that $f(a) = 0$ for every $a \in \mathbb{Z}_p$. Further, this implies that g could be any mapping from $\mathbb{Z}_q$ to $\mathbb{Z}_p$, since a pair (f, g) is always free if one of the the two functions is the zero mapping. We consider two factorizations $\alpha = [B_1, B_2]$ and $\alpha' = [B_1', B_2']$

of $\mathbb{Z}_p \times \mathbb{Z}_q$ to be equal if $\{B_1, B_2\} = \{B'_1, B'_2\}$. From here, it follows easily that the total number of normalized factorizations of $\mathbb{Z}_p \times \mathbb{Z}_q$ is equal to $p^{q-1} + q^{p-1} - 1$.

Example 3.2. *Consider the mappings $f : \mathbb{Z}_3 \to \mathbb{Z}_4$, $g : \mathbb{Z}_4 \to \mathbb{Z}_3$, defined as*

$$f = \begin{pmatrix} 0 & 1 & 2 \\ 0 & 2 & 0 \end{pmatrix} \; g = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 0 & 1 & 0 & 1 \end{pmatrix}.$$

It is not hard to see that a pair (f, g) is free. Therefore, it is possible to factorize $\mathbb{Z}_3 \times \mathbb{Z}_4$ in the way shown in Theorem 2.1. Thus, we obtain $\alpha = [B_1, B_2]$, a factorization of Z_{12}, where $B_1 = \{0, 8, 10\}$, $B_2 = \{0, 1, 6, 7\}$.

The following theorem explains that under certain conditions, we always have a strong clip of (f, g), where $f : \mathbb{Z}_p \to \mathbb{Z}_q$, $g : \mathbb{Z}_q \to \mathbb{Z}_p$.

Theorem 3.2. *Let $f : \mathbb{Z}_p \to \mathbb{Z}_q$ and $g : \mathbb{Z}_q \to \mathbb{Z}_p$ be mappings such that $|Im(f)| > 1$, $|Im(g)| > 1$, $f(0) = 0$, $g(0) = 0$. Then a pair of mappings (f,g) is chained whenever p and q are different primes.*

Proof. Let us suppose that a pair $(f,\ g)$ is free. By Theorem 2.1, $\alpha = [B_1, B_2]$ is a factorization of $\mathbb{Z}_p \times \mathbb{Z}_q$ where

$$B_1 = \{(a, f(a)) |\, 0 \le a \le p-1\},\ B_2 = \{(g(b), b) |\, 0 \le b \le q-1\}.$$

Since $f(0) = 0$ and $g(0) = 0$, it is a normalized factorization. By Rédei's theorem, either B_1 or B_2 is a group. Therefore, either $f(a) = 0,\ a \in \mathbb{Z}_p$ or $g(b) = 0,\ b \in \mathbb{Z}_q$. However, this contradicts the assumption that $|\mathrm{Im}(f)| > 1$, $|\mathrm{Im}(g)| > 1$. Therefore, $(f$,$g)$ must be chained. □

The previous theorem says that under the conditions stated above, there always exist numbers $i_1, i_2 \in \mathbb{Z}_p$ and $j_1, j_2 \in \mathbb{Z}_q$, $i_1 \neq i_2$, $j_1 \neq j_2$ such that

$$f(i_1) - f(i_2) \equiv j_1 - j_2 \pmod{q}$$

$$g(j_1) - f(j_2) \equiv i_1 - i_2 \pmod{p}$$

when p and q are different primes. In other words, it says that every two mappings $f : \mathbb{Z}_p \to \mathbb{Z}_q$ and $g : \mathbb{Z}_q \to \mathbb{Z}_p$ are chained, unless one of them is a constant mapping.

Note that the previous claim is equivalent to Rédei's theorem for the case $\mathbb{Z}_p \times \mathbb{Z}_q$. Thus, it might be potentially interesting alternative way of proving Rédei's theorem. The following example shows that the assumption for p and q to be different primes can not be dropped.

Example 3.3. *Consider mappings $f : \mathbb{Z}_3 \to \mathbb{Z}_3$, $g : \mathbb{Z}_3 \to \mathbb{Z}_3$, defined as*

$$f = \begin{pmatrix} 0 & 1 & 2 \\ 0 & 1 & 2 \end{pmatrix} \; g = \begin{pmatrix} 0 & 1 & 2 \\ 0 & 2 & 1 \end{pmatrix}.$$

As we see, $|\mathrm{Im}(f)| > 1$, $|\mathrm{Im}(g)| > 1$, $f(0) = 0$, $g(0) = 0$. However, (f, g) is not chained. Therefore, $(f,\ g)$ is free and $\alpha = [B_1, B_2]$ is a factorization of $\mathbb{Z}_3 \times \mathbb{Z}_3$, where

$$B_1 = \{(0,0), (1,1), (2,2)\},\ \ B_2 = \{(0,0), (1,2), (2,1)\}.$$

4. SUMMARY

In this paper, a novel approach, based on circulant matrices, for studying group factorizations has been shown. We believe that there is a significant potential of circulant matrices for further research. Also, we underlined an interesting number theoretic result that is equivalent to Rédei's theorem for the special case of the group $\mathbb{Z}_p \times \mathbb{Z}_q$. Thus, there might be an interesting alternative approach for proving Rédei's theorem in that special case $\mathbb{Z}_p \times \mathbb{Z}_q$.

REFERENCES

1. Nataša Božović and Žarko Mijajlović. *Uvod u Teoriju Grupa*. Naučna knjiga, Beograd, 1990.
2. Vladimir Božović. *Factorization of finite groups*. VDM Verlag Dr. Müller, Saarbrücken, 2009.
3. Vladimir Božović and Nicola Pace. Factorization of groups using free mappings. *Journal of Algebra and its Applications*, 7(5):647–662, 2008.
4. P.J. Davis. *Circulant Matrices*. John Wiley and Sons, 1979.
5. A. D. Sands. On the factorization of finite groups. *J. London Math. Soc.*, 2(7):627–631, 1974.
6. S. Szabó. *Topics in Factorization of Abelian Groups*. Birkhäuser, 2004.